Math. Ann. 325, 413–448 (2003) **Mathematische Annalen**

DOI: 10.1007/s00208-002-0368-7

Abelian varieties over cyclotomic fields with good reduction everywhere

René Schoof

Received: 19 April 2001 / Revised version: 21 October 2001 /
Published online: 10 February 2003 – © Springer-Verlag 2003

Abstract. For every conductor $f \notin \{1, 3, 4, 5, 7, 8, 9, 11, 12, 15\}$ there exist non-zero abelian varieties over the cyclotomic field $\mathbf{Q}(\zeta_f)$ with good reduction everywhere. Suitable isogeny factors of the Jacobian variety of the modular curve $X_1(f)$ are examples of such abelian varieties. In the other direction we show that for all f in the above set there do not exist any non-zero abelian varieties over $\mathbf{Q}(\zeta_f)$ with good reduction everywhere except possibly when $f = 11$ or 15. Assuming the Generalized Riemann Hypothesis (GRH) we prove the same result when $f = 11$ and 15.

1. Introduction

In 1983 J.M. Fontaine [10] and V.A. Abraškin [1] proved one of the conjectures made by Shafarevič at the 1962 ICM in Stockholm: they showed that there do not exist any non-zero abelian varieties over $\mathbf{Q}$ with good reduction modulo every prime. In this paper we determine the cyclotomic fields $\mathbf{Q}(\zeta_f)$ to which their theorem can be extended. Here ζ_f denotes a primitive f-th root of unity. Our main result is the following.

Theorem 1.1. *For every conductor $f \notin \{1, 3, 4, 5, 7, 8, 9, 11, 12, 15\}$ there exist non-zero abelian varieties over $\mathbf{Q}(\zeta_f)$ with good reduction everywhere. Conversely, for all f in the above set there do not exist any non-zero abelian varieties over $\mathbf{Q}(\zeta_f)$ with good reduction everywhere except possibly when $f = 11$ or 15. Assuming the Generalized Riemann Hypothesis (GRH) the same is true when $f = 11$ and 15.*

The first statement of the theorem is a direct consequence of a result of R. Langlands [14, Prop.2 on p.263] implying that certain isogeny factors of the Jacobian varieties $J_1(f)$ of the modular curves $X_1(f)$ have good reduction everywhere over $\mathbf{Q}(\zeta_f)$. More precisely, $J_1(f)$ admits the Galois group of the covering $X_1(f) \longrightarrow X_0(f)$ as an automorphism group. This group is isomorphic to $(\mathbf{Z}/f\mathbf{Z})^*/\{\pm 1\}$. Therefore there is a decomposition into a product of isogeny factors

R. Schoof
Departimento di Mathematica, 2ª Università di Roma "Tor Vergata", I-00133 Roma, Italy
(e-mail: schoof@science.uva.nl)

$$J_1(f) \sim \prod_{\psi} J_{f,\psi},$$

where ψ runs over the rational even characters of $(\mathbf{Z}/f\mathbf{Z})^*$. The abelian varieties $J_{f,\psi}$ are defined over $\mathbf{Q}$. When the conductor of ψ is equal to f, the variety $J_{f,\psi}$ acquires good reduction everywhere over the maximal real subfield of $\mathbf{Q}(\zeta_f)$. The dimension of $J_{f,\psi}$ is equal to the dimension of the vector space of cusp forms of weight 2 for the modular group $\Gamma_1(f)$ and character ψ. For $f > 1$ it is given by

$$\dim J_{f,\psi} = \frac{f}{12}\prod_{p|f}\left(1+\frac{1}{p}\right) - \frac{1}{2}\#\{d|f : \gcd\left(d, \frac{f}{d}\right) = 1\}$$
$$-\frac{1}{4}\sum_{\substack{x\in\mathbf{Z}/f\mathbf{Z}\\ x^2+1=0}} \psi(x) - \frac{1}{3}\sum_{\substack{x\in\mathbf{Z}/f\mathbf{Z}\\ x^2+x+1=0}} \psi(x).$$

This formula [5] easily implies that for any conductor $f \notin \{1, 3, 4, 5, 7, 8, 9, 11, 12, 15\}$ there exists a character ψ of conductor f, for which $J_{f,\psi} \neq 0$. These happen to be the conductors f for which the genus of $X_1(f)$ is at least 2. Incidentally, we recall that conductors f are never congruent to 2 (mod 4). This is no restriction since $\mathbf{Q}(\zeta_f) = \mathbf{Q}(\zeta_{f/2})$ whenever $f \equiv 2 \pmod 4$.

This paper is concerned with the other two statements of Theorem 1.1. Their proof proceeds by studying finite flat group schemes and their extensions by one another over the global rings $\mathbf{Z}[\zeta_f]$. We give an outline of the strategy of the proof. For the conductors $f = 7$ and 11 certain “exotic” group schemes over $\mathbf{Z}[\zeta_f]$ appear. Below we discuss the modifications that need to be made in these cases.

First we show that for a suitable small prime number p, all simple p-group schemes over $\mathbf{Z}[\zeta_f]$ do, in fact, have order p. Here *p-group scheme* is short for “finite flat commutative group scheme of p-power order” and a p-group scheme is called simple if it does not have any non-trivial closed flat subgroup schemes. The proof uses Fontaine’s and Abrashkin’s bounds [1,10] on the ramification of the Galois action, Odlyzko’s discriminant bounds, global class field theory and some group theory. Odlyzko’s bounds [12] are much stronger if one assumes the truth of the Generalized Riemann Hypothesis (GRH). This explains why we obtain a stronger theorem when we assume GRH.

Then we employ the classification theorem of Oort and Tate [20] and check that the only group schemes of order p over $\mathbf{Z}[\zeta_f]$ are actually isomorphic to the constant group scheme $\mathbf{Z}/p\mathbf{Z}$ or its Cartier dual μ_p. This implies that every p-group scheme admits a filtration with closed flat subgroup schemes and subquotients isomorphic to either $\mathbf{Z}/p\mathbf{Z}$ or μ_p. Under some further easily verifiable conditions certain obstruction groups vanish and much more is true: one can show that every p-group scheme G over $\mathbf{Z}[\zeta_f]$ admits an exact sequence

$$0 \longrightarrow M \longrightarrow G \longrightarrow C \longrightarrow 0$$

with C a constant group scheme and M diagonalizable, i.e., M is Cartier dual to a constant group scheme.

To complete the proof of the theorem for $\mathbf{Q}(\zeta_f)$, one applies this result to the p-group scheme $A[p^k]$ of p^k-th torsion points of the Néron model of an abelian variety A over $\mathbf{Q}(\zeta_f)$ which is supposed to have good reduction everywhere. Reducing A modulo a prime ideal leads to a contradiction when $k \to \infty$ unless $A = 0$.

As we already pointed out, there are two notable exceptions to this outline and these take up most of the paper. For $f = 7$ we take $p = 2$. Since $2 = \pi\overline{\pi}$, where π denotes the prime $\frac{1+\sqrt{-7}}{2} \in \mathbf{Z}[\zeta_7]$, there are *four* simple 2-group schemes over $\mathbf{Z}[\zeta_7]$. These are $\mathbf{Z}/2\mathbf{Z}$, μ_2, a group scheme that is étale at $\overline{\pi}$ and multiplicative at π and one for which it is the other way around. We complete the proof by analyzing all possible extensions of these four group schemes by one another.

When $f = 11$ we also take $p = 2$. Under assumption of GRH we show that there exist precisely three simple 2-group schemes over $\mathbf{Z}[\zeta_{11}]$. These are $\mathbf{Z}/2\mathbf{Z}$, μ_2 and a certain self-dual group scheme E of order 4 that is local-local at 2. The main difficulty is then to prove that any extension of the group scheme E by itself is trivial.

In section 2 we provide the main ingredients of our proof. This leaves us with the explicit condition of Prop.2.2, involving certain p-extensions of $\mathbf{Q}(\zeta_f, \zeta_p)$. We check this condition, case by case, in section 3. The exceptional cases $f = 7$ and 11 are discussed in sections 4 and 5 respectively. For $f = 11$ we use the theory of Honda systems for a local computation. The computation is done in section 6.

It is not true that abelian varieties with good reduction everywhere over $\mathbf{Q}(\zeta_f)$ are necessarily isogeny factors of the Jacobian variety of $X_1(f)$. The latter are always isogenous to their Galois conjugates. Richard Pinch found the following elliptic curve over $\mathbf{Q}(\sqrt{509})$:

$$Y^2 + XY + \frac{1+\sqrt{509}}{2} Y = X^3 + (3+\sqrt{509})X^2 + \frac{327+3\sqrt{509}}{2} X + 88 + 17\sqrt{509}.$$

It has good reduction everywhere. Modulo the two primes over 5 it has 3 and 8 rational points respectively. Therefore the curve is not isogenous to its Galois conjugate and it cannot be an isogeny factor of $J_1(509)$.

For small conductors f not in the list of Theorem 1.1, the methods of this paper still give substantial information about the abelian varieties over $\mathbf{Q}(\zeta_f)$ that have good reduction everywhere. We mention the following result [18] without proof.

Theorem. *The elliptic curve E given by*

$$Y^2 + (i+1)XY + iY = X^3 + iX^2$$

acquires good reduction everywhere over $\mathbf{Q}(\zeta_{20})$. *Moreover, under assumption of the Generalized Riemann Hypothesis, every abelian variety over* $\mathbf{Q}(\zeta_{20})$ *with good reduction everywhere is isogenous to* E^g *for some* $g \geq 0$.

Finally, we remark that it is possible to prove similar results for other number fields F of small root discriminant. See [16, 17] for a study of abelian varieties over real quadratic fields with good reduction everywhere. I would like to thank Bas Edixhoven for many explanations and the referee for his numerous helpful comments on an earlier version of this paper.

2. Finite flat group schemes of p-power order

In this section we collect the basic ingredients of our proof. Let R be a commutative ring. For a prime p, a *p-group scheme* is a commutative finite flat group scheme of p-power order over R. If G is a p-group scheme, so is its Cartier dual $G^\vee$. The group schemes μ_{p^n} of the p^n-th roots of unity and their Cartier duals $\mathbf{Z}/p^n\mathbf{Z}$ are p-group schemes. A *constant* p-group scheme is an étale p-group scheme over R with trivial Galois action on its points. By Galois theory, a constant p-group scheme is isomorphic to a product of group schemes of the form $\mathbf{Z}/p^n\mathbf{Z}$. A *diagonalizable* p-group scheme is the Cartier dual of a constant p-group scheme. Equivalently, it is a product of group schemes of the form μ_{p^n}.

A p-group scheme is called *simple* if it does not admit any non-trivial closed flat subgroup schemes. Every p-group scheme of order p is simple. In particular, the p-group schemes $\mathbf{Z}/p\mathbf{Z}$ and μ_p are simple. Every p-group scheme G admits a filtration

$$0 = G_s \subset G_{s-1} \subset \ldots \subset G_1 \subset G_0 = G$$

by closed flat subgroup schemes with *simple* successive subquotients G_i/G_{i+1}.

The strategy to prove Theorem 1.1 is the same as in [10, section 3.4.3]. We summarize it in the Theorem below.

Theorem 2.1. *Let F be a number field and let O_F be its ring of integers. Let p be a prime. Suppose that*

(A) All simple p-group schemes over O_F have order p.
(B) The only p-group schemes of order p over O_F are $\mathbf{Z}/p\mathbf{Z}$ and μ_p.
(C) Over O_F we have that
  (i) every extension of a constant p-group scheme by a constant p-group scheme is again constant,
  (ii) every extension of a diagonalizable p-group scheme by a diagonalizable p-group scheme is again diagonalizable,
  (iii) any extension

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

  splits.

Then

(I) For every finite p-group scheme G over O_F there is an exact sequence

$$0 \longrightarrow M \longrightarrow G \longrightarrow C \longrightarrow 0$$

with M diagonalizable and C constant.

(II) There do not exist non-zero abelian varieties over F with good reduction everywhere.

Proof. Note that the condition in *(C)(iii)* is equivalent to the condition that every extension of a diagonalizable p-group scheme by a constant one is split. We proceed by induction on the order of G. If G has order p, it is simple and by *(B)* isomorphic to either $\mathbf{Z}/p\mathbf{Z}$ or μ_p. Let G be an arbitrary p-group scheme over O_F. By condition *(A)*, we can filter G with simple subquotients of order p. By condition (B), all these subquotients are in fact isomorphic to either $\mathbf{Z}/p\mathbf{Z}$ or μ_p. Therefore there is an exact sequence $0 \longrightarrow H \longrightarrow G \longrightarrow P \longrightarrow 0$ where P is either $\mathbf{Z}/p\mathbf{Z}$ or μ_p. By induction there exists an exact sequence $0 \longrightarrow M \longrightarrow H \longrightarrow C \longrightarrow 0$ with M diagonalizable and C constant. Consider the extension

$$0 \longrightarrow H/M \longrightarrow G/M \longrightarrow P \longrightarrow 0.$$

If $P \cong \mathbf{Z}/p\mathbf{Z}$, we deduce from *(C)(i)* that the group scheme G/M is constant, which implies *(I)*. If $P \cong \mu_p$, we deduce from *(C)(iii)* that $G/M \cong C \times P$. Let $M' \subset G$ be the closed flat subgroup scheme which contains M and for which $M'/M \cong P$. Then M' is an extension of P by M and hence, by *(C)(ii)* the group scheme M' is multiplicative and by construction $G/M' \cong C$. This proves *(I)*.

To prove *(II)*, let A be the Néron model of an abelian variety over F with good reduction everywhere. Let $n \geq 1$ and let $A[p^n]$ be the kernel of the multiplication by p^n map $A \longrightarrow A$. Since A has good reduction everywhere, $A[p^n]$ is a finite flat group scheme over O_F of order p^{2ng} where g is the dimension of A. By *(I)* there is an exact sequence

$$0 \longrightarrow M \longrightarrow A[p^n] \longrightarrow C \longrightarrow 0,$$

with M diagonalizable and C constant. By Cartier duality and the fact that the group schemes $A[p^n]^\vee$ and $A^{\text{dual}}[p^n]$ are isomorphic, there is another exact sequence:

$$0 \longrightarrow C^\vee \longrightarrow A^{\text{dual}}[p^n] \longrightarrow M^\vee \longrightarrow 0.$$

This gives rise to a closed immersion of the constant rank p^{2ng} group scheme $C \times M^\vee$ into the abelian variety $B_n = (A/M) \times (A^{\text{dual}}/C^\vee)$.

Now let $\mathfrak{q}$ be a prime of O_F and let k denote the finite field $O_F/\mathfrak{q}$. The abelian varieties A/M and $A^{\text{dual}}/C^\vee$ are isogenous to A over k. Therefore their numbers of points are equal to the number of points A over k. It follows that the number of points of B_n over k does not depend on n. On the other hand, the abelian varieties B_n have at least p^{2ng} points over k. This is only possible when $g = 0$ and the theorem follows.

As we will see below, conditions *(B)* and *(C)* of Theorem 2.1 are often true and in any case, it is usually easy to check them. On the other hand, checking condition *(A)* seems to be very hard in general. Conditions (A), (B) and (C) are addressed in Propositions 2.2, 2.5 and 2.6 below.

We introduce certain p-group schemes that were constructed by N. Katz and B. Mazur. See [11, Interlude (8.7)]. Let R be a ring and let $\varepsilon \in R^*$. Consider the R-algebra

$$A = \bigoplus_{i=0}^{p-1} R[X_i]/(X_i^p - \varepsilon^i).$$

For any R-algebra S with connected spectrum, the S-points of $T_\varepsilon = \mathrm{Spec}(A)$ are pairs (s, i) with $0 \le i < p$ and $s \in S$ satisfying $s^p = \varepsilon^i$. The scheme T_ε is a finite flat R-group scheme with multiplication of two points (t, i) and (s, j) given by

$$(t, i) \cdot (s, j) = \begin{cases} (ts, i + j); & \text{if } i + j < p, \\ (ts/\varepsilon, i + j - p); & \text{if } i + j \ge p. \end{cases}$$

The group scheme T_ε is killed by p. The projection $A \longrightarrow R[X_0]/(X_0^p - 1)$ induces a closed flat immersion of μ_p in T_ε. There is an exact sequence

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

Two extensions T_ε and $T_{\varepsilon'}$ are isomorphic whenever ε/ε' is a p-th power. If R is a field, the points of T_ε generate the field extension $R(\zeta_p, \sqrt[p]{\varepsilon})$. For $R = \mathbf{Z}$, $p = 2$ and $\varepsilon = -1$, the group scheme T_ε is the group scheme of order 4 in [13, p.58, Prop. 4.2., Ext.2].

In order to formulate the next proposition, we recall that the *root discriminant* δ_F of a number field F is given by $\delta_F = |\Delta_F|^{1/n}$ where Δ_F denotes the absolute discriminant of F and $n = [F : \mathbf{Q}]$.

Proposition 2.2. *(Condition (A)) Let F be a finite Galois extension of* $\mathbf{Q}$ *and let p be a prime. If every finite extension L of F satisfying the following conditions:*

1. *the field L is Galois over* $\mathbf{Q}$,
2. *the extension $F \subset L$ is unramified outside $p(\infty)$,*
3. $\sqrt[p]{\varepsilon} \in L^*$ *for every $\varepsilon \in O_F^*$,*
4. *the root discriminant of L satisfies*

$$\delta_L < \delta_F \cdot p^{1+\frac{1}{p-1}},$$

has the property that $P = \mathrm{Gal}(L/F(\zeta_p))$ is a finite p-group, then every simple p-group scheme over O_F has order p.

Proof. Let G be a simple p-group scheme over O_F. Then $p \cdot G = 0$. Let $\varepsilon_1, \ldots, \varepsilon_s$ denote generators of the group $O_F^*/(O_F^*)^p$. Let G' be the product of G by all its $\mathrm{Gal}(F/\mathbf{Q})$-conjugates, by μ_p and by the Katz-Mazur group schemes $T_{\varepsilon_1}, \ldots, T_{\varepsilon_s}$. The group scheme G' is a p-group scheme over O_F. Its points generate an extension L of F that is Galois over $\mathbf{Q}$ by construction. Since G' has p-power order, it is étale at the primes not dividing p and hence condition *2* is satisfied. The field L satisfies condition 4 because G' is killed by p so that [10, Cor.3.3.2] applies. Since the points of the group scheme T_{ε_i} generate the field $F(\zeta_p, \sqrt[p]{\varepsilon_i})$, condition *3* is also satisfied.

Therefore, by assumption, $P = \mathrm{Gal}(L/F(\zeta_p))$ is a p-group. Since the summands of G' are defined over F, the group P acts on each summand of $G'(\overline{F})$ and in particular on the p-group $G(\overline{F})$. We conclude that P has a non-trivial fixed point in $G(\overline{F})$. Since P is a normal subgroup of $\mathrm{Gal}(L/F)$, the P-invariants are a Galois submodule of $G(\overline{F})$. The Zariski closure of the corresponding F-group scheme is a flat closed subgroup scheme of G. Since G is simple, it is equal to G. This implies that P acts trivially on $G(\overline{F})$ and hence that the Galois action on $G(\overline{F})$ factors through $\Delta = \mathrm{Gal}(F(\zeta_p)/F)$.

The group Δ is cyclic of order a divisor of $p - 1$. The $\mathbf{F}_p[\Delta]$-module $G(\overline{F})$ is therefore a product of 1-dimensional eigenspaces. Since G is simple, there is only one such eigenspace and G has order p, as required.

Let R be a Noetherian ring, let $p \in R$ and let $\underline{Gr}_R$ denote the category of finite flat R-group schemes. Let $\widehat{R} = \lim\limits_{\leftarrow} R/p^n R$ and let $\underline{C}$ be the category of triples (G_1, G_2, θ) where G_1 is a finite flat $\widehat{R}$-group scheme, G_2 is a finite flat $R[\frac{1}{p}]$-group scheme and $\theta : G_1 \otimes_{\widehat{R}} \widehat{R}[\frac{1}{p}] \longrightarrow G_2 \otimes_{R[\frac{1}{p}]} \widehat{R}[\frac{1}{p}]$ is an isomorphism of $\widehat{R}[\frac{1}{p}]$-group schemes. Morphisms in $\underline{C}$ are pairs of morphisms of group schemes that are compatible with the morphisms θ.

Proposition 2.3. *Let R be a Noetherian ring and let $p \in R$. The functor $\underline{Gr}_R \longrightarrow \underline{C}$ that sends an R-group scheme G to the triple $(G \otimes_R \widehat{R}, G \otimes_R R[\frac{1}{p}], \mathrm{id} \otimes_R \widehat{R}[\frac{1}{p}])$ is an equivalence of categories.*

Proof. The proposition is an immediate consequence of [3, Thm.2.6]. Here M. Artin proves a similar equivalence of categories for finitely generated R-modules rather than finite flat R-group schemes, but the result for group schemes follows directly from functoriality.

Corollary 2.4. *Let R be a Noetherian ring, let $p \in R$ and let G and H be two finite flat group schemes over R. There is a natural exact "Mayer-Vietoris" sequence*

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_R(G, H) \longrightarrow \mathrm{Hom}_{\widehat{R}}(G, H) \times \mathrm{Hom}_{R[\frac{1}{p}]}(G, H) \\ \longrightarrow \mathrm{Hom}_{\widehat{R}[\frac{1}{p}]}(G, H) \xrightarrow{\delta} \mathrm{Ext}^1_R(G, H) \longrightarrow \mathrm{Ext}^1_{\widehat{R}}(G, H) \\ \times \mathrm{Ext}^1_{R[\frac{1}{p}]}(G, H) \longrightarrow \mathrm{Ext}^1_{\widehat{R}[\frac{1}{p}]}(G, H) \end{aligned}$$

where δ maps a $\widehat{R}[\frac{1}{p}]$-morphism $\varphi : G \longrightarrow H$ to the extension of G by H that corresponds to the triple $((H \times G)_{\widehat{R}}, (H \times G)_{R[\frac{1}{p}]}, \theta)$ where $\theta(h, g) = (h + \varphi(g), g)$.

Proof. Since this result plays a central role in our computations, we present its proof in some detail. Since $\widehat{R} \times R[\frac{1}{p}]$ is faithfully flat over R, the first morphism is injective. Exactness at the second group in the sequence is a direct consequence from Prop.2.3. To show that the sequence is exact at the third group, we observe that for $\varphi \in \mathrm{Hom}_{\widehat{R}[\frac{1}{p}]}(G, H)$ the extension $\delta(\varphi)$ is trivial if and only if there exists $f \in \mathrm{Hom}_{R[\frac{1}{p}]}(G, H)$ such that the morphism $(H \times G)_{\widehat{R}[\frac{1}{p}]} \longrightarrow (H \times G)_{\widehat{R}[\frac{1}{p}]}$ given by $(h, g) \mapsto (h + (f + \varphi)(g), g)$ can be extended to a morphism ψ over $\widehat{R}$. This in turn is equivalent to the existence of a pair $(\psi, f) \in \mathrm{Ext}^1_{\widehat{R}}(G, H) \times \mathrm{Ext}^1_{R[\frac{1}{p}]}(G, H)$ mapping to $\psi - f = \varphi$ in $\mathrm{Ext}^1_{\widehat{R}[\frac{1}{p}]}(G, H)$.

To prove exactness at the group $\mathrm{Ext}^1_R(G, H)$, let X be an extension of G by H over R. Suppose that f and f' are isomorphisms of X with the trivial extension $H \times G$ over $\widehat{R}$ and $R[\frac{1}{p}]$ respectively. Over the ring $\widehat{R}[\frac{1}{p}]$ the morphism $f' f^{-1}$ is an automorphism of the extension $H \times G$. In other words, $f' f^{-1}(h, g) = (h + \varphi(g), g)$ for some $\varphi \in \mathrm{Hom}_{\widehat{R}[\frac{1}{p}]}(G, H)$ and hence $\delta(\varphi) = [X]$. Finally, suppose that X and X' are extensions of H by G over the rings $\widehat{R}$ and $R[\frac{1}{p}]$ respectively. Let $\theta : X \longrightarrow X'$ be an isomorphism over $\widehat{R}[\frac{1}{p}]$. Then the R-group scheme that corresponds via Prop.2.3 to the triple (X, X', θ) is an extension of H by G over R that maps to the pair $(X, X') \in \mathrm{Ext}^1_{\widehat{R}}(G, H) \times \mathrm{Ext}^1_{R[\frac{1}{p}]}(G, H)$.

This completes the proof of the corollary.

In the applications, R is the ring of integers of a number field F, the element p is a prime number, and G and H are p-group schemes. Then G and H are étale over $R[\frac{1}{p}]$ and we can identify them with their Galois modules. The Galois action is unramified outside p. The ring $\widehat{R}$ is a finite product of finite extensions of $\mathbf{Z}_p$ over which we can apply the theory of Oort-Tate [20], Raynaud [15] and Fontaine [8,9]. Finally, the ring $\widehat{R}[\frac{1}{p}] \cong F \otimes \mathbf{Q}_p$ is a product of p-adic fields. Over each of these fields the group schemes can be identified with their local Galois modules. Recently Fabrizio Andreatta extended Cor.2.4 by constructing a natural long exact sequence involving the higher Ext-groups [2].

For the sake of simplicity we formulate the next two propositions for *complex* number fields F only. This is fine for our main application, which is the field $F = \mathbf{Q}(\zeta_f)$. The assumption only makes a difference when $p = 2$. In this case one should replace the class number h_F by the so-called *narrow* class number. We do not need this and leave the generalization to arbitrary F to the reader.

Proposition 2.5. *(Condition (B)) Let F be a complex number field of class number h_F and let p be a prime for which*

$$\gcd(p - 1, h_F) = 1.$$

If either of the following conditions is satisfied, the only group schemes of order p over the ring of integers O_F are μ_p and $\mathbf{Z}/p\mathbf{Z}$.

(a) p is prime in O_F.

(b) p is odd and unramified in F. Moreover, the sequence

$$O_F^* \longrightarrow (O_F/pO_F)^* \xrightarrow{N} (\mathbf{Z}/p\mathbf{Z})^* \longrightarrow 0$$

is exact. Here $N : O_F \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Z}/p\mathbf{Z}$ denotes the norm map reduced mod p.

(c) the p-the root of unity ζ_p is in O_F and $1 - \zeta_p$ is prime in O_F. Moreover the reduction map $O_F^* \longrightarrow (O_F/(1-\zeta_p)O_F)^*$ is surjective.

Proof. Let G be a p-group scheme of order p over O_F. The proof makes use of the local results in the Oort-Tate paper [20] and of Proposition 2.3 above. Alternatively one can apply [20, Thm.3].

Part *(a)* is the statement of the last corollary of [20].

Since $\gcd(p-1, h_F) = 1$, the conditions of *(b)* imply by class field theory that every Dirichlet character of F of order dividing $p-1$ that is unramified outside p factors through $\mathrm{Gal}(F(\zeta_p)/F)$. Since $\mathrm{Aut}(G)$ has order $p-1$, this implies that the Galois group acts on the points of G through a power ω^i of the Teichmüller character ω. Let $\mathfrak{p}$ be a prime of F dividing p. Since p is unramified, it follows from [20, p.15, Remark 5] that over the completion at $\mathfrak{p}$, the group scheme G is isomorphic to $\mathbf{Z}/p\mathbf{Z}$, μ_p or an unramified twist of these group schemes. Therefore either ω^i or ω^{1-i} is unramified at $\mathfrak{p}$. The character ω has order $p-1$ and since $p \neq 2$, it is non-trivial and hence ramified at $\mathfrak{p}$. It follows that $i = 0$ or 1. When $i = 0$, the Galois action is trivial and hence G is constant over each completion. By Prop.2.3 it is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ over O_F. Similarly, when $i = 1$ we have that $G \cong \mu_p$.

In case *(c)*, class field theory and the fact that $\gcd(p-1, h_F) = 1$ imply that every character of of F of order dividing $p-1$ that is unramified outside p is trivial. Therefore the Galois group acts trivially on the points of G. By [20, p.14] the Hopf algebra of G over the completion $\widehat{O}_F$ at the prime $(1-\zeta_p)$ has the form $\widehat{O}_F[X]/(X^p - aX)$ for some divisor a of p. Since the points of G are rational, a must be a $(p-1)$-th power in $\widehat{O}_F$. Therefore $a = 1$ or $-p$ times the $(p-1)$-th power of a unit, corresponding to the group schemes $\mathbf{Z}/p\mathbf{Z}$ and μ_p respectively. Proposition 2.3 implies then that $G \cong \mathbf{Z}/p\mathbf{Z}$ and μ_p over O_F.

This proves the proposition.

Proposition 2.6. *(Condition (C)) Let F be a complex number field and let p be a prime.*

(i) If p does not divide the class number of F, then any extension over O_F of constant p-group schemes by ane another is constant and every extension over O_F of diagonalizable p-group schemes by one another is diagonalizable.

(ii) Suppose that p does not divide the class number of $F(\zeta_p)$. If either of the following conditions is true, every extension

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

is split.

1. *The absolute ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p-1$ for all primes $\mathfrak{p}$ of F over p.*
2. *We have that $\zeta_p \in F$ and there is only one prime $\mathfrak{p}$ over p in F.*

Proof. (i) See also [10, section 3.4.3]. Suppose that there is an exact sequence

$$0 \longrightarrow C_1 \longrightarrow G \longrightarrow C_2 \longrightarrow 0$$

with C_1 and C_2 constant. Then G is étale and its points generate an unramified abelian p-extension L of F. Since p does not divide the class number h_F, we have that $L = F$, so that G is constant by Galois theory. This proves the first statement of *(i)*. The second follows by Cartier duality from *(i)*.

To prove part *(ii)*, we observe that $\mathbf{Z}/p\mathbf{Z}$ is étale while μ_p is connected at the primes over p. This implies that $\mathrm{Hom}_{O_F\otimes\mathbf{Z}_p}(\mu_p, \mathbf{Z}/p\mathbf{Z}) = 0$. Since μ_p and $\mathbf{Z}/p\mathbf{Z}$ are flat, it follows that $\mathrm{Hom}_{O_F}(\mu_p, \mathbf{Z}/p\mathbf{Z}) = 0$. Moreover, any extension of μ_p by $\mathbf{Z}/p\mathbf{Z}$ is split over $O_F \otimes \mathbf{Z}_p$, since over the completions at the primes over p the connected components of G give sections $\mu_p \longrightarrow G$. It follows that G is killed by p over $O_F \otimes \mathbf{Z}_p$. Since G is flat, it is also killed by p over O_F. This implies that the extension L obtained by adjoining the points of G to $F(\zeta_p)$ has degree dividing p and is unramified at all primes. Since p does not divide the class number of $F(\zeta_p)$, it follows that $L = F(\zeta_p)$. Therefore the exact sequence of Galois modules is split over F and hence G is split over $O_F[\frac{1}{p}]$.

Therefore, by Cor.2.4 there is an exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_{O_F[\frac{1}{p}]}(\mu_p, \mathbf{Z}/p\mathbf{Z}) &\longrightarrow \mathrm{Hom}_{F\otimes\mathbf{Q}_p}(\mu_p, \mathbf{Z}/p\mathbf{Z}) \\ &\longrightarrow \mathrm{Ext}^1_{O_F}(\mu_p, \mathbf{Z}/p\mathbf{Z}) \longrightarrow 0 \end{aligned}$$

If $e_{\mathfrak{p}} < p-1$ for all primes $\mathfrak{p}$ over p, the p-th roots of unity are not contained in any of the completions at $\mathfrak{p}$. This implies that $\mathrm{Hom}_{F\otimes\mathbf{Q}_p}(\mu_p, \mathbf{Z}/p\mathbf{Z}) = 0$ and hence $\mathrm{Ext}^1_{O_F}(\mu_p, \mathbf{Z}/p\mathbf{Z}) = 0$ as required. If $\zeta_p \in F$ and there is only one prime over p, the first and second group in the exact sequence have order p. It follows that $\mathrm{Ext}^1_{O_F}(\mu_p, \mathbf{Z}/p\mathbf{Z})$ vanishes as required.

This proves the proposition.

Proposition 2.6 does not discuss extensions of the form

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

over rings of integers O_F of number fields F. These may be non-trivial when the ring O_F contains units of infinite order. The group schemes constructed by Katz and Mazur [11, Interlude 8.7] provide examples of such non-trivial extensions. See [12, p.58, Prop.4.1] for the case $F = \mathbf{Q}$.

3. Cyclotomic fields

In this section we investigate conditions *(A), (B)* and *(C)* of Theorem 2.1. Before doing this, we recall the following group theoretic facts. These are useful in reducing the computations below.

Lemma 3.1. *Let* Γ *be a finite group. Let* Γ' *denote its commutator subgroup and let* Γ'' *denote the commutator subgroup of* Γ'*. Then* Γ'' *admits no subgroups* $H \neq \Gamma''$ *that are normal in* Γ *and for which* Γ''/H *is cyclic of order prime to* $[\Gamma' : \Gamma'']$.

Proof. Let $H \subset \Gamma''$ be a a normal subgroup of Γ for which Γ''/H has order prime to $[\Gamma' : \Gamma'']$. Consider the exact sequence of groups

$$1 \longrightarrow \Gamma''/H \longrightarrow \Gamma'/H \longrightarrow \Gamma'/\Gamma'' \longrightarrow 1.$$

Since the orders of Γ'/Γ'' and Γ''/H are coprime, the sequence splits. Conjugation induces a homomorphism $h : \Gamma \longrightarrow \mathrm{Aut}(\Gamma''/H)$, because Γ'' and H are normal subgroups of Γ. Since $\mathrm{Aut}(\Gamma''/H)$ is abelian, Γ' is contained in the kernel of h. Therefore Γ'/Γ'' acts trivially on Γ''/H. It follows that Γ'/H is abelian and hence that $\Gamma'' = H$ as required.

Corollary 3.2. *Let* Γ *be a finite group satisfying*
- Γ'/Γ'' *is a 2-group;*
- $\#\Gamma'' < 25$.

Then either Γ'' *is a 2-group or 9 divides the order of* Γ''*.*

Proof. First of all, we note that Γ'' has order less than 60, so that it is solvable. Let $H \subset \Gamma''$ be the minimal subgroup for which Γ''/H is abelian of odd order. It is characteristic and hence normal in Γ. Since $\#\Gamma'' < 25$, Lemma 3.1 implies that either Γ''/H has order 9, in which case the proof is complete, or $\Gamma'' = H$. In the latter case Γ''/Γ''' is a 2-group.

If Γ''/Γ''' is cyclic, then $M = \Gamma'''/\Gamma''''$ is a group of odd order. Since $\#M < 25$, an application of Lemma 3.1 to the group Γ'/Γ'''' shows that M has order 9 or is trivial. In either case the proof is complete. If Γ''/Γ''' is not cyclic, it has order at least 4 and hence $\#\Gamma''' \leq 6$. An application of Lemma 3.1 to Γ' shows that Γ'''/Γ'''' is a 2-group. If the order of Γ'''/Γ'''' is 1 or 4, the group Γ'''' is clearly trivial and we are done. If the order is 2, the group Γ'''' has odd order and an application of Lemma 3.1 to the group Γ'' shows that Γ'''' is trivial as well.

This completes the proof of the corollary.

We deal with the cases $f = 1, 3$ and 4 by observing that the three corresponding cyclotomic fields are subfields of $\mathbf{Q}(\zeta_{12})$. For each of the remaining conductors f we choose a suitable prime p. Since we employ Odlyzko's discriminant bounds [12] to verify condition *(A)*, it is important that p is small. For $f = 5, 7, 8, 9, 11, 12$

and 15 we choose $p = 2, 2, 3, 2, 2, 3$ and 2 respectively. In this section we do not discuss the exceptional cases cases $f = 7$ and 11. These are dealt with in sections 4 and 5 respectively.

The fact that conditions (B) and (C) are satisfied for $f = 5, 8, 9, 12$ and 15 follows from Propositions 2.5 and 2.6. We leave the easy verifications to the reader and concentrate on condition (A). We show that it too is satisfied in each case so that Theorem 2.1 applies and Theorem 1.1 follows for each conductor f in the list.

For the fields L of Proposition 2.2 we first use Odlyzko's discriminant bounds to transform the bound on the root discriminant of the extension L of $F = \mathbf{Q}(\zeta_f)$ into an upper bound for the degree of L over $\mathbf{Q}$. By Condition (A) the field L contains the extension $F' = F(\sqrt[p]{O_F^*})$ of F. In all eight cases Odlyzko's bounds luckily imply that $[L : F'] < 60$, so that $\mathrm{Gal}(L/F')$ is solvable. We use class field theory and group theory to show that $\mathrm{Gal}(L/F')$ is a p-group. This implies that $\mathrm{Gal}(L/F(\zeta_p))$ is a p-group, which is precisely what we need to know to be able to apply Prop.2.2 to verify condition *(A)*.

All computations can easily be done by hand. For class numbers of cyclotomic fields, see L.C. Washington's book [21, Ch.11]. For discriminant bounds, see the tables in J. Martinet's paper [12].

Case. $f = 5$. In this case $p = 2$ and $\delta_L < 4 \cdot 5^{3/4} = 13.375\ldots$. From the table in [12] we read that $[L : \mathbf{Q}] \leq 42$. We have the following inclusions

$$\mathbf{Q} \underset{4}{\subset} \mathbf{Q}(\zeta_5) \underset{4}{\subset} \mathbf{Q}(\zeta_{20}, \sqrt{\varepsilon}) \underset{\leq 2}{\subset} L,$$

where ε denotes the unit $(1 + \sqrt{5})/2$ of $\mathbf{Z}[\zeta_5]$. We conclude that $\mathrm{Gal}(L/\mathbf{Q}(\zeta_5))$ is a 2-group.

Case. $f = 8$. In this case $p = 3$ and $\delta_L < 4 \cdot 3^{3/2} = 20.785\ldots$. From the table in [12] we read that $[L : \mathbf{Q}] < 900$. We have the following inclusions

$$\mathbf{Q} \underset{4}{\subset} \mathbf{Q}(\zeta_8) \underset{2}{\subset} \mathbf{Q}(\zeta_{24}) \underset{3}{\subset} \mathbf{Q}(\zeta_{24}, \sqrt[3]{\varepsilon}) \underset{\leq 37}{\subset} L,$$

where ε denotes the unit $1 + \sqrt{2}$ of $\mathbf{Z}[\zeta_8]$. Let $\Gamma = \mathrm{Gal}(L/\mathbf{Q}(\zeta_{24}))$. The class number of $\mathbf{Q}(\zeta_{24})$ is 1. There are two primes $\mathfrak{p}$ and $\mathfrak{p}'$ over 3 in $\mathbf{Z}[\zeta_{24}]$. They satisfy $\mathfrak{p}^2\mathfrak{p}' = (\sqrt{-3})$. The units ζ_{24} and $1 - \zeta_{24}$ and their Galois conjugates generate a subgroup of index 3 inside the group

$$(\mathbf{Z}[\zeta_{24}]/(3))^* \cong \mathbf{F}_9^* \times \mathbf{F}_9^* \times \mathbf{F}_9 \times \mathbf{F}_9.$$

We briefly explain how to do this short computation. Other similar calculations in this section are left to the reader. Let ζ denote the 8th root of unity $\zeta_{24}^9 \in \mathbf{Z}[\zeta_{24}]$. Since $X^4 + 1 \equiv (X^2 + X - 1)(X^2 - X - 1) \pmod{3}$, we have that, say, $\zeta^2 + \zeta - 1 \equiv 0 \pmod{\mathfrak{p}}$ and $\zeta^2 - \zeta - 1 \equiv 0 \pmod{\mathfrak{p}'}$. For each of the order 8 cyclic groups $(\mathbf{Z}[\zeta_{24}]/\mathfrak{p})^*$ and $(\mathbf{Z}[\zeta_{24}]/\mathfrak{p}')^*$ we choose the image of ζ as a generator. Since $\zeta_{24} \equiv \zeta \pmod{\sqrt{-3}}$, we identify the image of ζ_{24} in $(\mathbf{Z}[\zeta_{24}]/(\sqrt{-3}))^*$ with the vector $(1, 1)$ in $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. Since

$$\begin{aligned} 1 - \zeta_{24} &\equiv 1 - \zeta \equiv -\zeta^2 \;\; \equiv \zeta^6 \pmod{\mathfrak{p}}, \\ &\equiv 1 - \zeta \equiv -\zeta^{-1} \equiv \zeta^3 \pmod{\mathfrak{p}'}, \end{aligned}$$

the image of $1 - \zeta_{24}$ is identified with the vector $(6, 3)$. Since the vectors $(1, 1)$ and $(6, 3)$ generate the additive group $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$, the images of the units ζ_{24} and $1 - \zeta_{24}$ generate the unit group $(\mathbf{Z}[\zeta_{24}]/(\sqrt{-3}))^*$.

It remains to deal with the 3-part. The 8th powers of the units ζ_{24} and $1 - \zeta_{24}$ are contained in it. Clearly $\zeta_3 = \zeta_{24}^8$ is a cube root of unity. Put $\pi = \zeta_3 - 1$. The conjugates of $1 - \zeta_{24}^a$ are of the form $1 - \zeta^a(1 + \pi)^a$ for $a \in (\mathbf{Z}/24\mathbf{Z})^*$. We have that

$$(1 - \zeta^a(1 + \pi)^a)^8 \equiv (1 - \zeta^a)^8 - 8a\pi\zeta^a(1 - \zeta^a)^7 \equiv 1 + \frac{a\zeta^a}{1 - \zeta^a}\pi \pmod{\pi^2}.$$

The multiplicative group $(\mathbf{Z}[\zeta_{24}]/(3))^*$ modulo the subgroup generated by the units ζ_{24} and $1 - \zeta_{24}$ and their conjugates is isomorphic to the *additive* group $\mathbf{Z}[\zeta_{24}]/(\sqrt{-3})$ modulo the subgroup generated by 1 and by the numbers $\frac{a\zeta^a}{1-\zeta^a}$ for $a \in (\mathbf{Z}/24\mathbf{Z})^*$. Equivalently, it is isomorphic to the additive group of the ring $\mathbf{F}_3[X]/(X^4 + 1)$ modulo the subgroup generated by 1 and by the elements $\frac{aX^a}{1-X^a}$. It suffices to take $a = 1$ and 5 and the quotient group turns out to have order 3. This completes the computation.

It follows from class field theory that the ray class field of $\mathbf{Q}(\zeta_{24})$ of conductor $(3) = \mathfrak{p}^2\mathfrak{p}'^2$ is an extension of degree dividing 3. The relative discriminant of $K = \mathbf{Q}(\zeta_{24}, \sqrt[3]{\varepsilon})$ over $\mathbf{Q}(\zeta_{24})$ is equal to 9. Therefore, by the conductor discriminant formula, K is equal to the ray class field of conductor (3). Let K' be the maximal subfield of L which is an abelian extension of $\mathbf{Q}(\zeta_{24})$. Then $K \subset K'$. If K' were strictly larger than K, then there would exist characters of $\mathrm{Gal}(K'/\mathbf{Q}(\zeta_{24}))$ of conductor $\mathfrak{p}^a\mathfrak{p}'^b$ with either a or b at least 3. The conductor discriminant formula then implies that $\delta_{K'} \geq 3^{76/72} \cdot \delta_{\mathbf{Q}(\zeta_{24})} = 4 \cdot 3^{14/9}$ which contradicts the fact that $\delta_{K'} \leq \delta_L < 4 \cdot 3^{3/2}$. We conclude that $\Gamma' = \mathrm{Gal}(L/K)$ is the commutator subgroup of $\Gamma = \mathrm{Gal}(L/\mathbf{Q}(\zeta_{24}))$.

Consider Γ'/Γ''. It is the Galois group of the maximal abelian extension of K inside L. The root discriminant of K is equal to $3^{7/6} \cdot 4 \approx 14.411$. Therefore by Odlyzko's bounds, the absolute degree of its Hilbert class field is at most 60 and the class number h_K of K satisfies $h_K < 60/24$ and hence $h_K \leq 2$. Since $\mathrm{Gal}(K/\mathbf{Q}(\zeta_{24}))$ is cyclic of order 3 and $\mathbf{Q}(\zeta_{24})$ has class number 1, the class number h_K cannot be equal to 2. Therefore $h_K = 1$. Since K is totally ramified over $\mathbf{Q}(\zeta_{24})$ at the primes over 3, the residue fields of these primes are the same and, just like $\mathbf{Q}(\zeta_{24})$, the field K does not admit any extensions that are at most tamely ramified at the primes over 3.

This implies that Γ'/Γ'' and hence Γ/Γ'' are 3-groups. However, Γ/Γ' is cyclic and this implies that Γ'/Γ'' is trivial. Since the group Γ' has order at most 37, it is solvable and we conclude that Γ' itself is trivial. Therefore $\mathrm{Gal}(L/\mathbf{Q}(\zeta_{24}))$ has order 3 and is a 3-group as required.

Case. $f = 9$. In this case $p = 2$ and $\delta_L < 4 \cdot 3^{3/2} = 20.785\ldots$. From the table in [12] we read that $[L : \mathbf{Q}] < 900$. We have the following inclusions

$$\mathbf{Q} \underset{6}{\subset} \mathbf{Q}(\zeta_9) \underset{2}{\subset} \mathbf{Q}(\zeta_{36}) \underset{4}{\subset} \mathbf{Q}(\zeta_{36}, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}) \underset{\leq 18}{\subset} L,$$

where ε_1 and ε_2 denote a basis for the unit group $\mathbf{Z}[\zeta_9]^*$ modulo torsion. Let $\Gamma = \mathrm{Gal}(L/\mathbf{Q})$. Since the root discriminant of $\mathbf{Q}(\zeta_{36\cdot 2}) = 4 \cdot \delta_{\mathbf{Q}(\zeta_9)} > \delta_L$, the field $\mathbf{Q}(\zeta_{36})$ is the largest abelian extension of $\mathbf{Q}$ contained in L and hence the commutator subgroup Γ' of Γ is equal to $\mathrm{Gal}(L/\mathbf{Q}(\zeta_{36}))$.

The class number of $\mathbf{Q}(\zeta_{36})$ is 1 and a short computation shows that the group

$$(\mathbf{Z}[\zeta_{36}]/(2))^* \cong \mathbf{F}_{64}^* \times \mathbf{F}_{64}$$

modulo the group of units generated by the global units ζ_{36}, $1 - \zeta_{36}$ and their conjugates, has order 4. Since the conductor of $K = \mathbf{Q}(\zeta_{36}, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_2})$ is (2), it follows from class field theory that K is equal to the ray class field of conductor 2 of $\mathbf{Q}(\zeta_{36})$. If $\mathbf{Q}(\zeta_{36})$ admitted an abelian extension inside L which is strictly larger than K, this extension would have conductor divible by $(1+i)^3$. By the conductor discriminant formula its root discriminant would be at least $2^{17/8} \cdot \delta_{\mathbf{Q}(\zeta_9)} > \delta_L$. This is impossible and we conclude that K is the largest abelian extension of $\mathbf{Q}(\zeta_{36})$ inside L. The Galois group $\Gamma' = \mathrm{Gal}(L/\mathbf{Q}(\zeta_{36}))$ is the commutator subgroup of Γ and the commutator subgroup Γ'' of Γ' satisfies $\#\Gamma'' \leq 18$.

By Cor.3.2, Γ'' and hence Γ' are either 2-groups, in which case we are done, or the order of Γ'' is divisible by 9. To see that the second possibility cannot occur, we distinguish two cases. If $\#\Gamma'' = 9$, The field K admits an abelian extension of degree 9 inside L that is at most tamely ramified at the prime over 2. This extension has absolute degree 432 and, by the conductor discriminant formula, its root discriminant is equal to $2^{67/35} \cdot 3^{3/2} = 18.876\ldots$. Odlyzko's discriminant bounds imply then that its absolute degree is less than 250, a contradiction. On the other hand, if $\#\Gamma'' = 18$, the field L is an abelian degree 9 extension of a quadratic extension K' of K. It has absolute degree 864. Let $\mathfrak{p}$ denote the unique prime over 2 in K and suppose that the conductor of K' is $\mathfrak{p}^a$. Then the root discriminant of K' is equal to $2^{a/16+7/4} \cdot 3^{3/2}$. Since $\delta_{K'} \leq \delta_L < 4 \cdot 3^{3/2}$, we have that $a \leq 3$. A final application of the conductor discriminant formula to the tame extension L of K' shows that $\delta_L \leq 2^{287/144} 3^{3/2} = 20.684\ldots$. Odlyzko's bounds imply then that $[L : \mathbf{Q}] < 800$, a contradiction.

This completes the proof in this case.

Case. $f = 12$. In this case $p = 3$ and $\delta_L < 18$. From the table in [12] we read that $[L : \mathbf{Q}] < 170$. We have the following inclusions

$$\mathbf{Q} \underset{4}{\subset} \mathbf{Q}(\zeta_{12}) \underset{3}{\subset} \mathbf{Q}(\zeta_{36}) \underset{3}{\subset} \mathbf{Q}(\zeta_{36}, \sqrt[3]{\varepsilon}) \underset{\leq 4}{\subset} L$$

where $\varepsilon = 1 - \zeta_{12}$ generates the unit group $\mathbf{Z}[\zeta_{12}]^*$ modulo torsion. Consider $K = \mathbf{Q}(\zeta_{36}, \sqrt[3]{\varepsilon})$. Let $\pi = 1 - \zeta_9$ denote the unique prime over 3 in $\mathbf{Q}(\zeta_{36})$ and let π^a be the conductor of K over $\mathbf{Q}(\zeta_{36})$. By the conductor discriminant formula the root discriminant of K is then equal to $3^{1+a/9}\delta_{\mathbf{Q}(\zeta_{12})}$. Since $K \subset L$, we have that $1 + a/9 < 3/2$, i.e., $a \leq 4$. This implies that $\delta_K \leq 3^{13/9} \cdot \sqrt{12} \approx 16.935$. Therefore, by Odlyzko's bounds, the Hilbert class field of K has absolute degree at most 120. This implies that the class number of K satisfies $h_K \leq 120/36$. In other words $h_K \leq 3$. Since the class number of $\mathbf{Q}(\zeta_{36})$ is 1, the class number of K is not 2. In addition, since the unit $1 - \zeta_{36}$ generates the unit group of $\mathbf{F}_9$, the field K does not admit any abelian extensions that are unramified outside 3 and at most tamely ramified at 3. This implies that $[L : K]$ divides 3 and the proof in this case is complete.

Case. $f = 15$. In this case $p = 3$ and, under GRH, we have $\delta_L < 5^{3/4} \cdot 9 = 30.094\ldots$. From the table (under GRH) in [12] we read that $[L : \mathbf{Q}] < 2400$. We have the following inclusions

$$\mathbf{Q} \underset{8}{\subset} \mathbf{Q}(\zeta_{15}) \underset{81}{\subset} K \underset{\leq 3}{\subset} L$$

where K denotes the extension of $\mathbf{Q}(\zeta_{15})$ obtained by adjoining the cube roots of the units of $\mathbf{Z}[\zeta_{15}]$. To prove that $\mathrm{Gal}(L/\mathbf{Q}(\zeta_{15}))$ is a 3-group, it suffices to show that $[L : K] \neq 2$. Suppose $[L : K] = 2$. Then the 3-Sylow subgroup of $\mathrm{Gal}(L/\mathbf{Q}(\zeta_{15}))$ is normal. This implies that $\mathbf{Q}(\zeta_{15})$ admits a quadratic extension inside L. Since the class number of $\mathbf{Q}(\zeta_{15})$ is 1 and since the multiplicative group $\mathbf{F}_{81}^*$ of the residue field of the unique prime over 3 is generated by the units ζ_{15} and $1 - \zeta_{15}$, it follows from class field theory that the field $\mathbf{Q}(\zeta_{15})$ admits no quadratic extension that is unramified outside 3. This contradiction shows that $\mathrm{Gal}(L/\mathbf{Q}(\zeta_{15}))$ is a 3-group, as required.

4. The case $f = 7$

In this section we discuss the exceptional case $f = 7$. We put $F = \mathbf{Q}(\zeta_7)$ and $O_F = \mathbf{Z}[\zeta_7]$. Since we do not want to use Odlyzko's stronger discriminant bounds that are only valid under GRH, we are forced to work with the prime 2. The complications for $f = 7$ are caused by the fact that 2 splits in F: we have that $2 = \pi\overline{\pi}$ with $\pi = -\zeta_7 - \zeta_7^2 - \zeta_7^4 = \frac{1+\sqrt{-7}}{2} \in O_F$. By [20, Introduction], there are therefore *four* simple group schemes of order 2 over O_F. Apart from $\mathbf{Z}/2\mathbf{Z}$ and μ_2 there is the group scheme $G_\pi = \mathrm{Spec}(A)$ where $A = O_F[X]/(X^2 - \pi X)$, the comultiplication being given by $X \mapsto 1 \otimes X + X \otimes 1 - \overline{\pi} X \otimes X$. The other group scheme $G_{\overline{\pi}}$ is both the Galois conjugate and the Cartier dual of G_π. The group scheme G_π is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ over the completion at $\overline{\pi}$ and to μ_2 over the completion at π. For $G_{\overline{\pi}}$ it is the other way around. It follows that condition *(B)* of Theorem 2.1 is not satisfied for $f = 7$ and $p = 2$. It turns out that condition *(C)* is not satisfied either: there is a non-split exact sequence

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \xrightarrow{j} G_\pi \times G_{\overline{\pi}} \longrightarrow \mu_2 \longrightarrow 0. \qquad (*)$$

Here the Hopf algebra homomorphism corresponding to j is the morphism

$$O_F[X, Y]/(X^2 - \pi X, Y^2 - \overline{\pi} Y) \longrightarrow O_F[T]/(T^2 - T)$$

given by $X \mapsto \pi T$ and $Y \mapsto \overline{\pi} T$. Note that both group schemes G_π and $G_{\overline{\pi}}$ are already defined over the quadratic subring $\mathbf{Z}[\pi]$ of O_F.

The proof that we give in this section is a modification of the proofs given in sections 2 and 3. First we use Prop.2.2 to verify condition *(A)* and provide a substitute for *(B)*.

Theorem 4.1. *Up to isomorphism there are precisely four simple* 2*-group schemes over the ring* $\mathbf{Z}[\zeta_7]$. *They are* $\mathbf{Z}/2\mathbf{Z}$, μ_2, G_π *and* $G_{\overline{\pi}}$. *All have order 2.*

Proof. Let L be as in Proposition 2.2. We show that $\mathrm{Gal}(L/F)$ is a 2-group. We have that $\delta_L < 7^{5/6} \cdot 4 = 20.245\ldots$. From the table in [12] we read that $[L : \mathbf{Q}] < 600$. We have the following inclusions

$$\mathbf{Q} \underset{6}{\subset} \mathbf{Q}(\zeta_7) \underset{2}{\subset} \mathbf{Q}(\zeta_{28}) \underset{4}{\subset} \mathbf{Q}(\zeta_{28}, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}) \underset{\leq 12}{\subset} L,$$

where ε_1 and ε_2 are generators for the unit group $\mathbf{Z}[\zeta_7]^*$ modulo torsion. Let $\Gamma = \mathrm{Gal}(L/\mathbf{Q})$. Since the root discriminant of $\mathbf{Q}(\zeta_{28 \cdot 2}) = 4 \cdot \delta_{\mathbf{Q}(\zeta_7)} > \delta_L$, the field $\mathbf{Q}(\zeta_{28})$ is the largest abelian extension of $\mathbf{Q}$ contained in L and hence the commutator subgroup Γ' of Γ is equal to $\mathrm{Gal}(L/\mathbf{Q}(\zeta_{28}))$. We wish to show that Γ' is a 2-group.

The class number of $\mathbf{Q}(\zeta_{28})$ is equal to 1. There are two primes $\mathfrak{p}$ and $\mathfrak{p}'$ over 2 in $\mathbf{Z}[\zeta_{28}]$. The units ζ_7 and $1 - \zeta_{28}$ generate the group

$$\left(\mathbf{Z}[\zeta_7]/\mathfrak{p}\mathfrak{p}'\right)^* \cong \mathbf{F}_8^* \times \mathbf{F}_8^*.$$

By class field theory, the field $\mathbf{Q}(\zeta_{28})$ admits no extension that is unramified outside 2 and at most tamely ramified at 2. Therefore $\Gamma'/\,\Gamma''$ is a 2-group.

Since $\#\Gamma'' \leq 12$, it follows from Cor.3.2 that either Γ' is a 2-group, in which case we are done, or Γ'' has order 9. To exclude the second possibility, we first note that the absolute degree of L would be 432. Moreover, the field $K = \mathbf{Q}(\zeta_{28}, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_2})$ is contained in the ray class field of conductor (2) of $\mathbf{Q}(\zeta_{28})$ and L is an abelian extension of K that is at most tamely ramified at the primes over 2. It follows from the conductor discriminant formula that the root discriminant of L satisfies $\delta_L \leq 2^{67/36} \cdot 7^{5/6} = 18.386\ldots$. Odlyzko's bounds imply then that $[L : \mathbf{Q}] < 200$, a contradiction.

Therefore, by Prop.2.2, all simple 2-group schemes over $\mathbf{Z}[\zeta_7]$ have order 2. Since $2 = \pi\overline{\pi}$ in $\mathbf{Z}[\zeta_7]$, it follows from the discussion in [20, Introduction] that the only group schemes of order 2 are the ones listed. This proves the Theorem.

Next we study extensions of the four simple group schemes by one another and provide a substitute for condition *(C)*.

Proposition 4.2. *Over the ring $O_F = \mathbf{Z}[\zeta_7]$ we have the following.*

(i) Every extension of a constant 2-group scheme by a constant 2-group scheme is constant. Every extension of a diagonalizable 2-group scheme by a diagonalizable 2-group scheme is diagonalizable.

(ii) $\mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z})$ *has order 2. The exact sequence (*) represents the non-trivial class.*

(iii) $\mathrm{Ext}^1_{O_F}(G_\pi, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Ext}^1_{O_F}(G_{\overline{\pi}}, \mathbf{Z}/2\mathbf{Z}) = 0$ *and* $\mathrm{Ext}^1_{O_F}(\mu_2, G_\pi) = \mathrm{Ext}^1_{O_F}(\mu_2, G_{\overline{\pi}}) = 0$.

(iv) $\mathrm{Ext}^1_{O_F}(G_\pi, G_{\overline{\pi}}) = \mathrm{Ext}^1_{O_F}(G_{\overline{\pi}}, G_\pi) = 0$ *and* $\mathrm{Ext}^1_{O_F}(G_\pi, G_\pi) = \mathrm{Ext}^1_{O_F}(G_{\overline{\pi}}, G_{\overline{\pi}}) = 0$.

Proof. Recall that $F = \mathbf{Q}(\zeta_7)$. The ring $\widehat{O}_F = O_F \otimes \mathbf{Z}_2$ is the product of the two completions O_π and $O_{\overline{\pi}}$ at π and $\overline{\pi}$ respectively. Both rings O_π and $O_{\overline{\pi}}$ are unramified cubic extensions of $\mathbf{Z}_2$.

Since F has class number 1, part *(i)* follows from Prop.2.6 *(i)*. To prove *(ii)* one observes that over the ring $\widehat{O}_F$ the group scheme μ_2 is connected while $\mathbf{Z}/2\mathbf{Z}$ is étale. Therefore $\mathrm{Hom}_{\widehat{O}_F}(\mu_2, \mathbf{Z}/2\mathbf{Z})$ and hence $\mathrm{Hom}_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z})$ vanish. In addition, any extension

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

is split over the ring $\widehat{O}_F \cong O_\pi \times O_{\overline{\pi}}$ by the connected components. It follows that the field extension H of F generated by the points of G is everywhere unramified. Since the class number of F is 1, we have that $H = F$. In other words, the extension G is locally as well as generically split. The Mayer-Vietoris exact sequence of Cor.2.4 provides us therefore with an exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_{O_F[\frac{1}{2}]}(\mu_2, \mathbf{Z}/2\mathbf{Z}) &\longrightarrow \mathrm{Hom}_{F\otimes\mathbf{Q}_2}(\mu_2, \mathbf{Z}/2\mathbf{Z}) \\ &\longrightarrow \mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z}) \longrightarrow 0. \end{aligned}$$

The group $\mathrm{Hom}_{O_F[\frac{1}{2}]}(\mu_2, \mathbf{Z}/2\mathbf{Z})$ has order 2. On the other hand, since there are two primes over 2 in F, the $\mathbf{Q}_2$-algebra $F \otimes \mathbf{Q}_2$ is a product of two fields and hence the order of $\mathrm{Hom}_{F\otimes\mathbf{Q}_2}(\mu_2, \mathbf{Z}/2\mathbf{Z})$ is 4. It follows that $\mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z})$

has order 2. Since the scheme $G_\pi \times G_{\overline{\pi}}$ is connected, the exact sequence (*) is not split and therefore it provides the non-trivial extension class. This proves *(ii)*.

To prove *(iii)*, let G be an extension of G_π by $\mathbf{Z}/2\mathbf{Z}$ over O_F:

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow G_\pi \longrightarrow 0.$$

Since the O_π-group scheme G_π is connected, the groups $\mathrm{Hom}_{O_\pi}(G_\pi, \mathbf{Z}/2\mathbf{Z})$ and hence $\mathrm{Hom}_{O_F}(G_\pi, \mathbf{Z}/2\mathbf{Z})$ vanish. Over O_π the extension becomes $0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow \mu_2 \longrightarrow 0$. Therefore it is split by the connected component. It follows that G is killed by 2 over O_π. Since G is flat, it is also killed by 2 over O_F. Over $O_{\overline{\pi}}$ the group scheme G_π is isomorphic to $\mathbf{Z}/2\mathbf{Z}$. This implies that G is étale over $O_{\overline{\pi}}$. It follows that the field L obtained by adjoining the points of G to F is unramified at all primes. Since the class number of F is 1, we have that $L = F$ and we see that the Galois action on G is trivial and hence that G is split over $O_F[\frac{1}{2}]$. By Galois theory G is then also split over $O_{\overline{\pi}}$.

In other words, G is generically split as well as locally split. By Cor.2.4 we have an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{O_{\overline{\pi}}}(G_\pi, \mathbf{Z}/2\mathbf{Z}) \times \mathrm{Hom}_{O_F[\frac{1}{2}]}(G_\pi, \mathbf{Z}/2\mathbf{Z}) \longrightarrow$$
$$\longrightarrow \mathrm{Hom}_{F\otimes\mathbf{Q}_2}(G_\pi, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1_{O_F}(G_\pi, \mathbf{Z}/2\mathbf{Z}) \longrightarrow 0.$$

The groups $\mathrm{Hom}_{O_{\overline{\pi}}}(G_\pi, \mathbf{Z}/2\mathbf{Z})$ and $\mathrm{Hom}_{O_F\left[\frac{1}{2}\right]}(G_\pi, \mathbf{Z}/2\mathbf{Z})$ both have order 2 and the group $\mathrm{Hom}_{F\otimes\mathbf{Q}_2}(G_\pi, \mathbf{Z}/2\mathbf{Z})$ has order 4. We deduce that $\mathrm{Ext}^1_{O_F}(G_\pi, \mathbf{Z}/2\mathbf{Z}) = 0$.

We conclude that $\mathrm{Ext}^1_{O_F}(G_{\overline{\pi}}, \mathbf{Z}/2\mathbf{Z}) = 0$ as well, and hence, by duality,

$$\mathrm{Ext}^1_{O_F}(\mu_2, G_\pi) = \mathrm{Ext}^1_{O_F}(\mu_2, G_{\overline{\pi}}) = 0$$

as required.

Finally we prove *(iv)*. First we consider extensions of $G_{\overline{\pi}}$ by G_π:

$$0 \longrightarrow G_\pi \longrightarrow G \longrightarrow G_{\overline{\pi}} \longrightarrow 0.$$

Over the ring $O_{\overline{\pi}}$ the extension becomes $0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow \mu_2 \longrightarrow 0$ and is split by the connected component. It follows that G is killed by 2. In addition, adjoining the points of G to F gives a field extension H of degree at most 2 over F, which is unramified outside $\overline{\pi}$.

Over the ring O_π the extension looks like $0 \longrightarrow \mu_2 \longrightarrow G \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0$. We compute $\mathrm{Ext}^1_{O_\pi}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ by means of the exact sequence of *fppf* sheaves $0 \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Z} \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0$. This gives an exact sequence

$$0 \longrightarrow \mu_2(O_\pi) \longrightarrow \mathrm{Ext}^1_{O_\pi}(\mathbf{Z}/2\mathbf{Z}, \mu_2) \longrightarrow \mathrm{Ext}^1_{O_\pi}(\mathbf{Z}, \mu_2) \longrightarrow 0.$$

It follows from the Kummer sequence that $\mathrm{Ext}^1_{O_\pi}(\mathbf{Z}, \mu_2)$ is isomorphic to $O_\pi^*/(O_\pi^*)^2$. The same computation over the quotient field F_π of O_π gives rise to the following commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mu_2(O_\pi) \arrow[r] \arrow[d] & \mathrm{Ext}^1_{O_\pi}(\mathbf{Z}/2\mathbf{Z}, \mu_2) \arrow[r] \arrow[d] & O_\pi^*/(O_\pi^*)^2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mu_2(F_\pi) \arrow[r] & \mathrm{Ext}^1_{F_\pi}(\mathbf{Z}/2\mathbf{Z}, \mu_2) \arrow[r, "g"] & F_\pi^*/(F_\pi^*)^2 \arrow[r] & 0.
\end{tikzcd}$$

Here g is the Kummer map: if $F_\pi(\sqrt{\alpha})$ is the field generated by the points of an extension in $\mathrm{Ext}^1_{F_\pi}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$, then g maps the class of the extension to $\alpha \in F_\pi^*$ modulo squares. Since our G is an O_π-group scheme, α is in O_π^*. This implies that the conductor of $F_\pi(\sqrt{\alpha})$ over F_π is at most π^2.

We conclude from all this that the field H generated by the points of G, has conductor at most π^2 over F. The class number of F is 1 and a short computation shows that the units of O_F generate the group $O_\pi^*/(1 + (\pi^2))$. It follows then from class field theory that $H = F$. This implies that G is generically split. It follows that G is also split over the local field F_π. Since the left and rightmost vertical arrows in the diagram above are injective, so is the map $\mathrm{Ext}^1_{O_\pi}(\mathbf{Z}/2\mathbf{Z}, \mu_2) \longrightarrow \mathrm{Ext}^1_{F_\pi}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$. It follows that G is also split over the ring O_π.

Therefore G is locally split as well as generically split. It follows from Cor.2.4 that there is an exact sequence

$$0 \longrightarrow \mathrm{Hom}_{O_F}(G_{\overline{\pi}}, G_\pi) \longrightarrow \mathrm{Hom}_{\widehat{O}_F}(G_{\overline{\pi}}, G_\pi) \times \mathrm{Hom}_{O_F\left[\frac{1}{2}\right]}(G_{\overline{\pi}}, G_\pi) \longrightarrow$$
$$\longrightarrow \mathrm{Hom}_{F\otimes\mathbf{Q}_2}(G_{\overline{\pi}}, G_\pi) \longrightarrow \mathrm{Ext}^1_{O_F}(G_{\overline{\pi}}, G_\pi) \longrightarrow 0$$

A computation of the groups involved gives the exact sequence

$$0 \longrightarrow 0 \longrightarrow (0 \times \mathbf{F}_2) \times \mathbf{F}_2 \longrightarrow \mathbf{F}_2^2 \longrightarrow \mathrm{Ext}^1_{O_F}(G_{\overline{\pi}}, G_\pi) \longrightarrow 0$$

implying that $\mathrm{Ext}^1_{O_F}(G_{\overline{\pi}}, G_\pi) = 0$ and, by symmetry, that $\mathrm{Ext}^1_{O_F}(G_\pi, G_{\overline{\pi}}) = 0$ as required.

Finally we consider extensions of G_π by itself:

$$0 \longrightarrow G_\pi \longrightarrow G \longrightarrow G_\pi \longrightarrow 0.$$

Over the ring O_π the extension looks like $0 \longrightarrow \mu_2 \longrightarrow G \longrightarrow \mu_2 \longrightarrow 0$ and over $O_{\overline{\pi}}$ like $0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0$. The absolute Galois group of F acts on $G(\overline{F})$ via a character χ of order at most 2 which is only ramified at π. Then it acts on the points of the dual group via a character χ' that is unramified outside $\overline{\pi}$. If $G(\overline{F})$ were cyclic of order 4, then $\chi'\chi = \omega_4$. Here ω_4 denotes the Teichmüller character giving the action on the 4th roots of unity. Since the character ω_4 has conductor 4, the conductors of χ and χ' are equal to π^2 and $\overline{\pi}^2$ respectively. We already saw above that the ray class fields of F of conductor

π^2 and hence of conductor $\overline{\pi}^2$ are trivial. This implies that $\omega_4 = \chi'\chi = 1$, a contradiction. Therefore G is killed by 2.

Since G is killed by 2, the Galois group acts on $G(\overline{F})$ via a quadratic character χ that is unramified at $\overline{\pi}$ and for which $\omega_2\chi^{-1}$ is unramified at π. Since the Teichmüller character ω_2 is trivial, this means that the action is everywhere unramified and therefore trivial. We conclude that G is generically split. Since the Galois action on G is trivial and since G is étale over $O_{\overline{\pi}}$ and multiplicative over O_π, the group scheme G is by Galois theory also split over the rings O_π and $O_{\overline{\pi}}$. So, G is split both locally and generically. By Cor.2.4, there is an exact sequence

$$\begin{aligned} 0 \longrightarrow\ &\mathrm{Hom}_{O_F}(G_\pi, G_\pi) \longrightarrow \mathrm{Hom}_{\widehat{O}_F}(G_\pi, G_\pi) \times \mathrm{Hom}_{O_F[\frac{1}{2}]}(G_\pi, G_\pi) \longrightarrow \\ &\longrightarrow \mathrm{Hom}_{F\otimes\mathbf{Q}_2}(G_\pi, G_\pi) \longrightarrow \mathrm{Ext}^1_{O_F}(G_\pi, G_\pi) \longrightarrow 0. \end{aligned}$$

A computation of the groups involved gives the exact sequence

$$0 \longrightarrow \mathbf{F}_2 \longrightarrow \mathbf{F}_2^2 \times \mathbf{F}_2 \longrightarrow \mathbf{F}_2^2 \longrightarrow \mathrm{Ext}^1_{O_F}(G_\pi, G_\pi) \longrightarrow 0,$$

showing that $\mathrm{Ext}^1_{O_F}(G_\pi, G_\pi) = 0$ and, by symmetry, that $\mathrm{Ext}^1_{O_F}(G_{\overline{\pi}}, G_{\overline{\pi}}) = 0$ as required.

Corollary 4.3. *Let G be a 2-group scheme over $\mathbf{Z}[\zeta_7]$. Then it admits a filtration*

$$0 \subset G_1 \subset G_2 \subset G$$

with G_1 diagonalizable, G/G_2 étale and G_2/G_1 isomorphic to a product of group schemes isomorphic to G_π and $G_{\overline{\pi}}$.

Proof. The proof is a variation on the proof of Theorem 2.1. We filter G with closed flat subgroup schemes G_i in such a way that the subquotients are simple. By Theorem 4.1, the simple 2-group schemes are isomorphic to $\mathbf{Z}/2\mathbf{Z}$, μ_2, G_π or $G_{\overline{\pi}}$. By Proposition 4.2, we can modify the filtration as follows. If for some index i there are successive steps $G_{i-1} \hookrightarrow G_i \hookrightarrow G_{i+1}$ in the filtration with $G_i/G_{i-1} \cong \mathbf{Z}/2\mathbf{Z}$ and $G_{i+1}/G_i \cong G_\pi$ or $G_{\overline{\pi}}$, then we apply Prop.4.2 *(iii)* we replace G_i by another subgroup scheme G'_i with $G_{i-1} \hookrightarrow G'_i \hookrightarrow G_{i+1}$ so that $G'_i/G_{i-1} \cong G_\pi$ or $G_{\overline{\pi}}$ and $G_{i+1}/G'_i \cong \mathbf{Z}/2\mathbf{Z}$. If on the other hand $G_i/G_{i-1} \cong \mathbf{Z}/2\mathbf{Z}$ and $G_{i+1}/G_i \cong \mu_2$, then there are two possibilities. If the extension

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G_{i+1}/G_{i-1} \longrightarrow \mu_2 \longrightarrow 0$$

is split, then we replace G_i by a subgroup scheme G'_i with $G_{i-1} \hookrightarrow G'_i \hookrightarrow G_{i+1}$ so that $G'_i/G_{i-1} \cong \mu_2$ or $G_{\overline{\pi}}$ and $G_{i+1}/G'_i \cong \mathbf{Z}/2\mathbf{Z}$. If the extension is not split, we apply Prop.4.2 *(ii)* we replace G_i by a subgroup scheme G'_i with $G_{i-1} \hookrightarrow G'_i \hookrightarrow G_{i+1}$ so that $G_i/G_{i-1} \cong G_\pi$ and $G_{i+1}/G_i \cong G_{\overline{\pi}}$. Loosely speaking, “we can either push the subquotient $\mathbf{Z}/2\mathbf{Z}$ to the right, or make it disappear”.

This means that we can modify the filtration in such a way that we end up with a filtration

$$0 \subset G_2 \subset G$$

for which G/G_2 is filtered with subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$, while G_2 admits a filtration without subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$. We have "pushed all subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$ to the right". Similarly, applying Cartier duality, we can push all subquotients μ_2 occurring in the filtration of G_2 to the left. To be sure, this process does not introduce any subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$. The result is a filtration

$$0 \subset G_1 \subset G_2 \subset G$$

where G_1 is an extension of group schemes isomorphic to μ_2, the quotient G/G_2 is an extension of group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$ and G_2/G_1 admits a filtration with group schemes isomorphic to G_π and $G_{\overline{\pi}}$. It follows then from Prop.4.2 *(i)* that G_1 is diagonalizable and that G/G_2 is constant. Moreover, Prop.4.2 *(iv)* implies that G_2/G_1 is a product of copies of G_π and $G_{\overline{\pi}}$. This proves the Corollary.

Proposition 4.4. *There are no non-zero abelian varieties over $F = \mathbf{Q}(\zeta_7)$ with good reduction everywhere.*

Proof. Let A be the Néron model over $O_F = \mathbf{Z}[\zeta_7]$ of an abelian variety with good reduction everywhere and let $n \geq 1$. By Corollary 4.3 the 2-group scheme $A[2^n]$ admits a filtration

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

with G_1 diagonalizable, $A[2^n]/G_2$ étale and G_2/G_1 isomorphic to a product of group schemes isomorphic to G_π and $G_{\overline{\pi}}$. Since G_2/G_1 is annihilated by 2 and since the group structure of $A[2^n](\overline{F})$ is $(\mathbf{Z}/2^n\mathbf{Z})^{2g}$, the order of G_2/G_1 is at most 2^{2g}. As in the proof of Theorem 2.1, we note that the abelian varieties A/G_2 and $A^{\text{dual}}/G_1^\vee$ are all isogenous to A. Therefore they all have the same number of points modulo a prime ideal of O_F as A itself. It follows that the orders of the group schemes G_1 and $A[2^n]/G_2$ are bounded independently of n. This implies that the order of $A[2^n]$ remains bounded as $n \to \infty$, but this is impossible unless $A = 0$ as required.

5. The case f = 11

In this section we discuss the exceptional case $f = 11$. We study 2-group schemes over $\mathbf{Z}[\zeta_{11}]$. The main complication is the fact that Condition (A) of Theorem 2.1 is not satisfied: there exists a simple 2-group scheme E of order 4 over $\mathbf{Z}[\zeta_{11}]$. It is already defined over the subring $R = \mathbf{Z}[\alpha]$, where $\alpha = -\zeta_{11} - \zeta_{11}^3 - \zeta_{11}^4 - \zeta_{11}^5 - \zeta_{11}^9 = \frac{1+\sqrt{-11}}{2}$, and can be described in any of the three following ways.

- Let E_1 be the $\mathbf{F}_4$-vector space scheme [15, Ex.3.b] over $\widehat{R} = R \otimes \mathbf{Z}_2 \cong \mathbf{Z}_2[\zeta_3]$ with Hopf algebra $\widehat{R}[T]/(T^4 - 2T)$. Let E_2 be the $R[\frac{1}{2}]$-group scheme whose corresponding Galois module is a 2-dimensional $\mathbf{F}_2$-vector space on which $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-11}))$ acts irreducibly through the ray class group of $\mathbf{Q}(\sqrt{-11})$ of conductor 2. Since 2 is inert in $\mathbf{Q}(\sqrt{-11})$ this ray class group has order 3. Since the ray class field of conductor 2 of $\mathbf{Q}_2(\sqrt{-11}) = \mathbf{Q}_2(\zeta_3)$ is obtained by adjoining a cube root of 2, there is an isomorphism $\varphi : E_1(\overline{\mathbf{Q}}_2) \overset{\cong}{\longrightarrow} E_2(\overline{\mathbf{Q}}_2)$ of local Galois modules. The equivalence of categories of Prop.2.3 implies then that there exists a groupscheme E over R corresponding to the triple (E_1, E_2, φ). The group scheme E is self-dual, local-local over $\widehat{R}$ and admits an automorphism of order 3 that turns it into an $\mathbf{F}_4$-vector space scheme over R.
- Alternatively one can construct the group scheme E as the 2-torsion subgroup scheme of the Néron model $\mathcal{E}$ over R of the elliptic curve

  $$Y^2 + Y = X^3 - X^2 - 7X + 10.$$

  This is the curve 121D in the notation in the Antwerp Tables [4]. It is 121B in J. Cremona's Table [7]. The curve $\mathcal{E}$ admits complex multiplication by the ring R and its reduction type at the prime $\sqrt{-11}$ is I_0^*. The component group is of type 2×2.
- Finally, although not very useful, we can describe the group scheme E completely explicitly. Let $f(X) = X^3 - \alpha X^2 - \overline{\alpha} X + 1 \in R[X]$. Then $E = \mathrm{Spec}(R[X]/(g(X))$ where

  $$g(X) = Xf(X + \alpha) = X^4 + 2\alpha X^3 + (2\alpha - 4)X^2 - 2X.$$

  The group law is given by

  $$x + y + xy(6\overline{\alpha} - 14 + 5(\alpha - 4)(x + y) + 4\alpha(x^2 + y^2) + (16\alpha - 9)xy \\ +(\alpha + 9)(x^2y + xy^2) + 2\overline{\alpha}x^2y^2)$$

  and the automorphism of E given by

  $$x \mapsto (5 + \alpha)x + 3(1 + \overline{\alpha})x^2 - (1 + \alpha)x^3,$$

  is of order 3.

We fix some notation. Let $F = \mathbf{Q}(\zeta_{11})$ and $O_F = \mathbf{Z}[\zeta_{11}]$. We write $\widehat{O}_F$ for the completion of O_F at the unique prime over 2 and $\widehat{F}$ for its quotient field. Let K denote the ray class field of $\mathbf{Q}(\sqrt{-11})$ of conductor (2). We have that $K = \mathbf{Q}(\sqrt{-11}, \beta)$ where β is a zero of the polynomial f above: it satisfies $\beta^3 - \alpha\beta^2 - \overline{\alpha}\beta + 1 = 0$. Since $f(\alpha) = -\alpha\overline{\alpha} + 1 = -2$, the element $\pi = \alpha - \beta$ generates the unique prime of K over 2. We have that $(\pi)^3 = (2)$. The composite field $H = FK = \mathbf{Q}(\zeta_{11}, \beta)$ is the ray class field of conductor (2) of F.

Proposition 5.1. *(GRH) The only simple 2-power order group schemes over* $\mathbf{Z}[\zeta_{11}]$ *are* $\mathbf{Z}/2\mathbf{Z}$, μ_2 *and* E.

Proof. Let G be a simple 2-power order group scheme over $O_F = \mathbf{Z}[\zeta_{11}]$. Then $2 \cdot G = 0$. Let G' be the product of the Galois conjugates of G by the group scheme E and by the Katz-Mazur group schemes T_ε. Here ε runs through an $\mathbf{F}_2$-basis $\{-1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4\}$ of the unit group O_F^* modulo squares. Let L be the field obtained by adjoining the points of G' to F. By Fontaine's Theorem we have that $\delta_L < \delta_{\mathbf{Q}(\zeta_{11})} \cdot 4 = 11^{9/10} \cdot 4 = 34.619\ldots$. Odlyzko's discriminant bounds give (under GRH) that $[L : \mathbf{Q}] < 10000$. We have the following inclusions of fields.

$$\begin{tikzcd}
& K \arrow[r, phantom, "\underset{5}{\subset}"] & H \arrow[r, phantom, "\underset{2}{\subset}"] & H(i) \arrow[r, phantom, "\underset{2^4}{\subset}"] & K' \arrow[r, phantom, "\underset{\leq 10}{\subset}"] & L. \\
\mathbf{Q}(\sqrt{-11}) \arrow[ur, dash, "3"'] \arrow[r, phantom, "\overset{5}{\subset}"] & F \arrow[ur, dash, "3"'] \arrow[r, phantom, "\overset{2}{\subset}"] & F(i) \arrow[ur, dash, "3"'] & & &
\end{tikzcd}$$

Here $K' = F(i, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \sqrt{\varepsilon_3}, \sqrt{\varepsilon_4})$.

Claim. $\mathrm{Gal}(L/H)$ is a 2-group.

To prove this we put $\Gamma = \mathrm{Gal}(L/\mathbf{Q}(\sqrt{-11}))$. The subfield $H(i) = \mathbf{Q}(\zeta_{11}, i, \beta)$ is an abelian extension of $\mathbf{Q}(\sqrt{-11})$. By class field theory any larger abelian extension inside L would have conductor at least (8) and hence root discriminant at least $2^{13/6} \cdot 11^{9/10}$, contradicting Fontaine's bound. Therefore $H(i)$ is the largest abelian extension of $\mathbf{Q}(\sqrt{-11})$ inside L and the commutator subgroup of Γ is equal to $\Gamma' = \mathrm{Gal}(L/H(i))$.

The root discriminant of $H(i)$ is equal to $11^{9/10} 2^{4/3} = 21.809\ldots$ and Odlyzko's bounds imply that the degree of its Hilbert class field is at most 170. This implies that the class number of $H(i)$ is at most 2. There is only one prime over 2 in $H(i)$. Its residue field is $\mathbf{F}_{2^{10}}$ and the multiplicative group of this field is generated by the units ζ_{11}, $1 - \zeta_{44}$ and β. We briefly explain why. The group $\#\mathbf{F}_{1024}^*$ has order $3 \cdot 11 \cdot 31$. Clearly ζ_{11} has order 11. Since $f(1) = 1$, we have that $\beta \not\equiv 1 \pmod 2$. Since the image of β is contained in the subfield $\mathbf{F}_{2^2}$, it has order 3. Finally, the image of the unit $(1 - \zeta_{44})^{33}$ is congruent to the norm of $1 - \zeta_{11} \in \mathbf{F}_{2^{10}}$ to the subfield $\mathbf{F}_{2^5}$, which is $(1 - \zeta_{11})(1 - \zeta_{11}^{-1}) \neq 1$. Therefore it has order 31. It follows, by class field theory, that $H(i)$ does not admit any odd degree abelian extensions that are unramified outside 2. This implies that Γ'/Γ'' is a 2-group.

Since K' is abelian over $H(i)$, we have that $[\Gamma' : \Gamma''] \geq 16$ and hence $\#\Gamma'' \leq 10$. Cor.3.2 implies therefore that either Γ'' is a 2-group in which case the claim follows, or Γ'' has order 9. To exclude the second possibiliy, we observe that K' is the fixed field of Γ'', so that the Galois group $\Upsilon = \mathrm{Gal}(K'/K(i))$ acts on Γ'' by conjugation. The group Υ has order 80. It is isomorphic to the semi-direct product of $\mathbf{Z}/5\mathbf{Z}$ by $\mathbf{F}_2^4$, the group $(\mathbf{Z}/5\mathbf{Z})$ acting non-trivially on $\mathbf{F}_2^4$. Since the order of $\mathrm{Aut}(\Gamma'')$ is not divisible by 5, all elements in Υ of order 5 are contained in the kernel of the natural map $\Upsilon \longrightarrow \mathrm{Aut}(\Gamma'')$. Therefore Υ, being generated by its 5-Sylow subgroups, acts trivially on Γ''. Since the orders of Υ and Γ'' are coprime, this implies that there is an extension $K(i) \subset L' \subset L$ with $\mathrm{Gal}(L'/K(i))$ abelian of order 9, that is unramified outside the unique prime over 2. Since the root discriminant of $K(i)$ is $11^{1/2}2^{4/3} = 8.35\ldots$, Odlyzko's bounds imply that the class number of $K(i)$ is 1. Since there lies only one prime over 2 in $K(i)$ and since the multiplicative group of its residue field has order 3, the field L' cannot exist by class field theory.

This proves that Γ'' and hence $\mathrm{Gal}(L/H)$ are 2-groups and the claim follows.

Since the group scheme G is simple, its points $G(\overline{F})$ are fixed by the 2-group $\mathrm{Gal}(L/H)$ and the absolute Galois group of F acts on $G(\overline{F})$ via the group $\Delta = \mathrm{Gal}(H/F)$, which is of order 3. Since irreducible $\mathbf{F}_2[\Delta]$-modules are of order 2 or order 4, we conclude that G has order 2 or order 4. If the order of G is 2, it follows from [20, Thm.3] that $G \cong \mathbf{Z}/2\mathbf{Z}$ or $G \cong \mu_2$. Here we use the fact that the class number of F is 1 and that 2 is a primitive root modulo 11.

If the order of G is 4, the group Δ acts non-trivially on $G(\overline{F})$ and therefore the points of G and E constitute isomorphic Galois modules. In other words, there is an isomorphism $\varphi : G \xrightarrow{\cong} E$ over the ring $O_F[\frac{1}{2}]$. Since E is local-local at 2, we conclude from Raynaud's paper [15, 3.3.5] that there is an isomorphism $\varphi' : G \xrightarrow{\cong} E$ over $\widehat{O}_F$ as well. By composing the isomorphism φ with an automorphism of E, we can ensure that the isomorphisms φ, φ' agree over $\widehat{F}$. Therefore the equivalence of categories of Prop.2.3 implies that the group schemes E and G are isomorphic over O_F. This proves the Proposition.

Next we prove a substitute for Prop.2.6. Note that we do not assume GRH here.

Proposition 5.2. *Over $O_F = \mathbf{Z}[\zeta_{11}]$ we have the following*

(i) Every extension of a constant 2-group scheme by a constant 2-group scheme is constant. Every extension of a diagonalizable 2-group scheme by a diagonalizable 2-group scheme is diagonalizable.

(ii)

$$\mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Ext}^1_{O_F}(E, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Ext}^1_{O_F}(\mu_2, E) = 0.$$

(iii) Any extension of E by itself splits.

Proof. Since the class number of F is 1, part *(i)* follows from Prop.2.6 *(i)*. The fact that $\mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z}) = 0$ follows from Prop.2.6*(ii)*. To prove the other two statements of part *(ii)*, consider an extension of E by $\mathbf{Z}/2\mathbf{Z}$:

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow E \longrightarrow 0.$$

Since over the ring $\widehat{O}_F$, the group scheme E is local while $\mathbf{Z}/2\mathbf{Z}$ is étale, the connected component splits the sequence. This implies that G is killed by 2.

Moreover, the field extension obtained by adjoining the points of G to F is unramified and therefore trivial. We conclude that G is locally and generically split. Since there is only one prime over 2 and since $\mathrm{Hom}_{\widehat{F}}(E, \mathbf{Z}/2\mathbf{Z}) = 0$, it follows from the Mayer-Vietoris sequence of Cor.2.3 that G is actually split over O_F. The fact that $\mathrm{Ext}^1_{O_F}(\mu_2, E) = 0$ follows by duality. This proves *(ii)*.

The proof of part *(iii)* takes up the rest of the paper. It involves a calculation with Honda systems that we give in section 6. We first consider extensions of E by itself over the ring $\widehat{O}_F$. The elliptic curve $\mathcal{E}$ given by $Y^2+Y = X^3$ is supersingular in characteristic 2. Its 2-torsion points generate the extension $\widehat{F}(\sqrt[3]{2})$ of $\widehat{F}$. This field is equal to $\widehat{H} = \widehat{F}(\beta)$, the completion of H at the unique prime over 2. It follows that the Galois modules associated to $\mathcal{E}[2]$ and E are isomorphic. By [15, 3.3.5] the two local-local group schemes $\mathcal{E}[2]$ and E are isomorphic over $\widehat{O}_F$. For each of the three automorphism τ of $\mathcal{E}$, there is an extension $\mathcal{E}[4]_\tau$ of E by E given by

$$\begin{tikzcd} 0 \arrow[r] & \mathcal{E}[2] \arrow[r] & \mathcal{E}[4] \arrow[r, "\tau\cdot[2]"] & \mathcal{E}[2] \arrow[r] & 0 \end{tikzcd}$$

Here $[m] : \mathcal{E} \longrightarrow \mathcal{E}$ denotes the multiplication by m morphism and $\mathcal{E}[m]$ is its the kernel. The extensions $\mathcal{E}[4]_\tau$ are non-trivial and pairwise non-equivalent as extensions of abelian groups.

For later reference we remark that the X-coordinates of the 4-torsion points of the elliptic curve $\mathcal{E}$ are zeroes of the polynomial $2X^6 + 10X^3 - 1$. It follows that the 4-torsion points generate the bi-quadratic extension $\widehat{H}(\sqrt{-1}, \sqrt[4]{-3})$ of $\widehat{H}$. The three quadratic characters have conductor π^4 over $\widehat{H}$.

Claim 1. The group $\mathrm{Ext}^1_{\widehat{O}_F}(E, E)$ is generated by the extensions that are killed by 2 and by the extensions $\mathcal{E}[4]_\tau$.

Let $\Gamma = \mathrm{Gal}(\overline{\mathbf{Q}}_2/\widehat{F})$. From the spectral sequence $H^p(\Gamma, \mathrm{Ext}^q_{\mathrm{ab}}(E, E)) \Longrightarrow \mathrm{Ext}^{p+q}_{\widehat{F}}(E, E)$ we deduce the following commutative diagram with exact rows

$$\begin{tikzcd} 0 \arrow[r] & \mathrm{Ext}^1_{\widehat{O}_F,2}(E, E) \arrow[r] \arrow[d] & \mathrm{Ext}^1_{\widehat{O}_F}(E, E) \arrow[r] \arrow[d] & \mathrm{cok} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathrm{Ext}^1_{\widehat{F},2}(E, E) \arrow[r] & \mathrm{Ext}^1_{\widehat{F}}(E, E) \arrow[r] & \mathrm{Ext}^1_{\mathrm{ab}}(E, E)^\Gamma & \end{tikzcd}$$

Here the index ‘2’ means ‘annihilated by 2’. Any extension G of E by E over $\widehat{O}_F$ that is killed by 2 over $\widehat{F}$, is itself killed by 2. Therefore the left hand square is Cartesian and the rightmost vertical arrow is injective. Since the Γ-modules $\mathrm{Ext}^1_{\mathrm{ab}}(E, E)$ and $\mathrm{Hom}_{\mathrm{ab}}(E, E)$ are dual to one another, the order of $\mathrm{Ext}^1_{\mathrm{ab}}(E, E)^\Gamma$ is equal to $\#\mathrm{Hom}_{\mathrm{ab}}(E, E)^\Gamma = 4$. It follows that the index of $\mathrm{Ext}^1_{\widehat{O}_F,2}(E, E)$ in $\mathrm{Ext}^1_{\widehat{O}_F}(E, E)$ is at most 4. Since the images of the extensions $\mathcal{E}[4]_\tau$ are all distinct in $\mathrm{Ext}^1_{\mathrm{ab}}(E, E)$, the claim follows.

Claim 2. The points of E generate the cyclic cubic extension $H = F(\beta)$ of F. The points of an extension G of E by E over O_F generate a field extension of H that is a composite of quadratic extensions of conductor at most π^4.

Only the statement about the conductors needs proof. This is a local question. Recall that $\widehat{H} = \widehat{F}(\beta)$ is the quotient field of $\widehat{O}_H$, the completion of O_H at $\pi = \alpha - \beta$, the unique prime over 2. If G is locally one of the extensions $\mathcal{E}[4]_\tau$, we are done, because in that case its points are either rational or generate the bi-quadratic extension $\widehat{H}(\sqrt{-1}, \sqrt[4]{-3})$ of $\widehat{H}$ of conductor π^4.

On the other hand, if G is an extension of E by E over $\widehat{O}_F$ that is killed by 2, we apply the results of the calculation of section 6. Proposition 6.4 says that the points of G lying over a non-zero point a of E generate a Galois extension of $\widehat{H}$ of degree 4, exponent 2 and relative discriminant 4. Therefore all characters of this extension have conductor dividing π^2.

An arbitrary extension G of E by E is the sum in $\mathrm{Ext}^1_{\widehat{O}_F}(E, E)$ of these two types of extensions. Since $G(\overline{F})$ is a subquotient of the product of the groups of points of its summands, the characters of the field extension of $\widehat{H}$ generated by the points of G have conductor at most π^4. This implies Claim 2.

Claim 3. (i) The ray class field of H of conductor π^3 is equal to H itself.
(ii) The ray class field of H of conductor π^4 is the field $K' = H(i, \sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \sqrt{\varepsilon_3}, \sqrt{\varepsilon_4})$.

Proof. The root discriminant of H is equal to $2^{2/3}11^{9/10} = 15.715\ldots$ and Odlyzko's discriminant bounds imply that the degree of the Hilbert class field is at most 56. Since $[H : \mathbf{Q}] = 30$, this implies that the class number of H is 1. We saw in the proof of Prop. 5.1 that the units ζ_{11}, $1 - \zeta_{44}$ and β generate the multiplicative group of the residue field $\mathbf{F}_{2^{10}}$ of the unique prime over 2. This implies that the ray class field of H of conductor π is equal to H. Therefore the ray class group of conductor π^2 is isomorphic to $V = (1 + (\pi))/(1 + (\pi^2))$ modulo global units. The Galois group $\mathrm{Gal}(H/\mathbf{Q})$ is a semi-direct product of $\mathrm{Gal}(H/F) \cong \mathbf{F}_4^*$ by $\mathrm{Gal}(F/\mathbf{Q}) \cong \mathrm{Gal}(\mathbf{F}_{2^{10}}/\mathbf{F}_2)$. Since (π) is the unique prime over 2, it acts on $V \cong \mathbf{F}_{2^{10}}$ and it does so in the obvious way. We have that $V = V_1 \times V_2$, where V_1 is the submodule of V of the fixed points of the order 5 subgroup $\mathrm{Gal}(H/K)$ and $V_2 \subset \mathbf{F}_{2^{10}}$ is the kernel of the trace map to the subfield $\mathbf{F}_{2^2}$. The $\mathrm{Gal}(H/\mathbf{Q})$-modules V_1 and V_2 are irreducible of order 4 and 4^4 respectively. Since the unit $\beta \in K$ has the property that $\beta^3 \not\equiv 1 \pmod{\pi^2}$, its cube generates V_1. Finally, we observe that the image of the unit $u = (\zeta_{11} - \beta)^{2^{10}-1}$ in V is not $\mathrm{Gal}(H/K)$-invariant, since

$$\begin{aligned} u = (\zeta_{11} - \alpha + \pi)^{2^{10}-1} &\equiv (\zeta_{11} - \alpha)^{2^{10}-1} + (2^{10} - 1)(\zeta_{11} - \alpha)^{2^{10}-2}\pi \pmod{\pi^2}, \\ &\equiv 1 + \frac{\pi}{\zeta_{11} - \alpha} \pmod{\pi^2}, \end{aligned}$$

so that $\sigma(u)/u \not\equiv 1 \pmod{\pi^2}$ for any generator σ of $\mathrm{Gal}(H/K)$. Therefore the Galois module generated by β^3 and u inside V is strictly larger than V_1. It follows that u and β^3 generate V and hence that the ray class group of conductor π^2 of H is trivial.

The ray class group of H of conductor π^3 is isomorphic to $W = (1 + (\pi))/(1 + (\pi^3))$ modulo global units that are congruent to 1 (mod π). Since W/W^2 is isomorphic to $V = (1 + (\pi))/(1 + (\pi^2))$ and since the ray class group of H of conductor π^2 is trivial, the ray class group of conductor π^3 is also trivial. This proves the first statement.

Since the field K' has conductor at most π^4 over H, the ray class field of conductor π^4 has degree at least 2^5. On the other hand, $-1 \equiv 1 + 2 \pmod 4$ and the $(2^{10} - 1)$-th powers of the cyclotomic units $(\zeta_{11}^a - 1)/(\zeta_{11} - 1)$ are congruent to

$$\begin{aligned}\left(\frac{\zeta_{11}^{a\cdot 2^9} - 1}{\zeta_{11}^{2^9} - 1}\right)^2 \frac{\zeta_{11} - 1}{\zeta_{11}^a - 1} &\equiv \frac{\zeta_{11}^{a/2} - 1}{\zeta_{11}^{1/2} - 1} \cdot \frac{\zeta_{11}^{1/2} + 1}{\zeta_{11}^{a/2} + 1}\\ &\equiv 1 + 2\left(\frac{1}{\zeta_{11}^{1/2} - 1} - \frac{1}{\zeta_{11}^{a/2} + 1}\right) \pmod 4.\end{aligned}$$

Therefore the ray class group of conductor π^4 is isomorphic to the quotient of the additive group $\mathbf{F}_{2^{10}}$ modulo by the subgroup generated by 1 and by the elements $\frac{1}{\zeta_{11}^{1/2}-1} - \frac{1}{\zeta_{11}^{a/2}+1}$ for $a \in (\mathbf{Z}/11\mathbf{Z})^*$. This group has order 2^5.

The claim now follows from class field theory.

End of proof. By Claims 2 and 3, the points of any extension G of E by E over O_F generate an extension L of H contained in the ray class field K'. Therefore the natural action of the Galois group $\Delta = \mathrm{Gal}(H/F)$ of order 3 on $\mathrm{Gal}(L/H)$ is trivial. Locally, in the group $\mathrm{Ext}^1_{\widehat{O}_F}(E, E)$, the extension G is equivalent to a sum $[\mathcal{E}[4]_\tau] + [\tilde{G}]$. Here $\tilde{G}$ is an extension that is killed by 2 and τ is either an automorphism of order 3 of the elliptic curve $\mathcal{E}$, in which case $\mathcal{E}[4]_\tau$ is the extension of E by E introduced above, or $\tau = 0$ in which case $\mathcal{E}[4]_\tau$ denotes the split extension. Let $\widehat{L}$, $\widehat{L}'$ and $\widehat{L}''$ denote the extensions of $\widehat{H}$ generated by the points of G, $\mathcal{E}[4]$ and $\tilde{G}$ respectively. Each of $\widehat{L}$, $\widehat{L}'$ and $\widehat{L}''$ is contained in the composite of the other two.

If $\tau \neq 0$, the field $\widehat{L}'$ is the totally ramified quartic extension $\widehat{H}(i, \sqrt[4]{-3})$ of $\widehat{H}$. This is a Galois extension of $\mathbf{Q}_2(\sqrt{-3})$. The natural action of the group $\mathrm{Gal}(\widehat{H}/\widehat{F})$ on the Galois group $\mathrm{Gal}(\widehat{L}'/\widehat{H})$ is trivial. Since the global Galois group $\Delta = \mathrm{Gal}(H/F)$ acts trivially on $\mathrm{Gal}(L/H)$, the local Galois group $\mathrm{Gal}(\widehat{H}/\widehat{F})$ acts trivially on $\mathrm{Gal}(\widehat{L}/\widehat{H})$. Since $\widehat{L}'' \subset \widehat{L}'\widehat{L}$, the group $\Delta \cong \mathrm{Gal}(\widehat{H}/\widehat{F})$ also acts trivially on $\mathrm{Gal}(\widehat{L}''/\widehat{H})$.

On the other hand, since $\tilde{G}$ is killed by 2, the extension $\widehat{L}''$ has conductor at most π^2 over $\widehat{H}$. This follows from Prop.6.4 of the next section. Since $\widehat{H}$ is tame over $\widehat{F}$, any generator σ of Δ has the property that $\sigma(\pi)/\pi$ is congruent to a non-trivial cube root of unity modulo π. It follows that Δ acts without fixed points on the group $(1+(\pi))/(1+(\pi^2))$. By class field theory, $\widehat{L}''$ is therefore actually an *unramified* extension of $\widehat{H}$. This implies that the order 5 Galois group of $\widehat{H}$ over $\widehat{K}=\mathbf{Q}_2(\beta)$ acts trivially on $\mathrm{Gal}(\widehat{L}''/\widehat{H})$. Since $\mathrm{Gal}(\widehat{H}/\widehat{K})$ also acts trivially on $\mathrm{Gal}(\widehat{L}'/\widehat{H})$ and since $\widehat{L}\subset\widehat{L}'\widehat{L}''$, we deduce that $\mathrm{Gal}(\widehat{H}/\widehat{K})$ acts trivially on $\mathrm{Gal}(\widehat{L}/\widehat{H})$ as well. Since L is totally ramified over F, this implies that the global Galois group $\Delta=\mathrm{Gal}(H/K)$ acts trivially on $\mathrm{Gal}(L/H)$. It follows that $L\subset H(i)$ and hence locally that $\widehat{L}\subset\widehat{H}(i)$. Since $\widehat{L}'\subset\widehat{L}\widehat{L}''$, it follows that the ramification index of $\widehat{L}'$ over $\widehat{H}$ is at most 2. A contradiction.

It follows that $\tau=0$ and hence that G is killed by 2. By Prop.6.4 and the fact that the ray class field of H of conductor π^2 is equal to H itself, the action of $\mathrm{Gal}(L/H)$ on its points is trivial. In other words, G is generically trivial. Since G is local-local, it is by Raynaud [15, 3.3.5] locally determined by its Galois module. This implies that G is also locally trivial. Since there is only one prime lying over 2, it follows from the Mayer-Vietoris sequence in Cor.2.4 that the extension G is trivial over O_F.

This proves the Proposition.

Theorem 5.3. *(GRH) There are no non-zero abelian varieties over* $\mathbf{Q}(\zeta_{11})$ *with good reduction everywhere.*

Proof. Let A be the Néron model of an abelian variety of dimension g with good reduction everywhere. The same arguments as in the proof of Cor.4.3 show that Prop.5.1 and Prop.5.2 imply that the group scheme $A[2^n]$ admits a filtration over $\mathbf{Z}[\zeta_{11}]$ with closed flat subgroup schemes

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

with G_1 diagonalizable, G_2/G_1 a product of group schemes isomorphic to E and $A[2^n]/G_2$ constant. By Prop.5.2 *(iii)*, the group $G_2/G_1(\overline{F})$ is annihilated by 2. Therefore the order of $G_2/G_1(\overline{F})$ is at most 2^{2g}. We reduce the abelian varieties A/G_2 and $A^{\mathrm{dual}}/G_1^\vee$ modulo a prime $\mathfrak{q}$ of $\mathbf{Z}[\zeta_{11}]$. Since they are both isogenous to A, they have as many points as A modulo $\mathfrak{q}$. It follows that the orders of G_1 and $A[2^n]/G_2$ are bounded independently of n. This implies that the order of $A[2^n]$ remains bounded as $n\to\infty$. This is impossible unless $A=0$ as required.

6. A local group scheme of order p^4

In this section we do a local computation with Honda systems. The main result, Proposition 6.3, is used in section 5. See [8,9] and especially [6, Ch.1] for Honda systems.

Let p be a prime and let k be a finite field of characteristic p. Let W denote the ring of Witt vectors over k and let K be the quotient field of W. Let $\sigma : W \longrightarrow W$ denote the Frobenius automorphism of W. It is determined by the fact that $\sigma(x) \equiv x^p \pmod{p}$ for all $x \in W$. The Dieudonné ring $D_k = W[F, V]$ is the ring generated by *Frobenius* F and *Verschiebung* V. We have that $FV = VF = p$ and that $Fa = \sigma(a)F$ and $Va = \sigma^{-1}(a)V$ for all $a \in W$. If $k \neq \mathbf{F}_p$, the ring D_k is not commutative. Let CW_k denotes the group functor of *Witt covectors* and let $\widehat{CW}_k$ be the associated formal k-group scheme [6,9]. For any k-algebra R, the group $CW_k(R)$ admits a unique D_k-module structure for which the Teichmüller lift $[x]$ of $x \in k$ acts as $[x]\mathbf{a} = (\ldots, x^{p^{-n}}a_{-n}, \ldots, x^{p^{-1}}a_{-1}, xa_0)$ and for which $F\mathbf{a} = (\ldots, a_{-n}^p, \ldots, a_{-1}^p, a_0^p)$ and $V\mathbf{a} = (\ldots, a_{-n-1}, \ldots, a_{-2}, a_{-1})$. Note that this implies that $p\mathbf{a} = (\ldots, a_{-n-1}^p, \ldots, a_{-2}^p, a_{-1}^p)$. We also recall the definition of the Hasse-Witt exponential. Let $\overline{W}$ denote the ring of integers of $\overline{K}$. Then $\exp : \widehat{CW}_k(\overline{W}/p\overline{W}) \longrightarrow \overline{K}/p\overline{W}$ is the group homomorphism given by

$$\exp(\ldots, a_{-n}, \ldots, a_{-1}, a_0) = \sum_{n\geq 0} p^{-n}\tilde{a}_{-n}^{p^n},$$

where $\tilde{a}_{-n}$ is any lift of a_{-n} to $\overline{W}$.

A *local-local* group scheme over W is a finite flat local commutative group scheme whose Cartier dual is also local. There are no such group schemes over W of order p. In this section we study local-local group schemes E over W of order p^2. Using the theory of Honda systems we determine the extensions of the group schemes E by themselves that are killed by p. For $p = 2$, this computation is an essential ingredient in the proof of Theorem 5.3.

Proposition 6.1. *Let E be a local-local group scheme over W of order p^2. Then*

(i) E is killed by p. The corresponding Honda system (M, L) is given by $M = k\mathbf{e}_1 \oplus k\mathbf{e}_2$ and $L = k\mathbf{e}_1$ with Frobenius and Verschiebung morphisms F and V given by

$$V = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad F = \begin{pmatrix} 0 & 0 \\ \lambda & 0 \end{pmatrix},$$

for some $\lambda \in k^*$. The isomorphism class of (M, L) only depends on the image of λ in k^* modulo $(k^*)^{\sigma^2-1} = (k^*)^{p^2-1}$.

(ii) The points of E form the Galois module $\{a \in \overline{W}/p\overline{W} : a^{p^2} + p\tilde{\lambda}^p a \equiv 0 \pmod{p^2}\}$ with addition law $a + a' + \lambda^{-p}\Phi(a^p, a'^p)$. Here $\Phi(x, y)$ denotes the Witt polynomial $((x + y)^p - x^p - y^p)/p$. The points generate the field $K(\zeta_{p+1}, \sqrt[p^2-1]{p\tilde{\lambda}^p})$, which is a totally ramified extension of degree $p^2 - 1$ over $K(\zeta_{p+1})$. Here $\tilde{\lambda}$ denotes a lift of λ to $\overline{W}$.

Proof. (i) If E is not killed by p, then the same is true for M, so that $M = W/p^2W$. Since E is local-local, both F and V are nilpotent [6, Def.2.1]. Therefore $pM \subset \ker V$. Since V is injective when restricted to L, we must have that

$L = 0$. Since the natural map $L/pL \longrightarrow M/FM$ an isomorphism. This implies that F is surjective, a contradiction.

Therefore M is killed by p and is a module over $D_k/pD_k = k[F, V]$. It can be equipped with a k-basis so that $M = k\mathbf{e}_1 \oplus k\mathbf{e}_2$, $L = k\mathbf{e}_1$, the Verschiebung operator V satisfies $V\mathbf{e}_1 = \mathbf{e}_2$ and $V\mathbf{e}_2 = 0$. This implies that the Frobenius operator F kills $\mathbf{e}_2$. On the other hand $F\mathbf{e}_1 = \lambda\mathbf{e}_2$ for some $\lambda \in k^*$. Replacing the basis vactors $\mathbf{e}_1$, $\mathbf{e}_2$ by $t^p\mathbf{e}_1$ and $t\mathbf{e}_2$ respectively, preserves all relations, but replaces λ by λt^{1-p^2}. This proves *(i)*.

(ii) The action of $\mathrm{Gal}(\overline{K}/K)$ on the points of the group scheme E is induced by its action on $\mathrm{Hom}_{D_k}(M, \widehat{CW}_k(\overline{W}/p\overline{W}))$. Since $V\mathbf{e}_1 = \mathbf{e}_2$, any D_k-homomorphism φ from M to $\widehat{CW}_k(\overline{W}/p\overline{W})$ is determined by $\varphi(\mathbf{e}_1)$. Since $V^2\mathbf{e}_1 = 0$ and $F\mathbf{e}_1 = \lambda\mathbf{e}_2 = \lambda V\mathbf{e}_1$, we have that

$$\varphi(\mathbf{e}_1) = (\ldots,\quad 0,\quad 0,\quad \tfrac{a^p}{\lambda},\quad a)$$

for a certain $a \in \overline{W}/p\overline{W}$ satisfying $a^{p^2} = 0$. The Galois module $E(\overline{K})$ is isomorphic to the subgroup of homomorphisms φ that map L to the kernel of the Hasse-Witt exponential. These correspond precisely to the Witt covectors $(\ldots,\ 0,\ 0,\ \tfrac{a^p}{\lambda},\ a)$ for which $a^{p^2} + p\lambda^p a \equiv 0 \pmod{p^2}$. This proves the Proposition.

The group schemes E are $\mathbf{F}_{p^2}$-vector space schemes in the sense of Raynaud [15]. The different values for λ correspond to unramified twists. The p-torsion points of supersingular elliptic curves curves over W are group schemes of this type.

From now on we fix $\lambda \in k^*$. The next theorem describes the extensions of E by itself that are killed by p in terms of Honda systems.

Proposition 6.2. *Any extension*

$$0 \longrightarrow E \longrightarrow G \longrightarrow E \longrightarrow 0$$

of p-group schemes over W that is killed by p corresponds to an extension of Honda systems

$$0 \longleftarrow \quad (M, L) \quad \xleftarrow{f} \quad (\mathcal{M}, \mathcal{L}) \quad \xleftarrow{g} \quad (M, L) \quad \longleftarrow 0$$

where $\mathcal{M} = k\mathbf{e}_1 \times k\mathbf{e}_2 \times k\mathbf{e}'_1 \times k\mathbf{e}'_2$ and $\mathcal{L} = k\mathbf{e}_1 \oplus k\mathbf{e}_2$ and $f(x_1, x_2, x'_1, x'_2) = (x_2, x'_2)$ and $g(x_1, x_2) = (x_1, 0, x_2, 0)$ respectively and with Frobenius and Verschiebung morphisms F and V of the Honda system $(\mathcal{M}, \mathcal{L})$ given by

$$F = \begin{pmatrix} 0 & -\lambda\beta^p & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \lambda & \lambda\delta & 0 & 0 \\ 0 & \lambda & 0 & 0 \end{pmatrix}, \qquad V = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & \beta \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

for some $\beta, \delta \in k$. Two extensions G and G′ are isomorphic if and only if $(\beta, \delta) = (\beta', \delta')$ in the additive group $k \times (k/(\sigma^2 - 1)k)$.

Proof. Since G is killed by p, the underlying D_k-module of the Honda system $(\mathcal{M}, \mathcal{L})$ is a vector space of dimension 4 over k. We choose a basis $\{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}'_1, \mathbf{e}'_2\}$ for M as follows: the vectors $\mathbf{e}_1$ and $\mathbf{e}'_1$ are the basis vectors for the Honda submodule (M, L) asociated to the quotient group scheme E of G. In other words, $L = k\mathbf{e}_1$ and $\mathbf{e}'_1 = V\mathbf{e}_1$. We lift a generator for the submodule L of the quotient Honda system (M, L) corresponding to the subgroup scheme E to M and call it $\mathbf{e}_2$. Finally we let $\mathbf{e}'_2 = V\mathbf{e}_2$. In this way $L = k\mathbf{e}_1 \oplus k\mathbf{e}_2$. The choice of the vector $\mathbf{e}_2$ is unique up to vectors in $k\mathbf{e}_1$. Then

$$\begin{aligned} V\mathbf{e}'_1 &= 0, \\ F\mathbf{e}_1 &= \lambda\mathbf{e}'_1, \\ V\mathbf{e}'_2 &= \alpha\mathbf{e}_1 + \beta\mathbf{e}'_1, \\ F\mathbf{e}_2 &= \lambda\mathbf{e}'_2 + \gamma\mathbf{e}_1 + \delta\mathbf{e}'_1, \end{aligned}$$

for certain $\alpha, \beta, \gamma, \delta \in k$. From the fact that $FV\mathbf{e}'_2 = 0$ and $VF\mathbf{e}_2 = 0$ we deduce that $\alpha = 0$ and that $\lambda\beta^p + \gamma = 0$ respectively. It is convenient to replace δ by δ/λ. This gives the formulas

$$\begin{aligned} V\mathbf{e}'_2 &= \beta\mathbf{e}'_1, \\ F\mathbf{e}_2 &= \lambda\mathbf{e}'_2 - \lambda\beta^p\mathbf{e}_1 + \lambda\delta\mathbf{e}'_1 \end{aligned}$$

for certain $\beta, \delta \in k$. Finally we investigate the ambiguity in the choice of the basis vector $\mathbf{e}_2$. Replacing $\mathbf{e}_2$ by $\mathbf{e}_2 + r^p\mathbf{e}_1$ and $\mathbf{e}'_2$ by $\mathbf{e}'_2 + r\mathbf{e}'_1$ for any $r \in k$, preserves all relations, except that it replaces δ by $\delta + r^{p^2} - r$. Therefore only the image of $\delta \in k/(\sigma^2 - 1)k$ is determined by the extension class of G. It is not difficult to see that for every $\beta \in k$ and $\delta \in k/(\sigma^2 - 1)k$, there is a unique extension class G.

This proves the proposition.

Next we investigate the Galois modules $G(\overline{K})$. We fix a lift $\tilde{\lambda} \in \overline{W}$ of λ. By Prop.6.1 *(ii)* we may identify the elements of the Galois module $E(\overline{K})$ with the set $\{a \in \overline{W}/p\overline{W} : a^{p^2} + p\tilde{\lambda}^p a \equiv 0 \pmod{p^2}\}$.

Proposition 6.3. *Let G be an extension of E by E with parameters β and δ as in the previous proposition. For every zero $a \in \overline{W}$ of the polynomial $X^{p^2} + p\tilde{\lambda}^p X$, the field K'_a generated by the points of G that map to the point a $\pmod{p\overline{W}}$ in $E(K')$ is a Galois extension of K' of degree dividing p^2. It is generated by the zeroes of the polynomial*

$$f(X) = \left(X^p + \tilde{\lambda}\tilde{\beta}^p a - \tilde{\delta}a^p\right)^p + \tilde{\lambda}^p pX - \tilde{\lambda}^p\tilde{\beta}^{p^2} a^p p^{p-1} \in K_a[X].$$

Here $\tilde{\beta}$ and $\tilde{\delta}$ denote fixed lifts to W of β and δ respectively. Moreover, the zeroes of the polynomial $f(X)$ are distinct modulo p.

Proof. Since the points of G that map to a are a coset of the subgroup formed by the points of the subgroup scheme E, the field K'_a contains K'. Moreover, K'_a is a Galois extension of K' and for any point $g \in G$ mapping to a, the map $\mathrm{Gal}(K'_a/K') \longrightarrow E(\overline{K})$ given by $\sigma \mapsto \sigma(g) - g$ is an injective homomorphism. This shows that $\mathrm{Gal}(K'_a/K')$ is a group of order dividing p^2.

We study the D_k-morphisms from $\mathcal{M}$ to $\widehat{CW}_k(\overline{W}/p\overline{W})$, that map the submodule $\mathcal{L}$ into the kernel of the Hasse-Witt exponential. These morphisms form a $\mathrm{Gal}(\overline{K}/K)$-module isomorphic to $G(\overline{K})$.

Since $V\mathbf{e}_1 = \mathbf{e}'_1$ and $V\mathbf{e}_2 = \mathbf{e}'_2$, any such morphism φ is determined by the images of $\mathbf{e}_1$ and $\mathbf{e}_2$. Since $V\mathbf{e}'_1 = 0$, we have that $V^2\mathbf{e}_1 = 0$ and $V^3\mathbf{e}_2 = V^2\mathbf{e}'_2 = V\beta\mathbf{e}'_1 = 0$. This implies that

$$\begin{aligned}\varphi(\mathbf{e}_1) &= (\ldots,\quad 0,\quad 0,\quad 0,\quad b,\quad a\,),\\ \varphi(\mathbf{e}_2) &= (\ldots,\quad 0,\quad 0,\quad c',\quad b',\quad a'\,),\end{aligned}$$

for certain $a, b, a', b', c' \in k$. The facts that $VF\mathbf{e}_1 = VF\mathbf{e}_2 = VF\mathbf{e}'_1 = VF\mathbf{e}'_2 = 0$, that $F\mathbf{e}_1 = \lambda\mathbf{e}'_1 = \lambda V\mathbf{e}_1$ and that $V^2\mathbf{e}_2 = V\mathbf{e}'_2 = \beta\mathbf{e}'_1 = \beta V\mathbf{e}_1$ give rise to the following five relations

$$b^p = 0, \quad b'^p = 0, \quad c'^p = 0, \quad a^p = \lambda b, \quad c' = \beta b.$$

Finally, we have the relation

$$\begin{aligned}F\mathbf{e}_2 &= \lambda\mathbf{e}'_2 - \lambda\beta^p\mathbf{e}_1 + \lambda\delta\mathbf{e}'_1\\ &= \lambda V\mathbf{e}_2 - \lambda\beta^p\mathbf{e}_1 + \lambda\delta V\mathbf{e}_1.\end{aligned}$$

Since $b'^p = c'^p = 0$, we have that $F\varphi(\mathbf{e}_2) = (\ldots,\quad 0,\quad 0,\quad a'^p\,)$. On the other hand, $F\varphi(\mathbf{e}_2) = \varphi(F\mathbf{e}_2)$ is equal to the following sum of Witt covectors

$$\begin{aligned}&(\ldots,\quad 0,\quad c',\quad b'\,)[\lambda] + (\ldots,\quad 0,\quad b,\quad a\,)[-\lambda\beta^p]\\ &\quad + (\ldots,\quad 0,\quad 0,\quad b\,)[\lambda\delta]\\ &= (\ldots,\quad 0,\quad \lambda^{1/p}c',\quad \lambda b'\,) + (\ldots,\quad 0,\quad -\lambda^{1/p}\beta b,\quad -\lambda\beta^p a\,)\\ &\quad + (\ldots,\quad 0,\quad 0,\quad \lambda\delta b\,)\\ &= (\ldots,\quad 0,\quad \lambda^{1/p}c',\quad \lambda(b' + \delta b)\,) + (\ldots,\quad 0,\quad -\lambda^{1/p}\beta b,\quad -\lambda\beta^p a\,)\\ &= (\ldots,\quad 0,\quad \lambda^{1/p}(c' - \beta b),\quad \lambda(b' + \delta b - \beta^p a) + \Phi(\lambda^{1/p}c', -\lambda^{1/p}\beta b)\,).\end{aligned}$$

Recall that $\Phi(x, y)$ is the Witt polynomial $((x+y)^p - x^p - y^p)/p$. Equating both covectors, we find once again that $c' = \beta b$. Substituting this relation into Φ, we obtain the term $\Phi(\lambda^{1/p}\beta b, -\lambda^{1/p}\beta b)$. It vanishes since $b^p = 0$. Equating the rightmost coordinates gives us therefore the relation

$$a'^p = \lambda(b' + \delta b - \beta^p a).$$

We use these relations to eliminate the variables b, b' and c' in the expresssions for $\varphi(\mathbf{e}_1)$ and $\varphi(\mathbf{e}_2)$:

$$\begin{array}{lllll} \varphi(\mathbf{e}_1) = (\ldots, & 0, & \frac{a^p}{\lambda}, & a\,), & \\ \varphi(\mathbf{e}_2) = (\ldots, & 0, & \beta\frac{a^p}{\lambda}, & \beta^p a + \frac{a'^p}{\lambda} - \delta\frac{a^p}{\lambda}, & a'\,). \end{array}$$

It follows that the points of G correspond to pairs (a, a') satisfying the condition that φ maps $\mathcal{L}$ to the kernel of the Hasse-Witt exponential. This translates into the following four relations.

$$\begin{aligned} a^{p^2} &\equiv 0 \pmod{p}, \\ (\tilde{\lambda}\tilde{\beta}^p a + a'^p - \tilde{\delta}a^p)^p &\equiv 0 \pmod{p}, \\ a + \frac{1}{p}\left(\frac{a^p}{\tilde{\lambda}}\right)^p &\equiv 0 \pmod{p}, \\ a' + \frac{(a'^p + \tilde{\lambda}\tilde{\beta}^p a - \tilde{\delta}a^p)^p}{p\tilde{\lambda}^p} + \frac{1}{p^2}\left(\tilde{\beta}\frac{a^p}{\lambda}\right)^{p^2} &\equiv 0 \pmod{p}. \end{aligned}$$

Here $\tilde{\beta}$ and $\tilde{\delta}$ denote lifts of β and δ to W. The first two relations show that the third and the fourth make sense. The third relation is equivalent to the relation $a^{p^2} + p\tilde{\lambda}^p a \equiv 0 \pmod{p^2}$. It is consistent with the definition of a. We rewrite the last term in the last relation as $-\tilde{\beta}^{p^2} a^p p^{p-2}$. Note that this term is zero modulo p when $p > 2$. We find that a' is a zero of the polynomial

$$pX + \tilde{\lambda}^{-p}\left(X^p + \tilde{\lambda}\tilde{\beta}^p a - \tilde{\delta}a^p\right)^p - \tilde{\beta}^{p^2} a^p p^{p-1} \pmod{p^2}.$$

This shows that the zeroes of the polynomial $f(X)$ generate the extension K'_a. In addition, since there are exactly p^2 points in $G(\overline{K})$ mapping to a in $E(\overline{K})$, there are exactly p^2 different zeroes of $f(X)$ modulo p.

This proves the proposition.

Finally we compute the discriminant of the extension K'_a of K' of Prop.6.3. Since $a^{p^2} + \tilde{\lambda}^p pa = 0$, either $a = 0$ or the valuation of a is $1/(p^2 - 1)$ times that of p. In the first case the polynomial $f(X)$ of Prop.6.3 is equal to $X^{p^2} + \tilde{\lambda}^p pX$, which is the equation of the subgroup scheme E of G. It follows that our description of $G(\overline{K})$ is compatible with the one of the Galois module $E(\overline{K})$ of Prop. 6.1. From now on we assume that $a \neq 0$ and we normalize the valuation v by putting $v(a) = 1$. This implies that $v(p) = p^2 - 1$.

Proposition 6.4. *Let G be an extension of E by E with parameters β and δ as in Proposition 6.2. Let $a^{p^2} + \tilde{\lambda}^p pa = 0$ and suppose that $a \neq 0$.*

(i) If $\beta = \delta = 0$, then $f(X) = X^{p^2} + \tilde{\lambda}^p pX$ and the field K'_a is equal to K'.

(ii) If δ is not zero in $k/(\sigma^2-1)k$, but $\beta=0$ and we take $\tilde\beta=0$, then the polynomial $f(X)$ is equal to

$$f(X)=\left(X^p-\tilde\delta a^p\right)^p+\tilde\lambda^p pX,$$

and the extension K'_a is unramified over K'.

(iii) If $\beta\neq 0$, the polynomial $f(X)$ is irreducible over K' and the field K'_a is a totally ramified Galois extension of type $p\times p$ over K'. The discriminant of K'_a over K' is equal to p^p times a unit. The non-trivial characters have conductor a^p.

Proof. We have that $G\cong E\times E$ whenever $\beta=\delta=0$. Part *(i)* is then clear, since we can take $\tilde\beta=\tilde\delta=0$ To prove *(ii)*, Let $x\in\overline{W}$ denote a zero of $f(X)$. Then $pv(x^p-\delta a^p)=v(p)+v(x)$ and both sides are finite. This easily implies that we cannot have $v(x)<v(a)$ or $v(x)>v(a)$. Therefore $v(x)=v(a)=1$. Taking $\tilde\beta=0$ and putting $x=ay$, we obtain the relation

$$\tilde\lambda^p pay+(a^py^p-a^p\tilde\delta)^p=0.$$

Dividing by ap, we see that $-y+(y^p-\tilde\delta)^p\equiv 0 \pmod{p/a}$. This gives rise to the étale relation $y^{p^2}-y-\tilde\delta^p\equiv 0 \pmod{p/a}$. It follows that the action of $\mathrm{Gal}(\overline{K}/K)$ on $G(\overline{K})$ is *unramified* when $\beta=0$. On the other hand, $\mathrm{Gal}(K'_a/K')$ has exponent p. Since by assumption δ is not zero in $k/(\sigma^2-1)k$, it follows that the field K'_a is an unramified degree p extension of K'.

To prove *(iii)*, we first show that K'_a is totally ramified of degree p^2. Let x be a zero of $f(X)$ and let $y=x^p+a\beta^p\lambda-\delta a^p$. Then

$$\lambda^{-p}y^p=\tilde\beta^{p^2}a^pp^{p-1}-px.$$

If $v(x)<1/p$ we definitely also have that $v(px)<v(a^pp^{p-1})$ so that $v(px)=pv(y)$. Moreover, $v(y)=v(x^p)$, so that $p^2-1+v(x)=p^2v(x)$ and hence $v(x)=1$. This contradicts our assumption. On the other hand, if $v(x)>1/p$, we have that $v(y)=v(a)=1$. On the other hand, y^p is divisible by p so that $v(y)>(p^2-1)/p$ which is absurd. Therefore $v(x)=1/p$.

This implies that $v(px)<v(a^pp^{p-1})$ so that $v(y^p)=p^2-1+v(x)=p^2-1+1/p$. It follows that the valuation of $\pi=xy/a^p$ is equal to $1/p^2$. Therefore $K'\subset K'_a$ is totally ramified and $f(X)$ is irreducible over K'.

In order to compute the discriminant of K'_a over K', we let $x+t$ denote a second zero of $f(X)$, distinct from x. This zero also has valuation $1/p$ and hence $v(t)\geq 1/p$. Then

$$\begin{aligned}f(x+t)&=\tilde\lambda^p p(x+t)+\left((x+t)^p+\tilde\lambda\beta^pa-\tilde\lambda^p\tilde\delta a^p\right)^p-\tilde\lambda^p\tilde\beta^{p^2}a^pp^{p-1}=0,\\ &\equiv\tilde\lambda^p p(x+t)+\left(t^p+y\right)^p-\tilde\lambda^p\tilde\beta^{p^2}a^pp^{p-1}\equiv 0 \pmod{p^2},\end{aligned}$$

Next we subtract the relation $f(x) = \tilde{\lambda}^p px + y^p - \tilde{\lambda}^p \tilde{\beta}^{p^2} a^p p^{p-1} = 0$ and compute the result modulo $a^2 p$. Since y has valuation equal to $p - 1/p + 1/p^2$ and since $v(t) \geq 1/p$, we have that $(t^p + y)^p \equiv t^{p^2} + y^p \pmod{a^2 p}$ and we find that

$$pt + \tilde{\lambda}^{-p} t^{p^2} \equiv 0 \pmod{a^2 p}.$$

Since $f(X)$ has distinct zeroes modulo p, we have that $t \not\equiv 0 \pmod{p}$. Therefore t has the same valuation as a and we let $t = sa$. We divide by ap and find that

$$s^{p^2} - s \equiv 0 \pmod{a}.$$

Let $\tau \in \mathrm{Gal}(K'_a/K')$. We study the effect of τ on the uniformizer π introduced above. Suppose that $\tau(x) = x + sa \pmod{a^2}$ for some $s \in \overline{K}$. We have

$$\begin{aligned}\tau(y) &= (x + sa)^p + a(\tilde{\beta}^p \tilde{\lambda} + \tilde{\delta} a^{p-1}) \pmod{a^{p+1}},\\ &= x^p + s^p a^p + a(\tilde{\beta}^p \tilde{\lambda} + \tilde{\delta} a^{p-1}) \pmod{a^{p+1}},\\ &= y + s^p a^p \pmod{a^{p+1}}.\end{aligned}$$

Therefore $\tau(y/a^{p-1}) = y/a^{p-1} + s^p a \pmod{a^2}$ and

$$\tau(\frac{xy}{a^{p-1}}) \equiv \left(\frac{y}{a^{p-1}} + as^p\right)(x + sa) \pmod{a^2}$$

and hence

$$\tau(\pi) \equiv \pi + s\frac{y}{a^{p-1}} + xs^p \pmod{a}.$$

Since $v(y/a^{p-1}) = 1 - 1/p + 1/p^2 > 1/p = v(x)$, we see that the valuation of $\tau(\pi) - \pi$ is equal to $v(x) = 1/p$. Therefore the minimum polynomial of π has discriminant equal to $(x^{p^2(p^2-1)}) = (a^{p(p^2-1)}) = (p^p)$. Since the ring of integers $O_{K'_a}$ is equal to $O_{K'}[\pi]$, this is also the relative discriminant of the field K'_a over K'.

This proves the Proposition.

References

[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**, 1–46 (1988)

[2] Andreatta, F.: Formal patching of fpqc sheaves and Ext groups, preprint 2001

[3] Artin, M.: Algebraization of formal moduli: II. Existence of modifications. Annals Math. **91**, 88–135 (1970)

[4] Birch, B., Kuyk, W. (eds).: Modular functions in one variable IV. Lecture Notes in Math. **476**, Springer-Verlag, New York 1975

[5] Cohen, H., Oesterlé, J.: Dimensions des espaces de formes modulaires, p. 69–78 in Modular functions in one variable VI. Lecture Notes in Math. **627**, Springer-Verlag, New York 1977

[6] Conrad, B.: Finite group schemes over bases with low ramification. Compositio Math. **119**, 239–320 (1999)

[7] Cremona, J.: Algorithms for modular elliptic curves, Cambridge University Press, Cambridge 1992

[8] Fontaine, J.-M.: Groupes finis commutatifs sur les vecteurs de Witt. Comptes Rendues Acad. Sci. Paris **280**, 1423–1425 (1975)

[9] Fontaine, J.-M.: Groupes p-divisibles sur les corps locaux. Astérisque **47–48**, Soc. Math. France, Paris 1977

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

[11] Katz, N., Mazur, B.: Arithmetic moduli of elliptic curves, Annals of Math. Studies **108**, Princeton University Press, Princeton 1985

[12] Martinet, J.: Petits discriminants des corps de nombres, in J.V. Armitage, Journées Arithmetiques 1980, CUP Lecture Notes Series **56**, Cambridge University Press, Cambridge 1981

[13] Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. IHES **47**, 33–186 (1977)

[14] Mazur, B., Wiles, A.: Class fields of abelian extensions of $\mathbf{Q}$. Invent. Math. **76**, 179–330 (1984)

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

[16] Schoof, R.: Abelian varieties over $\mathbf{Q}(\sqrt{6})$ with good reduction everywhere, In: Class Field Theory – Its Centenary and Prospect. (ed) K. Miyake, Advanced Studies in Pure Mathematics, Tokyo 2001

[17] Schoof, R.: Abelian varieties over real quadratic fields with good reduction everywhere, preprint 2000

[18] Schoof, R.: Abelian varieties over the field of the 20th roots of unity that have good reduction everywhere, p. 291–296 in Ciliberto, C. et al., Proceedings of the NATO advanced research workshop Applications of Algebraic Geometry to Coding Theory, Physics and Computation, Kluwer, Dordrecht 2001

[19] Shafarevič, I.: Algebraic number fields, Proceedings of the International Congres of Mathematics, Stockholm 1962. Amer. Math. Soc. Translations **31**, 25–39 (1963)

[20] Tate, J.T., Oort, F.: Group schemes of prime order. Ann. Scient. École Norm. Sup. **3**, 1–21 (1970)

[21] Washington, L.C.: Introduction to cyclotomic fields, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York 1982