Advanced Studies in Pure Mathematics 30, 2001
Class Field Theory – Its Centenary and Prospect
pp. 287–306

Abelian Varieties over $\mathbf{Q}(\sqrt{6})$ with Good Reduction Everywhere

René Schoof

Abstract.

The elliptic curve with Weierstrass equation $Y^2 + \sqrt{6}XY - Y = X^3 - (2+\sqrt{6})X^2$ has good reduction modulo every prime of the ring of integers of $\mathbf{Q}(\sqrt{6})$. We show that every abelian variety over $\mathbf{Q}(\sqrt{6})$ that has good reduction everywhere is isogenous to a power of this elliptic curve.

§1. Introduction

In [12] B. Setzer shows that the elliptic curve $\mathcal{E}$ given over $\mathbf{Q}(\sqrt{6})$ by the equation

$$Y^2 + \sqrt{6}XY - Y = X^3 - (2+\sqrt{6})X^2$$

has good reduction at all primes of the ring of integers $\mathbf{Z}[\sqrt{6}]$. This can be seen from the fact that the discriminant of $\mathcal{E}$ is equal to the unit $(5+2\sqrt{6})^3$. Let $F = \mathbf{Q}(\sqrt{-2}, \sqrt{-3})$ denote the unique unramified quadratic extension of $\mathbf{Q}(\sqrt{6})$. In this paper we prove the following two theorems. Below we give the easy proof of the fact that the two results directly imply one another.

Theorem 1.1. *Every abelian variety over $\mathbf{Q}(\sqrt{6})$ that has good reduction at all primes of $\mathbf{Z}[\sqrt{6}]$ is isogenous over $\mathbf{Q}(\sqrt{6})$ to a power of the elliptic curve $\mathcal{E}$.*

Theorem 1.2. *Every abelian variety over F that has good reduction at all primes of the ring of integers O_F is isogenous over F to a power of the elliptic curve $\mathcal{E}$.*

Received December 7, 1998
Revised February 12, 1999

For several number fields K it is known that there do not exist any non-zero abelian varieties over K at all with good reduction everywhere [1, 5, 11]. In contrast, Theorems 1.1 and 1.2 say that over the number fields $\mathbf{Q}(\sqrt{6})$ and $\mathbf{Q}(\sqrt{-2}, \sqrt{-3})$, there exists, up to isogeny, precisely one *simple* abelian variety with good reduction everywhere. At present $\mathbf{Q}(\sqrt{6})$ and its unramified extension $\mathbf{Q}(\sqrt{-2}, \sqrt{-3})$ are the only number fields for which I know how to prove a statement like Theorem 1.1 or 1.2. Under the assumption of the Generalized Riemann Hypothesis however, one can prove similar results for a few more number fields.

We briefly sketch the proof of Theorem 1.2. An abelian variety with good reduction everywhere over $F = \mathbf{Q}(\sqrt{-2}, \sqrt{-3})$ is by definition the generic fiber of an abelian scheme A over O_F. Let $g = \dim(A)$. Let E denote an abelian scheme of dimension 1 over O_F with generic fiber isomorphic to Setzer's curve $\mathcal{E}$. We show that for every $n \geq 1$ the finite flat subgroup schemes $A[2^n]$ and $E^g[2^n]$ of 2^n-torsion points are isomorphic over O_F. Faltings' isogeny Theorem [4] implies then that A and E^g are isogenous.

In order to show the statement about the torsion points, we give a rather complete description of the commutative finite flat group schemes over O_F of rank a power of 2. In Section 2 we first determine all simple such group schemes; we invoke A.M. Odlyzko's discriminant bounds [9] and the theorems of J.-M. Fontaine [5] and V. Abraškin [1] on the ramification of the action of the Galois group on the points of these group schemes. Since we use the "unconditional" Odlyzko bounds, it is crucial that we consider group schemes whose rank is a power of 2 rather than a power of some prime $p > 2$. The next step is the determination of several extensions of the simple group schemes by one another. This is the content of Section 3. In this section we make use of a local result of C. Greither's [6]. From this and an application of Weil's Riemann Hypothesis for abelian varieties over finite fields, we obtain severe restrictions on the structure of the group schemes $A[2^n]$. In Section 4 we prove that $A[2^n] \cong E^g[2^n]$ for all $n \geq 1$ and we derive Theorem 1.2 from this.

In the remainder of the introduction we collect some information concerning the elliptic curve E. The j-invariant of E is 8000. Therefore E acquires complex multiplication by $\mathbf{Z}[\sqrt{-2}]$ over the extension $F = \mathbf{Q}(\sqrt{-2}, \sqrt{-3})$ of $\mathbf{Q}(\sqrt{6})$. The endomorphism $\sqrt{-2} \in \mathrm{End}(E)$ induces a 2-isogeny from E to E' that is defined over $\mathbf{Q}(\sqrt{6})$. Here E' denotes the quadratic twist of E that is associated to the extension $\mathbf{Q}(\sqrt{-2}, \sqrt{-3})$.

From this we easily deduce that Theorem 1.2 implies Theorem 1.1.

Suppose that A is an abelian variety over $\mathbf{Q}(\sqrt{6})$ that has good reduction everywhere. Then A also has good reduction everywhere over the extension F and hence it is isogenous to E^g over F. Taking Weil restrictions, it follows that $A \times A'$ is isogenous to $E^g \times E'^g$ over $\mathbf{Q}(\sqrt{6})$. Here A' denotes the twist of A associated to the quadratic extension $\mathbf{Q}(\sqrt{6}) \subset F$. Since E is isogenous to E', Theorem 1.1 follows.

Conversely, to see that Theorem 1.1 implies Theorem 1.2, we consider an abelian variety A over F that has good reduction everywhere and we take its Weil restriction to $\mathbf{Q}(\sqrt{6})$. Since the extension $\mathbf{Q}(\sqrt{6}) \subset F$ is only ramified at the infinite primes, the Weil restriction has good reduction everywhere over $\mathbf{Q}(\sqrt{6})$. Therefore it is isogenous to E^{2g}, where $g = \dim A$. Theorem 1.2 now follows easily by extending the base field to F.

We make some final remarks concerning the curve E. The three points of order 2 of E have their x-coordinates equal to $x = -\frac{1}{2}$ and $\frac{1+\sqrt{6}\pm(\sqrt{-2}+\sqrt{-3})i}{2}$ respectively. Their y-coordinates are given by $y = \frac{-\sqrt{6}x+1}{2}$. The point with $x = -\frac{1}{2}$ is the only 2-torsion point that is rational over $\mathbf{Q}(\sqrt{-2}, \sqrt{-3})$. The curve E has exactly six torsion points defined over $\mathbf{Q}(\sqrt{6})$. They are $(0,0)$ and its multiples $(2+\sqrt{6}, -5-2\sqrt{6})$, $(-\frac{1}{2}, \frac{1}{2(\sqrt{6}-2)})$, $(2+\sqrt{6}, 0)$, $(0,1)$ and ∞. Over F the curve E has exactly 18 rational torsion points, nine of which are the 3-torsion points. The curve E admits two $\mathbf{Q}(\sqrt{6})$-rational isogenies of degree 3. The kernel of one consists of the $\mathbf{Q}(\sqrt{6})$-rational points of order 3. The other has the points $(-1, \frac{(\pm\sqrt{-3}+1)(\pm\sqrt{-2}+1)}{2})$ and ∞ in its kernel. Dividing E by either of its rational subgroups of order 3, we obtain two more elliptic curves over $\mathbf{Q}(\sqrt{6})$ that have good reduction everywhere. The j-invariants of these curves are equal to $8000(49\pm12\sqrt{6})^3(5\pm2\sqrt{6})^2$. The curves admit complex multiplication by the non-maximal order $\mathbf{Z}[3\sqrt{-2}]$. See [8] for a description of these curves and their $\mathbf{Q}(\sqrt{6})$-rational isogenies. The existence of these curves shows that we cannot replace "isogenous" by "isomorphic" in Theorems 1.1 and 1.2.

§2. Simple 2-group schemes

In this section we determine all simple finite flat commutative group schemes over the ring of integers of $F = \mathbf{Q}(\sqrt{-2}, \sqrt{-3})$ of rank a power of 2. The main result is Theorem 2.3. In this section we denote by ζ_n a primitive n-the root of unity. As usual we let $i = \zeta_4$.

Let p be a prime and let R be a commutative domain with 1. In this section and the next we study finite flat commutative group schemes of p-power order over various rings R. We call such group schemes *p-group schemes*. Examples are provided by the constant group schemes $\mathbf{Z}/p^n\mathbf{Z}$ and their Cartier duals μ_{p^n}. For later use we recall a construction, due to N. Katz and B. Mazur, of certain p-group schemes of rank p^2. See [7, Interlude 8.7] or [11] for more details. For a unit $\varepsilon \in R^*$ we consider the R-algebra

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

The scheme $G_\varepsilon = \mathrm{Spec}(A)$ is a finite flat group scheme over R with multiplication of two points (t,i) and (s,j) (with $t^p = \varepsilon^i$, $s^p = \varepsilon^j$ and $0 \le i,j < p$) 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 G_ε is an extension of $\mathbf{Z}/p\mathbf{Z}$ by μ_p. It is killed by p and its $\overline{K}$-valued points generate the extension $K(\zeta_p, \sqrt[p]{\varepsilon})$ of the quotient field K of R. Two group schemes G_ε and $G_{\varepsilon'}$ are isomorphic if and only if ε/ε' is a p-th power.

A p-group scheme is called *simple* if it does not admit any closed flat subgroup schemes other than 0 and itself. Any p-group scheme of rank p is simple. Every p-group scheme admits a filtration with closed flat subgroup schemes whose successive quotients are simple.

In our main application we take $p = 2$ and $R = O_F$, the ring of integers of $F = \mathbf{Q}(\sqrt{-2}, \sqrt{-3})$. Let $\eta = \sqrt{-2} + \sqrt{-3}$. The unit group O_F^* is generated by ζ_6 and η. There lies a unique prime over 2 in O_F. It is generated by $\sqrt{-2}$ and its residue field has 4 elements. We'll see below that F does not admit any non-trivial everywhere unramified abelian extensions.

We already mentioned the fact that the constant group scheme $\mathbf{Z}/2\mathbf{Z}$ and its Cartier dual μ_2 are simple 2-group schemes over O_F. Another simple 2-group scheme is provided by the kernel $E[\pi]$ of the endomorphism $\pi = \sqrt{-2} \in \mathrm{End}(E)$ of Setzer's elliptic curve E that has been described in the introduction. Since E has good reduction everywhere, $E[\pi]$ is finite and flat over O_F. Since E has supersingular reduction at the unique prime over 2, the group scheme $E[\pi]$ is local and has a local Cartier dual. The main result of this section is Theorem 2.3. It says that these three group schemes are the only simple 2-group schemes over O_F.

The proof of Theorem 2.3 involves a rather detailed knowledge of

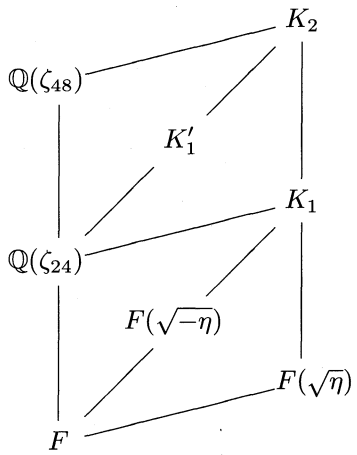
certain extensions of the number field F that are only ramified at the unique prime over 2. We isolate the facts we use in two lemmas.

Lemma 2.1. *Let* $\eta = \sqrt{-2} + \sqrt{-3}$ *and let* K *be a number field satisfying*

$$F \subset K \subset F(\zeta_{16}, \sqrt{\eta}).$$

Then there is only one prime of K *lying over* 2 *and* K *does not admit any non-trivial abelian extension that is at most tamely ramified at this prime.*

Proof. The degree $[F(\zeta_{16}, \sqrt{\eta}) : F]$ is equal to 8. Note that $F(i) = \mathbf{Q}(\zeta_{24})$. We let $K_1 = F(i, \sqrt{\eta}) = \mathbf{Q}(\zeta_{24}, \sqrt{\eta})$ and $K_2 = F(\zeta_{16}, \sqrt{\eta}) = \mathbf{Q}(\zeta_{48}, \sqrt{\eta})$. The fields K satisfying $F \subset K \subset K_2$ fit in the following diagram:



The techniques to prove this lemma are standard. We first compute the discriminants Δ_K and the root discriminants $\partial_K = |\Delta_K|^{1/[K:\mathbf{Q}]}$ of all subfields K.

All fields K are abelian extensions of F that are unramified outside 2. We compute the conductors of the Dirichlet characters of $\mathrm{Gal}(K_2/F)$. By [3, Lemma 6], the root discriminant of $\mathbf{Q}(\zeta_{24})$ is equal to $4\sqrt{3}$. Applying the conductor discriminant formula to the extension $F \subset \mathbf{Q}(\zeta_{24})$, we see that the conductor of the corresponding quadratic character is equal to $(\sqrt{-2})^2 = (2)$. On the other hand, since $\eta \equiv 1 + \sqrt{-2} \pmod 2$, it follows from class field theory that the 2-part of the ray class group of F of conductor (2) has order at most 2. It follows that $\mathbf{Q}(\zeta_{24})$ is the full ray class field of conductor (2) of F and that the

character corresponding to $\mathbf{Q}(\zeta_{24})$ is the unique character of conductor (2). Since the discriminants of the polynomials $T^2 \pm \eta$ are equal to (4), the quadratic characters corresponding to the extensions $F(\sqrt{\eta})$ and $F(\sqrt{-\eta})$ each have conductor (4), possibly divided by an even power of $(\sqrt{-2})$. Since neither character can have conductor (2), both have conductor equal to (4). Finally, since the root discriminant of $\mathbf{Q}(\zeta_{48})$ is equal to $8\sqrt{3}$ (see [3, Lemma 6]), it follows easily from an application of the conductor discriminant formula over F that both characters of order 4 of $\mathrm{Gal}(\mathbf{Q}(\zeta_{48})/F)$ have conductor $(\sqrt{-2})^5$. This implies that all four characters of order 4 of $\mathrm{Gal}(K_2/F)$ have conductor $(\sqrt{-2})^5$.

An application of the conductor discriminant formula over F gives that the root discriminants of the intermediate fields are given by

$$\begin{aligned} \partial_F &= \sqrt{24} \leq 4.899, \\ \partial_{F(\sqrt{\pm\eta})} &= 2\sqrt{24} \leq 9.798, \\ \partial_{K_1} &= 2^{5/4}\sqrt{24} \leq 11.65, \\ \partial_{K_1'} = \partial_{\mathbf{Q}(\zeta_{48})} &= 8\sqrt{3} \leq 13.866, \\ \partial_{K_2} &= 2^{15/8}\sqrt{24} \leq 17.9696. \end{aligned}$$

It follows that the prime over 2 in K_2 is totally ramified over F. Hence there is in every intermediate field K precisely one prime lying over 2.

Next we apply Odlyzko's discriminant bounds [9, p.187] to show that none of the subfields K admit a non-trivial everywhere unramified abelian extension. For every subfield K, let h_K denote the degree of the maximal abelian everywhere unramified extension H_K of K. We must show that $h_K = 1$ for each K. We start with F itself. The root discriminants of F and H_F are equal to $\sqrt{24} \leq 4.899$. Odlyzko's discriminant bounds imply that $[H_F : \mathbf{Q}] \leq 6$ and hence $[H_F : F] = 1$. In a similar way, Odlyzko's discriminant bounds imply at once that $h_K = 1$ for $K = \mathbf{Q}(\zeta_{24})$ and K_1. The bounds imply that $h_K \leq 2$ for the two subfields $K = F(\sqrt{\pm\eta})$. Since only the prime over 2 ramifies in these quadratic extensions of F, it follows from [14, Thm. 10.4] that $h_K = 1$ for $K = F(\sqrt{\pm\eta})$. Odlyzko's bounds imply that $h_K \leq 3$ for $K = \mathbf{Q}(\zeta_{48})$ and $K = K_1'$. Both fields are cyclic extensions of degree 4 of F. Since the common quadratic subfield $\mathbf{Q}(\zeta_{24})$ admits no non-trivial abelian everywhere unramified extension, it follows from [14, Thm. 10.8] that h_K cannot be equal to 3. Since only the unique prime over 2 is ramified, h_K cannot be equal to 2 either. Therefore $h_K = 1$ for both fields K. Finally Odlyzko's bounds show that $h_{K_2} \leq 5$. Since the Galois group of K_2 over $\mathbf{Q}(\zeta_{24})$ is isomorphic to the Klein four group, the odd

part of h_{K_2} is equal to the product of the odd parts of the numbers h_K corresponding to the three quadratic subfields K. Therefore the odd part of h_{K_2} is trivial. By [14, Thm. 10.4], the degree h_{K_2} cannot be 2 or 4 either. Therefore it is 1.

Finally we apply class field theory to show that none of the subfields K admits an abelian extension that is at most tamely ramified at the unique prime over 2. Since $h_K = 1$ for each subfield K, the ray class group of conductor the unique prime over 2 is isomorphic to the multiplicative group $\mathbf{F}_4^*$ modulo the images of the global units. Since $\zeta_3 \in O_K^*$ for each subfield K, this ray class group is trivial for each K. This proves the Lemma.

Lemma 2.2. *Let L be a Galois extension of $\mathbf{Q}$ that contains F and for which the following hold:*

- *$F \subset L$ is unramified except at the unique prime over 2;*
- *i and $\sqrt{\eta}$ are contained in L;*
- *the root discriminant ∂_L of L satisfies $\partial_L < 8\sqrt{6}$.*

Then $[L : F]$ is a power of 2.

Proof. Since $\partial_L < 8\sqrt{6} \leq 19.596$, Odlyzko's bounds [9] imply that $[L : \mathbf{Q}] \leq 380$. This implies that $[L : F(i, \sqrt{\eta})] \leq 380/16$. Therefore we have the following inclusions of fields (the superscripts indicate the relative degrees):

$$\mathbf{Q} \overset{4}{\subset} F \overset{4}{\subset} F(\sqrt{\eta}, i) \overset{\leq 23}{\subset} L.$$

Since the degree $[L : F(\sqrt{\eta}, i)]$ is less than 60, the Galois group $\mathrm{Gal}(L/F(\sqrt{\eta}, i))$ and hence the Galois group $\pi = \mathrm{Gal}(L/\mathbf{Q})$ are *solvable* groups. We will show that π is a 2-group.

The largest abelian extension F' of $\mathbf{Q}$ inside L contains $F(i) = \mathbf{Q}(\zeta_{24})$. Since L is only ramified at the prime over 2 of F and since $\partial_L < 8\sqrt{6}$, there are only two possibilities for F'. Either $F' = \mathbf{Q}(\zeta_{24})$ or $F' = \mathbf{Q}(\zeta_{48})$. This shows that $\pi/\pi' = \mathrm{Gal}(F'/\mathbf{Q})$ is a 2-group. Here π' denotes the commutator subgroup of π. We distinguish the two cases.

Case 1. $F' = \mathbf{Q}(\zeta_{48})$.
Since $[L : \mathbf{Q}] \leq 380$, we have the following diagram of extensions (the superscripts indicate the relative degrees):

$$\mathbf{Q} \overset{16}{\subset} \mathbf{Q}(\zeta_{48}) \overset{2}{\subset} \mathbf{Q}(\zeta_{48}, \sqrt{\eta}) \overset{\leq 11}{\subset} L.$$

By Lemma 2.1, the field $\mathbf{Q}(\zeta_{48})$ does not admit an abelian extension that is at most tamely ramified at its unique prime over 2. This implies that π'/π'' is a finite 2-group.

The order of π'/π'' is at least 2. If it is actually equal to 2, the fixed field of π'' is $\mathbf{Q}(\zeta_{48}, \sqrt{\eta})$. By Lemma 2.1, this field does not admit an abelian extension that is only tamely ramified at the unique prime over 2. Therefore π''/π''' is a 2-group. This implies that π'/π''' is a 2-group which is cyclic modulo its commutator subgroup. Therefore π'/π''' itself is cyclic and hence π''/π''' and hence π'' are trivial. It follows that π is a 2-group.

If the order of π'/π'' is at least 4, we have that $\#\pi'' \leq 5$, so that π'' is abelian. If $\#\pi''$ has order 2 or 4, the group π is a 2-group and we are done. If not, then π'' is cyclic of odd order and the exact sequence

$$0 \longrightarrow \pi'' \longrightarrow \pi' \longrightarrow \pi'/\pi'' \longrightarrow 0$$

is split. Since $\mathrm{Aut}(\pi'')$ is abelian, π' is in the kernel of the homomorphism $\pi \longrightarrow \mathrm{Aut}(\pi'')$ which is induced by conjugation. This implies that π' is isomorphic to the direct product of π'/π'' and π''. This shows that π'' is trivial. This shows that π is a 2-group as required.

Case 2. $F' = \mathbf{Q}(\zeta_{24})$. Since $[L : \mathbf{Q}] < 380$ we have the following diagram of extensions.

$$\mathbf{Q} \overset{8}{\subset} \mathbf{Q}(\zeta_{24}) \overset{2}{\subset} \mathbf{Q}(\zeta_{24}, \sqrt{\eta}) \overset{\leq 23}{\subset} L.$$

By Lemma 2.1, the field $\mathbf{Q}(\zeta_{24})$ does not admit an abelian extension that is at most tamely ramified at the unique prime over 2. This implies that π'/π'' is a finite 2-group.

The order of π'/π'' is at least 2. If it is actually equal to 2, the fixed field of π'' is $\mathbf{Q}(\zeta_{24}, \sqrt{\eta})$. By Lemma 2.1, this field does not admit an abelian extension that is only ramified at the unique prime over 2. Therefore π''/π''' is a 2-group. Since π'/π'' is cyclic, the group π'/π''' is itself cyclic. Therefore π'' is trivial and π is a 2-group.

Therefore we assume that $\#(\pi'/\pi'') \geq 4$ and hence $\#\pi'' \leq 11$.

Claim. The odd part of π''/π''' is cyclic.

Proof of the Claim. If the odd part of π''/π''' is is not cyclic we have that $\pi''/\pi''' \cong C(3) \times C(3)$ where $C(3)$ denotes a cyclic group of order 3. It follows that π''' is trivial, that $\#(\pi'/\pi'') = 4$ and that $[L : \mathbf{Q}] = 8 \cdot 4 \cdot 9 = 288$. Let K denote the fixed field of π''. We have the following inclusions

$$\mathbf{Q} \overset{8}{\subset} \mathbf{Q}(\zeta_{24}) \overset{2}{\subset} \mathbf{Q}(\zeta_{24}, \sqrt{\eta}) \overset{2}{\subset} K \overset{3\times 3}{\subset} L.$$

The field K is an abelian extension of $\mathbf{Q}(\zeta_{24})$ of degree 4 which is only ramified at the prime over 2. By Lemma 2.1, the subfield $\mathbf{Q}(\zeta_{24}, \sqrt{\eta})$

does not admit a non-trivial unramified abelian extension. Therefore the field K is a ramified quadratic extension. This implies that the prime over 2 in $\mathbf{Q}(\zeta_{24})$ is totally ramified in K and hence its residue field is again $\mathbf{F}_4$. Since $\zeta_3 \in K$, it follows from class field theory that K does not admit any cyclic extension of degree 3 which is tamely ramified at the unique prime over 2. Therefore, if $\pi''/\pi''' \cong C(3) \times C(3)$, the extension L is everywhere unramified over K. This implies that $\partial_L = \partial_K$.

Let χ denote the quadratic character corresponding to the extension $\mathbf{Q}(\zeta_{24}) \subset \mathbf{Q}(\zeta_{24}, \sqrt{\eta})$. We saw in the proof of Lemma 2.1 that the root discriminant of $\mathbf{Q}(\zeta_{24}, \sqrt{\eta})$ is equal to $2^{5/4}\sqrt{24}$. Since $\zeta_8 - 1$ generates the unique prime over 2 in $\mathbf{Q}(\zeta_{24})$, an application of the conductor discriminant formula over $\mathbf{Q}(\zeta_{24})$ then implies that the conductor of χ is equal to $(\zeta_8 - 1)^6$. Suppose $(\zeta_8 - 1)^a$ is the conductor of one of the other two non-trivial characters of $\mathrm{Gal}(K/\mathbf{Q}(\zeta_{24}))$. If $a > 6$, both these characters have conductor $(\zeta_8 - 1)^a$ and applying the conductor discriminant formula to K gives that

$$\frac{24}{2\sqrt{3}} 4^{\frac{6+2a}{32}} = \partial_K = \partial_L < 4\sqrt{24}.$$

In other words $a < 9$ and hence $a \leq 8$. Therefore $\partial_L = \partial_K \leq 2^{27/8} 3^{1/2} \leq 17.9697$. This inequality obviously also holds when $a \leq 6$. Odlyzko's bounds imply then that $[L : \mathbf{Q}] < 170$. This contradicts the fact that $[L : \mathbf{Q}] = 288$. Therefore it cannot happen that $\pi''/\pi''' \cong C(3) \times C(3)$ and our claim follows.

Let P denote the minimal subgroup $\pi''' \subset P \subset \pi''$ of odd index in π''. By the claim, π''/P is cyclic so that $\mathrm{Aut}(\pi''/P)$ is abelian. Therefore π' is in the kernel of the natural map $\pi \longrightarrow \mathrm{Aut}(\pi''/P)$ and the action by conjugation of π'/π'' on π''/P is trivial. Since the exact sequence

$$0 \longrightarrow \pi''/P \longrightarrow \pi'/P \longrightarrow \pi'/\pi'' \longrightarrow 0$$

is split, we conclude that π''/P is trivial. In other words, π''/π''' is a 2-group.

If π''/π''' is trivial, it follows from the solvability of π that π'' is trivial and hence that π is a 2-group. If π''/π''' has order 2, and π'/π'' has order 4, the group π/π''' would be a group of order 64. But this is impossible since all groups of order 64 have an abelian commutator subgroup. In all other cases either $\#(\pi''/\pi''') \geq 4$ or $\#(\pi'/\pi'') \geq 8$ so that the order of π is divisible by 128. Since $\#\pi \leq 380$, it follows that π is a 2-group as required.

Theorem 2.3. *The simple 2-group schemes over* O_F *are* $\mathbf{Z}/2\mathbf{Z}$, μ_2 *and* $E[\pi]$.

Proof. Suppose that G is a simple 2-group scheme over O_F. Then G is annihilated by 2. Let G' be the product of all $\mathrm{Gal}(F/\mathbf{Q})$-conjugates of G and of the Katz-Mazur group schemes G_ε where $\varepsilon \in O_F^*$ runs through a set of representatives of $O_F^*/(O_F^*)^2$. Then G' is a finite flat group scheme over O_F that is annihilated by 2. Let L be the extension that we obtain by adjoining the points of G' to F. This is an extension of F that is unramified except possibly at the unique prime of F lying over 2. By construction, L is a Galois extension of $\mathbf{Q}$ and it contains $\sqrt{\varepsilon}$ for every $\varepsilon \in O_F^*$. Since G' is killed by 2, the results of Fontaine [5] and Abraškin [1] imply that the root discriminant ∂_L of the number field L satisfies

$$\partial_L < \partial_F 2^{1+\frac{1}{2-1}} = 4\sqrt{24} \leq 19.596.$$

Therefore all conditions of Lemma 2.2 are satisfied and we conclude that $\mathrm{Gal}(L/F)$ is a 2-group.

Since all points of our simple group scheme G become rational over L, the Galois group $\mathrm{Gal}(L/F)$ acts on the group $G(\overline{F})$. Since both these groups are 2-groups, there is a non-trivial fixed point. Such a point generates a $\mathrm{Gal}(\overline{F}/F)$-submodule of $G(\overline{F})$ of order 2. In other words, the point generates a closed subgroup scheme of rank 2 of the base change of G to F. The Zariski closure of this subgroup scheme inside the O_F-group scheme G is a finite flat closed subgroup scheme of G over O_F. By simplicity it must be equal to G. This shows that G has rank 2.

To complete the proof we observe as in [10, p.1] or [13, Example (3.2)], that for any ring R, any finite flat R-group scheme of rank 2 is isomorphic to $G_{a,b} = \mathrm{Spec}(R[X]/(X^2 + aX))$ with comultiplication given by $X \mapsto u+v+buv \in R[u,v]/(u^2+au, v^2+av)$ for certain $a, b \in R$ satisfying $ab = 2$. Two group schemes $G_{a,b}$ and $G_{a',b'}$ are isomorphic when $a = ua'$ and $b = u^{-1}b'$ for some $u \in R^*$. In order to apply this to the ring O_F, we observe that $2 = -\sqrt{-2}^2$ is a factorization of 2 into prime factors and hence that there are, up to isomorphism, three group schemes of order 2 over O_F. They correspond to $a = 1, \sqrt{-2}, 2$ respectively. We recover $\mathbf{Z}/2\mathbf{Z}$ and μ_2 by taking $a = 1$ and $a = 2$ respectively. The group scheme corresponding to $a = \sqrt{-2}$ is local and self dual. It is isomorphic to the group scheme $E[\pi]$.

This proves the theorem.

§3. Extensions

As in the previous sections we let $F = \mathbf{Q}(\sqrt{-2}, \sqrt{-3})$ and write O_F for the ring of integers of F. In this section we compute various

extensions of the three simple 2-group schemes μ_2, $E[\pi]$ and $\mathbf{Z}/2\mathbf{Z}$ by one another over O_F. We do this by determining the extensions locally as well as generically. The global result over O_F follows from an application of an exact Mayer-Vietoris sequence.

The following result is in [11].

Proposition 3.1. (*"Mayer-Vietoris"*) *Let K be a number field, let p be a prime and let G and H be two p-group schemes over O_K. Then there is a natural exact sequence*

$$\begin{aligned} 0 \longrightarrow & \mathrm{Hom}_{O_K}(G,H) \longrightarrow \mathrm{Hom}_{O_K\otimes\mathbf{Z}_p}(G_p,H_p)\times \mathrm{Hom}_{O_K[1/p]}(G_{\frac{1}{p}},H_{\frac{1}{p}}) \\ & \longrightarrow \mathrm{Hom}_{K\otimes\mathbf{Q}_p}(G_1,H_1) \xrightarrow{\delta} \mathrm{Ext}^1_{O_K}(G,H) \\ & \longrightarrow \mathrm{Ext}^1_{O_K\otimes\mathbf{Z}_p}(G_p,H_p)\times \mathrm{Ext}^1_{O_K[1/p]}(G_{\frac{1}{p}},H_{\frac{1}{p}}) \\ & \longrightarrow \mathrm{Ext}^1_{K\otimes\mathbf{Q}_p}(G_1,H_1) \longrightarrow \dots \end{aligned}$$

Here G_p, $G_{\frac{1}{p}}$ and G_1 denote the base changes of G to $O_K\otimes\mathbf{Z}_p$, $O_K[1/p]$ and $K\otimes\mathbf{Q}_p$ respectively. Similarly for H_p, ... etc.

Most maps in the sequence of the proposition are the obvious ones. The only one that needs explanation is

$$\mathrm{Hom}_{K\otimes\mathbf{Q}_p}(G,H) \xrightarrow{\delta} \mathrm{Ext}^1_{O_K}(G,H).$$

We use the fpqc covering $\{\mathrm{Spec}(O_K\otimes\mathbf{Z}_p), \mathrm{Spec}(O_K[1/p])\}$ of $\mathrm{Spec}(O_K)$ to give a simple description of the category of p-group schemes over O_K and to define δ. See [2, Thm. 2.6] for this description and [11] for the definition of the map δ and for a proof of the fact that the sequence is exact.

Proposition 3.2. *We have the following:*

(i) $\mathrm{Ext}^1_{O_F}(\mu_2,\mathbf{Z}/2\mathbf{Z})$, $\mathrm{Ext}^1_{O_F}(E[\pi],\mathbf{Z}/2\mathbf{Z})$ *and* $\mathrm{Ext}^1_{O_F}(\mu_2,E[\pi])$ *are all trivial.*

(ii) $\mathrm{Ext}^1_{O_F}(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z})$ *is cyclic of order 2; it is generated by the extension $\mathbf{Z}/4\mathbf{Z}$.*

(iii) $\mathrm{Ext}^1_{O_F}(\mu_2,\mu_2)$ *is cyclic of order 2; it is generated by the extension μ_4.*

Proof. As we have seen in the previous section, the field F does not admit any unramified quadratic extensions. This is the main arithmetical ingredient in the proof.

(i) Suppose G is an extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$. In other words, there is an exact sequence of 2-group schemes over O_F

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

Over the completion of O_F at the unique prime over 2, the connected component gives a section and the sequence is split. Therefore the action of $Gal(\overline{F}/F)$ on $G(\overline{F})$ is everywhere unramified. It follows that the Galois action is actually trivial. So, the extension is locally as well as generically trivial.To finish the proof we observe that $\mathrm{Hom}_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Hom}_{O_F \otimes \mathbf{Z}_2}(\mu_2, \mathbf{Z}/2\mathbf{Z}) = 0$. Moreover, since there is only one prime of O_F lying over 2, both groups $\mathrm{Hom}_F(\mu_2, \mathbf{Z}/2\mathbf{Z})$ and $\mathrm{Hom}_{O_F \otimes \mathbf{Q}_2}(\mu_2, \mathbf{Z}/2\mathbf{Z})$ have order 2. Therefore it follows from the Mayer-Vietoris sequence of Prop. 3.1 that the extension is split over O_F. This proves (i).

Since $E[\pi]$ is a local group scheme, exactly the same proof shows that $\mathrm{Ext}^1_{O_F}(E[\pi], \mathbf{Z}/2\mathbf{Z})$ vanishes. By Cartier duality we then also have that $\mathrm{Ext}^1_{O_F}(\mu_2, E[\pi]) = 0$. This proves (i).

(ii) Any extension G of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$ is étale. Therefore, adjoining its points to F gives rise to an everywhere unramified extension of degree at most 2. It follows that the Galois action on $G(\overline{F})$ is actually trivial. By Galois theory, the étale group schemes over O_F are determined by their generic fibers. It follows that $G \cong \mathbf{Z}/4\mathbf{Z}$ or that $G \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ as required.

(iii) This part follows from part (ii) by Cartier duality.

Let O_2 denote the completion of O_F at the unique prime over 2. We have that $O_2 \cong \mathbf{Z}_2[\zeta_3][\sqrt{-2}]$. Let F_2 denote the quotient field of O_2. The following result is a special case of a result of Greither's [6].

Lemma 3.3. *Let* $U = \{u \in O_2^* : u \equiv 1 \pmod{\sqrt{-2}^3}\}$. *Then*

$$\mathrm{Ext}^1_{O_2}(E[\pi], E[\pi]) \cong U/(U \cap O_2^{*2}).$$

Moreover, the quadratic extension of F_2 *generated by the points of the extension of* $E[\pi]$ *by* $E[\pi]$ *corresponding to* $u \in U/(U \cap O_2^{*2})$ *is the field* $F_2(\sqrt{-u})$.

The first statement is a special case of [6, Cor. 3.6 (a)]. If one carefully goes through Greither's proof, one finds that the field extension corresponding to the unit $u \in U$ is $F_2(\sqrt{-u})$.

Proposition 3.4. *The extension group* $\mathrm{Ext}^1_{O_F}(E[\pi], E[\pi])$ *is cyclic of order* 2; *it is generated by the extension* $E[2]$.

Proof. Let G be an extension of $E[\pi]$ by $E[\pi]$ over O_F. We recall that F_2 denotes the quotient field of the completion of O_F at the unique prime over 2. By Lemma 3.3, the field obtained by adjoining the points of G to F_2 is $F_2(\sqrt{-u})$, where u is some unit that is congruent to 1 (mod $\sqrt{-2}^3$). Since $-u \equiv 1 \pmod{\sqrt{-2}^2}$, the discriminant and conductor of this quadratic extension of F_2 divide the discriminant of the polynomial $T^2 - \sqrt{-2}T - (1+u)/2$ which is $4/\sqrt{-2}^2 = (\sqrt{-2})^2$.

Since the action of $\mathrm{Gal}(\overline{F}/F)$ is unramified outside 2, this implies that the field obtained by adjoining the points of $G(\overline{F})$ to the number field F is contained in the ray class field of F of conductor $(2) = (\sqrt{-2})^2$. In the previous section we have already seen that the ray class field of F of conductor $(\sqrt{-2})$ is F itself. Since $-1 \equiv 1 \pmod 2$ and $\eta = \sqrt{-3}+\sqrt{-2} \equiv 1+\sqrt{-2} \pmod 2$, we see that the ray class group of F of conductor (2), which is isomorphic to $(O_F/(2))^*/\langle -1, \eta, \zeta_3\rangle$, has order at most 2. On the other hand, the extension $F \subset F(i)$ is easily seen to have conductor (2). This shows that the ray class field of F of conductor (2) is equal to $F(i)$.

It follows from this and the Mayer-Vietoris exact sequence of Prop. 3.1 that $\mathrm{Ext}^1_{O_F}(E[\pi], E[\pi])$ has order 2. As we remarked at the end of the introduction, the elliptic curve E admits only one rational point of order 2. Therefore $E[2]$ is a non-trivial extension of $E[\pi]$ by $E[\pi]$ and hence this extension represents the non-trivial element of $\mathrm{Ext}^1_{O_F}(E[\pi], E[\pi])$ and we are done.

The extensions of $\mathbf{Z}/2\mathbf{Z}$, μ_2 and $E[\pi]$ by one another that are not listed in Propositions 3.2 or 3.4, are in general not trivial. For instance, there is an exact sequence

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

The Katz-Mazur group schemes G_ε represent non-trivial classes in $\mathrm{Ext}^1_{O_F}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$.

§4. Abelian varieties

Let $F = \mathbf{Q}(\sqrt{-2}, \sqrt{-3})$. In this section we derive a structure theorem concerning 2-group schemes over O_F and prove Theorem 1.2. As is explained in the introduction, the endomorphism ring $\mathrm{End}(E)$ of

the Setzer curve E is isomorphic to $\mathbf{Z}[\sqrt{-2}]$. We write π for the endomorphism $\sqrt{-2}$. As usual, we denote the kernel of multiplication $\pi^m : E \longrightarrow E$ by $E[\pi^m]$. It is a finite flat O_F-group scheme of rank 2^m. For every $m, n \geq 0$ we have an exact sequence

$$0 \longrightarrow E[\pi^m] \longrightarrow E[\pi^{n+m}] \xrightarrow{\pi^m} E[\pi^n] \longrightarrow 0.$$

Lemma 4.1. *The natural homomorphisms*

$$(\mathrm{End}(E)/(\pi^n))[\pi^m] \xrightarrow{\varphi} \mathrm{Hom}(E[\pi^n], E[\pi^m]) \xrightarrow{\psi} \mathrm{Hom}_F(E[\pi^n], E[\pi^m])$$

are both isomorphisms. Here the leftmost group is a subgroup of a quotient of $\mathrm{End}(E)$*; the group in the middle is the group of* O_F*-group scheme homomorphisms* $f : E[\pi^n] \longrightarrow E[\pi^m]$ *and* $\mathrm{Hom}_F(E[\pi^n], E[\pi^m])$ *denotes the group of homomorphisms* $E[\pi^n](\overline{F}) \longrightarrow E[\pi^m](\overline{F})$ *of* $\mathrm{Gal}(\overline{F}/F)$*-modules.*

Proof. It is a standard fact that the map $\psi\varphi$ is injective. It follows that φ is injective. To see that ψ is injective, let $f : E[\pi^n] \longrightarrow E[\pi^m]$ be an O_F-morphism of groupschemes for which $\psi(f) = 0$. This means that $f^*(I_B \otimes F) = F \otimes f^*(I_B)$ is zero. Here I_B denotes the augmentation ideal of the Hopf algebra B of $E[\pi^m]$. By flatness it follows that $f^*(I_B) = 0$, so that $f = 0$. Since both φ and ψ are injective, it suffices to show that $\#\mathrm{Hom}_F(E[\pi^n], E[\pi^m])$ is at most $\#(\mathrm{End}(E)/(\pi^n))[\pi^m] = 2^{min(n,m)}$.

$\underline{n = 1}$. We proceed by induction with respect to m. When $m = 1$, the statement is obvious, When $m = 2$, we observe that the only Galois submodule of order 2 of $E[\pi^2] = E[2]$ is $E[\pi]$. Therefore the image of any homomorphism $E[\pi] \longrightarrow E[2]$ is contained in $E[\pi]$ and hence $\mathrm{Hom}_F(E[\pi], E[\pi]) \cong \mathrm{Hom}_F(E[\pi], E[2])$ has order 2.

When $m > 2$, we consider the exact sequence

$$0 \longrightarrow \mathrm{Hom}_F(E[\pi], E[2]) \longrightarrow \mathrm{Hom}_F(E[\pi], E[\pi^m]) \xrightarrow{\theta} \mathrm{Hom}_F(E[\pi], E[\pi^{m-2}]),$$

where $\theta(f) = 2 \cdot f = f \cdot 2$. It follows that $\theta = 0$ and hence that $\#\mathrm{Hom}_F(E[\pi], E[2^m]) = \#\mathrm{Hom}_F(E[\pi], E[2]) = 2$.

$\underline{n > 1,\ m < n}$. We proceed by induction with respect to n. Consider the exact sequence

$$0 \longrightarrow \mathrm{Hom}_F(E[\pi^{n-1}], E[\pi^m]) \longrightarrow \mathrm{Hom}_F(E[\pi^n], E[\pi^m]) \xrightarrow{\theta} \mathrm{Hom}_F(E[\pi], E[\pi^m]).$$

Since $n > m$, no $f \in \mathrm{Hom}_F(E[\pi^n], E[\pi^m])$ is injective. Since $E[\pi]$ is the unique minimal Galois submodule of $E[\pi^n]$, this means that $\theta(f)$ is zero and it follows that the first two groups in the exact sequence are isomorphic. Therefore $\#\mathrm{Hom}_F(E[\pi^n], E[\pi^m]) = \#\mathrm{Hom}_F(E[\pi^{n-1}], E[\pi^m]) = 2^m$ as required.

$n > 1$, $m \geq n$. The same exact sequence implies that

$$\#\mathrm{Hom}_F(E[\pi^n], E[\pi^m]) \leq \#\mathrm{Hom}_F(E[\pi^{n-1}], E[\pi^m]) \cdot \#\mathrm{Hom}_F(E[\pi], E[\pi^m])$$

and hence, inductively, that $\#\mathrm{Hom}_F(E[\pi^n], E[\pi^m]) \leq 2^{n-1} \cdot 2 = 2^n$.

This completes the proof of the lemma.

Lemma 4.2. *For each* $m \geq 1$,

$$\mathrm{Ext}^1_{O_F}(E[\pi], E[\pi^m])$$

is a group of order 2. *Moreover, the group* $E[\pi^{m+1}]$ *is a non-trivial extension of* $E[\pi]$ *by* $E[\pi^m]$.

Proof. For $m = 1$, this is Prop. 3.4. For $m > 1$, we apply the functor $\mathrm{Hom}(E[\pi], -)$ to the exact sequence $0 \longrightarrow E[\pi] \longrightarrow E[\pi^{m+1}] \longrightarrow E[\pi^m] \longrightarrow 0$. It follows from Lemma 4.1 and the fact, established in Prop. 3.4, that $\mathrm{Ext}^1_{O_F}(E[\pi], E[\pi])$ has order 2, that there is an injective homomorphism

$$\mathrm{Ext}^1_{O_F}(E[\pi], E[\pi^{m+1}]) \hookrightarrow \mathrm{Ext}^1_{O_F}(E[\pi], E[\pi^m]).$$

It follows by induction that $\#\mathrm{Ext}^1_{O_F}(E[\pi], E[\pi^m]) \leq 2$. The exact sequence $0 \longrightarrow E[\pi] \longrightarrow E[\pi^{m+1}] \longrightarrow E[\pi^m] \longrightarrow 0$ is not split, because it is not even split over $\overline{F}$. Therefore the extension group has exactly 2 elements, as required.

Theorem 4.3. *The objects of the form* $\oplus_{i=1}^r E[\pi^{n_i}]$ *form a full abelian subcategory* $\underline{C}$ *of the category of fppf sheaves over* O_F.

Proof. We need to show that kernels exist in $\underline{C}$. Since $E[\pi]$ is self-dual, cokernels then exist by duality. The category $\underline{C}$ obviously has all the other properties of an abelian category. Let therefore

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

be a homomorphism of fppf sheaves or, equivalently, of group schemes. By Lemma 4.1, there are endomorphisms $f_{ij} \in \mathrm{End}(E)$ that induce g. Therefore the kernel K of g is isomorphic to the kernel of

$$\bigoplus_{i=1}^{r} E[\pi^{n_i}] \xrightarrow{f_{ij}} E^s.$$

Consider the commutative diagram

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

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

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

respectively. The diagram has exact rows and columns and it easily implies that

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

Since $\mathbf{Z}[\sqrt{-2}]$ is a principal ideal domain, there exist an invertible $r \times r$-matrix B and an invertible $(r+s) \times (r+s)$-matrix B' with entries in $\mathrm{End}(E) \cong \mathbf{Z}[\sqrt{-2}]$ so that

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

This shows that K is isomorphic to the kernel of the map

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

Since the ideal generated by the determinants of the $r \times r$ submatrices of A contains a power of π, all entries g_i divide some power of π, so that $g_i = \pm\pi^{n_i}$ for some n_i. Therefore K has the required form. This proves the theorem.

Corollary 4.4. *Let G be a finite flat O_F-group scheme that admits a filtration by closed group schemes isomorphic to $E[\pi]$. Then*

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

Proof. We proceed by induction with respect to the rank of G. This means that we may assume that we have an exact sequence of 2-group schemes over O_F of the form

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

By Lemma 4.2, the group $\mathrm{Ext}^1_{O_F}(E[\pi], \oplus_{i=1}^r E[\pi^{n_i}])$ is a vector space of dimension r over $\mathbf{F}_2$. It is generated by the extensions e_j for $j = 1, \ldots, r$, where e_j is the extension

$$0 \longrightarrow \bigoplus_{\substack{i=1 \\ i \neq j}}^{r} E[\pi^{n_i}] \oplus E[\pi^{n_j}] \longrightarrow \bigoplus_{\substack{i=1 \\ i \neq j}}^{r} E[\pi^{n_i}] \oplus E[\pi^{n_j+1}] \longrightarrow E[\pi] \longrightarrow 0.$$

By Theorem 4.3, the group of extensions of $E[\pi]$ by $\oplus_{i=1}^r E[\pi^{n_i}]$ in the category $\underline{C}$ form a subgroup of $\mathrm{Ext}^1_{O_F}(E[\pi], \oplus_{i=1}^r E[\pi^{n_i}])$. Since all extensions e_j are extensions in $\underline{C}$, the two extension groups are actually equal. This implies that G is isomorphic to an object in $\underline{C}$ and the corollary follows.

Corollary 4.5. *Every 2-group scheme G over O_F admits a filtration with closed flat subgroup schemes*

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

for which

- *G_2 is diagonalizable; i.e. isomorphic to a product of group schemes of the form μ_{2^k};*
- *G_1/G_2 is a product of group schemes isomorphic to $E[\pi^k]$;*
- *G/G_1 is constant; i.e. isomorphic to a product of group schemes of the form $\mathbf{Z}/2^k\mathbf{Z}$.*

Moreover, the ranks of the subgroup schemes G_1 and G_2 are invariants of the group scheme G and do not depend on the filtration.

Proof. We filter G with closed flat subgroup schemes G_i in such a way that the subquotients are simple. By Theorem 2.3, the simple 2-group schemes are isomorphic to $\mathbf{Z}/2\mathbf{Z}$, μ_2 or $E[\pi]$. By Proposition 3.3 *(i)*, 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 $G_{i+1}/G_i \cong \mu_2$, then we can replace G_i by another subgroup scheme G_i' with $G_{i-1} \hookrightarrow G_i' \hookrightarrow G_{i+1}$ so that $G_i/G_{i-1} \cong \mu_2$ and $G_{i+1}/G_i \cong \mathbf{Z}/2\mathbf{Z}$. Similarly, if for some index i there are successive steps $G_{i-1} \hookrightarrow G_i \hookrightarrow G_{i+1}$ with $G_i/G_{i-1} \cong \mathbf{Z}/2\mathbf{Z}$ and $G_{i+1}/G_i \cong E[\pi]$, we can replace G_i by another subgroup scheme G_i' with $G_{i-1} \hookrightarrow G_i' \hookrightarrow G_{i+1}$ so that $G_i/G_{i-1} \cong E[\pi]$ and $G_{i+1}/G_i \cong \mathbf{Z}/2\mathbf{Z}$. Finally, if for some index i there are successive steps $G_{i-1} \hookrightarrow G_i \hookrightarrow G_{i+1}$ with $G_i/G_{i-1} \cong E[\pi]$ and $G_{i+1}/G_i \cong \mu_2$, we can replace G_i by another subgroup scheme G_i' with $G_{i-1} \hookrightarrow G_i' \hookrightarrow G_{i+1}$ so that $G_i/G_{i-1} \cong \mu_2$ and $G_{i+1}/G_i \cong E[\pi]$.

This implies that G admits a filtration $0 \subset G_2 \subset G_1 \subset G$ with the property that G_2 is filtered by copies of μ_2 only, G_1/G_2 is filtered by copies of $E[\pi]$ only and G/G_1 is filtered by $\mathbf{Z}/2\mathbf{Z}$'s only. It follows from Prop. 3.3 *(ii)* and Galois theory over O_F that G/G_1 is constant. By Prop. 3.3 *(iii)* and Cartier duality G_2 is diagonalizable. Finally, by Cor. 4.4, G_1/G_2 has the required form. This proves the first statement of the corollary.

The second statement follows from the fact that the rank of G/G_1 is equal to the order of the group $G(\overline{\mathbf{F}_2})$ and that the rank of G_2 is equal to the order of $G^{\mathrm{dual}}(\overline{\mathbf{F}_2})$. These ranks are additive in exact sequences.

Proof of Theorem 1.2. Let A be an abelian variety of dimension $g > 0$ over $F = \mathbf{Q}(\sqrt{-2}, \sqrt{-3})$ with good reduction everywhere. As before, we write A for an abelian scheme over O_F with generic fiber isomorphic to A. By Cor. 4.5, the 2-group scheme $A[2]$ admits a filtration

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

Suppose that $G_1 \neq A[2]$. In other words $A[2]$ admits a constant quotient of rank at least 2. By the second statement of Cor. 4.5, the 2-group scheme $A[2^n]$ admits, for each n, a constant quotient C_n of rank at

least 2^n. In other words, there is an exact sequence of 2-group schemes over O_F

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

where H_n is a closed flat subgroup scheme of $A[2^n]$ and C_n is constant of rank at least 2^n. Consider the abelian variety A/H_n. It admits the constant group scheme C_n as a closed subgroup scheme. Reducing A/H_n modulo some prime ideal $\mathfrak{p}$ of O_F with residue field isomorphic to $\mathbf{F}_q$ we find that

$$C_n(\mathbf{F}_q) \hookrightarrow (A/H_n)(\mathbf{F}_q)$$

and hence, by Weil's Theorem

$$2^n \leq (\sqrt{q}+1)^{2g}.$$

This cannot hold for every $n \geq 1$.

Therefore $A[2]/G_1 = 0$. By Cartier duality it follows that $G_2 = 0$ as well. This shows that $A[2]$ and hence every $A[2^n]$ admits a filtration with all simple subquotients isomorphic to $E[\pi]$. It follows from Corollary 4.4 that

$$A[2^n] \cong \bigoplus_{i=1}^{r} E[\pi^{n_i}].$$

Inspection of the geometric points easily shows that $r = g$ and $n_i = 2n$ for each i. Therefore

$$A[2^n] \cong E[\pi^{2n}]^g \cong E^g[2^n].$$

It follows that the 2-adic Tate modules of A and E^g are isomorphic $\mathrm{Gal}(\overline{F}/F)$-modules. By Faltings' theorem [4, Cor. 2 of Thm. 4] this implies that A and E^g areisogenous.

This completes the proof of Theorem 1.2.

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** (1988), 1–46.

[2] Artin M., Algebraization of formal moduli, II. Existence of modifications, Annals Math., **91** (1971), 88–135.

[3] Birch B.J., Cyclotomic fields and Kummer extensions, in "Algebraic Number Theory", (Cassels J.W.S. and Fröhlich A., eds.), Academic Press, London, 1967.

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

[5] Fontaine J.-M., Il n'y a pas de variété abélienne sur **Z**, Invent. Math., **81** (1985), 515–538.

[6] Greither C., Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring, Math. Zeitschrift, **210** (1992), 37–67.

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

[8] Kida M., Reduction of elliptic curves over certain real quadratic number fields, Math. Comp., **68** (1999), 1679–1685.

[9] Martinet J., Petits discriminants des corps de nombres, in "Journées Arithmétiques 1980", (J.V. Armitage, ed.), CUP Lecture Notes Series **56**, Cambridge University Press, Cambridge, 1981.

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

[11] Schoof R., Abelian varieties over cyclotomic fields with good reduction everywhere, in preparation.

[12] Setzer B., Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariants, Illinois J. Math., **25** (1981), 233–245.

[13] Tate J., Finite flat group schemes, in "Modular Forms and Fermat's Last Theorem", (Cornell G., Silverman J. and Stevens G., eds.), Springer-Verlag, New York, 1997.

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

Dipartimento di Matematica
Università di Roma
"Tor Vergata"
I-00133 Roma ITALY
E-mail address: schoof@wins.uva.nl