Preliminary version
August 23, 2010

II Università degli
Studi di Roma

TOR VERGATA

Semistable abelian varieties with good reduction outside 15.

René Schoof

Dipartimento di Matematica
2$^{\mathrm{a}}$ Università di Roma "Tor Vergata"
I-00133 Roma ITALY
Email: schoof@science.uva.nl

Abstract. We show that there are no non-zero semi-stable abelian varieties over $\mathbf{Q}(\sqrt{5})$ with good reduction outside 3 and we show that the only semi-stable abelian varieties over $\mathbf{Q}$ with good reduction outside 15 are, up to isogeny over $\mathbf{Q}$, powers of the Jacobian of the modular curve $X_0(15)$.

1. Introduction.

In his paper [3], Luis Dieulefait gives a proof of Serre's modularity conjecture for the case of odd level and arbitrary weight. By means of an intricate inductive procedure he reduces the issue to the case of Galois representations of level 3 and weight 2, 4 or 6. As explained in [3], these cases are taken care of by the following three theorems respectively.

Theorem 1.1. *There are no non-zero semi-stable abelian varieties over* $\mathbf{Q}$ *with good reduction outside* 3.

Theorem 1.2. *There are no non-zero semi-stable abelian varieties over* $\mathbf{Q}(\sqrt{5})$ *with good reduction outside* 3.

Theorem 1.3. *Every semi-stable abelian variety over* $\mathbf{Q}$ *with good reduction outside* 15 *is isogenous, over* $\mathbf{Q}$*, to a power of the Jacobian of the modular curve* $X_0(15)$.

Theorem 1.1 is due to Brumer and Kramer [2]. In this paper we prove Theorems 1.2 and 1.3, each of which directly imply Theorem 1.1.

In section 2 we discuss extensions of μ_p and $\mathbf{Z}/p\mathbf{Z}$ by one another. These play an important role in this paper. In section 3 we prove Theorem 1.2 and in section 4 we prove Theorem 1.3.

2. Extensions of μ_p and $\mathbf{Z}/p\mathbf{Z}$ by one another.

This section contains preliminary material used in the proofs of Theorems 1.2 and 1.3 given in the next two sections. Let F be a number field and set $\Gamma = \mathrm{Gal}(\overline{F}/F)$. Let S be a finite set of primes of F and let R denote the ring of S-integers.

Lemma 2.1. *Let p be a prime and let G, H be finite flat commutative group schemes over R that are killed by p. Let $\mathrm{Ext}^1_{R,[p]}(G,H)$ denote the subgroup of $\mathrm{Ext}^1_R(G,H)$ consisting of the extensions of G by H that are killed by p. Then there is a natural exact sequence*

$$0 \longrightarrow \mathrm{Ext}^1_{R,[p]}(G,H) \longrightarrow \mathrm{Ext}^1_R(G,H) \longrightarrow \left(\mathrm{Hom}_{\mathrm{ab}}(H(\overline{F}),G(\overline{F}))_\Gamma\right)^\vee .$$

Proof. First we consider extensions of G by H over the quotient field F. Clearly $\mathrm{Ext}^1_{F,[p]}(G,H)$ is the kernel of the natural map $\mathrm{Ext}^1_F(G,H) \longrightarrow \mathrm{Ext}^1_{\mathrm{ab}}(G(\overline{F}),H(\overline{F}))$. Moreover, Γ acts on $\mathrm{Ext}^1_{\mathrm{ab}}(G(\overline{F}),H(\overline{F}))$ and the image of the map is contained in the subgroup of the Γ-invariant extensions. Since $\mathrm{Ext}^1_{\mathrm{ab}}(G(\overline{F}),H(\overline{F}))$ is naturally isomorphic to the $\mathbf{F}_p$-dual of $\mathrm{Hom}_{\mathrm{ab}}(H(\overline{F}),G(\overline{F}))$, the lemma follows, but with the ring R replaced by its quotient field F.

To get the sequence over R, we observe that the following diagram is Cartesian

$$\begin{tikzcd}
\mathrm{Ext}^1_{R,[p]}(G,H) \arrow[r, "\subset"] \arrow[d] & \mathrm{Ext}^1_R(G,H) \arrow[d] \\
\mathrm{Ext}^1_{F,[p]}(G,H) \arrow[r, "\subset"] & \mathrm{Ext}^1_F(G,H)
\end{tikzcd}$$

Indeed, if the generic fiber of a finite flat group scheme over R is killed by p, then so is the group scheme itself. Therefore the induced map between the cokernels of the two horizontal homomorphisms is injective. This implies the lemma.

We first discuss extensions of $\mathbf{Z}/p\mathbf{Z}$ by μ_p. We begin by constructing one such extension over the ring $\mathbf{Z}[\zeta_p]$. Applying the functor $\mathrm{Hom}(\mathbf{Z}/p\mathbf{Z},-)$ to the exact sequence $0 \to \mu_p \to \mu_{p^2} \to \mu_p \to 0$, we obtain an injective homomorphism $\mathrm{Hom}(\mathbf{Z}/p\mathbf{Z},\mu_p) \longrightarrow \mathrm{Ext}^1(\mathbf{Z}/p\mathbf{Z},\mu_p)$. The group $\mathrm{Hom}(\mathbf{Z}/p\mathbf{Z},\mu_p)$ has order p and the image of any non-zero morphism $\mathbf{Z}/p\mathbf{Z} \to \mu_p$ is a non-split extension

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

with group of points $V(\overline{F})$ cyclic of order p^2.

Definition. For every S-unit $\varepsilon \in R^*$ we let G_ε denote the R-group scheme defined in [8, p.418]. It is an extension of $\mathbf{Z}/p\mathbf{Z}$ by μ_p. Its group of points is killed by p and the Galois group $\Gamma = \mathrm{Gal}(\overline{F}/F)$ acts through matrices of the form

$$\begin{pmatrix} \omega & \psi \\ 0 & 1 \end{pmatrix},$$

where ω is the cyclotomic character and, for a suitable choice of a p-th root of unity ζ_p in $\overline{F}$, the cocycle ψ is given by the formula $\zeta_p^{\psi(\sigma)} = \sigma(\sqrt[p]{\varepsilon})/\sqrt[p]{\varepsilon}$ for every $\sigma \in \Gamma$. Two group schemes G_ε and $G_{\varepsilon'}$ are isomorphic if and only if ε/ε' is a p-th power in R^*.

Proposition 2.2. *Let p be a prime and let w_p denote the number of p-th roots of unity in R. Then*

(i) The index of $\mathrm{Ext}^1_{R,[p]}(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ inside $\mathrm{Ext}^1_R(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ is equal to w_p;

(ii) If the class number of R is not divisible by p, then $\mathrm{Ext}^1_{R,[p]}(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ consists of the extensions provided by the group schemes G_ε with $\varepsilon \in R^*$ and the map $\varepsilon \mapsto G_\varepsilon$ induces an isomorphism between the groups R^*/R^{*p} and $\mathrm{Ext}^1_{R,[p]}(\mathbf{Z}/p\mathbf{Z}, \mu_p)$.

Proof. *(i)* A non-trivial homomorphism $\mu_p(\overline{F}) \longrightarrow \mathbf{Z}/p\mathbf{Z}$ is Γ-equivariant if and only if the field F contains the p-th roots of unity. Therefore Lemma 2.1 implies that the index is at most w_p. When $w_p = 1$ we have equality. If $w_p = p$ we observe that the group scheme V constructed above is *not* killed by p and we again have equality. This proves *(i)*.
(ii) By the long exact sequence of cohomology groups associated to the exact sequence $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \to 0$ of sheaves for the fppf topology, we get an exact sequence

$$0 \longrightarrow \mu_p(R) \longrightarrow \mathrm{Ext}^1_R(\mathbf{Z}/p\mathbf{Z}, \mu_p) \longrightarrow H^1_{\text{flat}}(\mathrm{Spec}(R), \mu_p) \longrightarrow 0.$$

The non-trivial classes in $\mathrm{Ext}^1_R(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ that come from $\mu_p(R)$ are all isomorphic to the group scheme V constructed above. By part *(i)*, the group $\mathrm{Ext}^1_{R,[p]}(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ is therefore isomorphic to $H^1_{\text{flat}}(\mathrm{Spec}(R), \mu_p)$. The latter group sits in the exact Kummer sequence

$$0 \longrightarrow R^*/R^{*p} \longrightarrow H^1_{\text{flat}}(\mathrm{Spec}(R), \mu_p) \longrightarrow Cl(R)[p] \longrightarrow 0.$$

The leftmost map is induced by the usual map $F^*/F^{*p} \longrightarrow H^1(\Gamma, \mu_p)$ from Kummer theory. Since p does not divide the class number of R, part *(ii)* follows.

Example. For $R = \mathbf{Z}$ and $S = \emptyset$ there are no non-split extensions of $\mathbf{Z}/p\mathbf{Z}$ by μ_p, except when $p = 2$. In this case $\varepsilon = -1$ and $\mathrm{Ext}^1_{\mathbf{Z}}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ has order 4. The group scheme G_{-1} is the unique such extension that is killed by 2. So it is self-dual. The Galois group acts on its points through matrices of the form

$$\begin{pmatrix} 1 & \omega_2 \\ 0 & 1 \end{pmatrix},$$

where $\omega_2 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_2$ is the character corresponding to the field $\mathbf{Q}(i)$. Explicitly, the Hopf algebra of G_{-1} is $\mathbf{Z}[X, Y]/(X^2 - 1 + 2Y, Y^2 - Y)$. The neutral element is $(1, 0)$ and the addition formula is given by

$$(x, y) + (x', y') \;=\; (xx'(1 - 2yy'), y + y' - 2yy').$$

The subgroup scheme μ_2 is given by the equation $Y = 0$, while the subring $\mathbf{Z}[Y]/(Y^2 - Y)$ gives rise to the morphism $G_{-1} \longrightarrow \mathbf{Z}/2\mathbf{Z}$.

The rest of this section is devoted to extensions of the form

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

We restrict ourselves to the case $p = 2$. This is all we need in the applications.

Proposition 2.3. *Suppose that $2 \notin S$. Then every extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$ over R is killed by 2. If in addition the class number of R is odd and 2 is prime in R, then there is a natural isomorphism*

$$\mathrm{Ext}^1_R(\mu_2, \mathbf{Z}/2\mathbf{Z}) \quad \xrightarrow{\cong} \quad \{\varepsilon \in R^* : \varepsilon \text{ is a square in } F_2^*\}/{R^*}^2.$$

Here F_2 denotes the 2-adic field $R \otimes \mathbf{Q}_2$ and the isomorphism maps an extension G to the unit $\varepsilon \in R^*$ that has the property that the Galois group acts on the points of G through matrices of the form

$$\begin{pmatrix} 1 & \chi \\ 0 & 1 \end{pmatrix}$$

where χ is the character given by the formula $(-1)^{\chi(\sigma)} = \sigma(\sqrt{\varepsilon})/\sqrt{\varepsilon}$ for every $\sigma \in \Gamma$.

Proof. Since μ_2 is connected and $\mathbf{Z}/2\mathbf{Z}$ is étale over $R \otimes \mathbf{Z}_2$, every extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$ over $R \otimes \mathbf{Z}_2$ is split and hence killed by 2. Since $2 \notin S$, the same is true over R. For similar reasons we also have $\mathrm{Hom}_R(\mu_2, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Ext}^1_R(\mu_2, \mathbf{Z}/2\mathbf{Z}) = 0$. Therefore the Mayer-Vietoris sequence in [8, Cor.2.4] gives rise to the exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_R(\mu_2, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1_{R[\frac{1}{2}]}(\mu_2, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1_{F_2}(\mu_2, \mathbf{Z}/2\mathbf{Z})$$

Since the group schemes μ_2 and $\mathbf{Z}/2\mathbf{Z}$ are isomorphic over the rings $R[\frac{1}{2}]$ and F_2, we may switch their roles and compute the Ext-groups using Kummer theory. See [9, section 4] for a similar calculation. A short computation, using the fact that 2 does not divide the class number of R, leads to the following commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mu_2(R[\frac{1}{2}]) \arrow[r] \arrow[d, equal] & \mathrm{Ext}^1_{R[\frac{1}{2}]}(\mu_2, \mathbf{Z}/2\mathbf{Z}) \arrow[r] \arrow[d] & R[\frac{1}{2}]^*/{R[\frac{1}{2}]^*}^2 \arrow[r] \arrow[d] & 0, \\
0 \arrow[r] & \mu_2(F_2) \arrow[r] & \mathrm{Ext}^1_{F_2}(\mu_2, \mathbf{Z}/2\mathbf{Z}) \arrow[r] & F_2^*/{F_2^*}^2 \arrow[r] & 0.
\end{tikzcd}$$

The Snake Lemma implies that $\mathrm{Ext}^1_R(\mu_2, \mathbf{Z}/2\mathbf{Z})$ is isomorphic to the kernel of the rightmost vertical map. Since 2 is prime, this is equal to the kernel of $R^*/{R^*}^2 \longrightarrow F_2^*/{F_2^*}^2$ as required.

We apply Proposition 2.3 to $F = \mathbf{Q}$ and $S = \{3, 5\}$. We have that $R = \mathbf{Z}[\frac{1}{15}]$. The unit group R^* is generated by -1, 3 and 5. The kernel of the map $R^*/{R^*}^2 \longrightarrow \mathbf{Q}_2^*/{\mathbf{Q}_2^*}^2$ is the cyclic group generated by -15. Therefore $\mathrm{Ext}^1_R(\mu_2, \mathbf{Z}/2\mathbf{Z})$ has order 2.

Definition. Let Φ denote the *unique* non-split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\frac{1}{15}]$:

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

Since Φ is unique, it is self-dual. The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $\Phi(\overline{\mathbf{Q}})$ through the unique quadratic character χ of conductor 15. The endomorphism ring of Φ is $\mathbf{F}_2$.

Explicitly, the Hopf algebra of Φ is $\mathbf{Z}[\frac{1}{15}][X,Y]/(X^2-X-2Y, Y^2+2Y)$. The neutral element is $(0,0)$ and the addition formula is given by

$$(x,y)+(x',y') \;=\; (x+x'-2xx'+\tfrac{2}{15}yy'(1-2x)(1-2x'), y+y'+yy').$$

The subgroup scheme $\mathbf{Z}/2\mathbf{Z}$ of Φ is given by the equation $Y=0$, while the subring $\mathbf{Z}[Y]/(Y^2+2Y)$ gives rise to the morphism $\Phi \longrightarrow \mu_2$.

The group scheme Φ is isomorphic to the group scheme of 2-torsion points of the semi-stable elliptic curve [1, p.82] of conductor 15 given by the minimal Weierstrass equation $Y^2+XY+Y = X^3+X^2$. The coordinates of the points of order 2 are $x=-1$ and $x=\frac{-1\pm\sqrt{-15}}{8}$. The Zariski closure of the subgroup generated by the point $(-1,0)$ is the closed subgroup scheme $\mathbf{Z}/2\mathbf{Z}$.

Remark 2.4. Let $F=\mathbf{Q}(\sqrt{5})$ and $S=\{3\}$. The ring of S-integers is $\mathbf{Z}[\eta,\frac{1}{3}]$ where $\eta = \frac{1}{2}(1+\sqrt{5})$. Put $F_2 = F\otimes \mathbf{Q}_2$. Since the kernel of the natural map

$$\mathbf{Z}[\eta,\tfrac{1}{3}]^*/(\mathbf{Z}[\eta,\tfrac{1}{3}]^*)^2 \;\longrightarrow F_2^*/F_2^{*2}.$$

is the *cyclic* group generated by -3, Prop. 2.3 implies that over $\mathbf{Z}[\eta,\frac{1}{3}]$ there is a *unique* non-split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$.

This group scheme is related to Φ as follows. Let $S'=\{3,\sqrt{5}\}$. The ring of S'-integers is $\mathbf{Z}[\eta,\frac{1}{15}]$. Since the kernel of the natural map

$$\mathbf{Z}[\eta,\tfrac{1}{15}]^*/(\mathbf{Z}[\eta,\tfrac{1}{15}]^*)^2 \;\longrightarrow F_2^*/F_2^{*2}.$$

is the cyclic group generated by -3, we see that also over $\mathbf{Z}[\eta,\frac{1}{15}]$ there is a unique non-split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$. It is the base change of the group scheme over $\mathbf{Z}[\eta,\frac{1}{3}]$ constructed above. Since $-15=-3(\sqrt{5})^2$, is also the base change of the $\mathbf{Z}[\frac{1}{15}]$-group scheme Φ.

Remark 2.5. Let $E=\mathbf{Q}(\zeta_3)$ and $S=\{5\}$. The ring of S-integers is $\mathbf{Z}[\zeta_3,\frac{1}{5}]$. Put $E_2=E\otimes\mathbf{Q}_2$. Since the kernel of the natural map

$$\mathbf{Z}[\zeta_3,\tfrac{1}{5}]^*/(\mathbf{Z}[\zeta_3,\tfrac{1}{5}]^*)^2 \;\longrightarrow E_2^*/E_2^{*2}.$$

is the cyclic group generated by 5, Prop. 2.3 implies that over $\mathbf{Z}[\zeta_3,\frac{1}{5}]$ there is a unique non-split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$. It is the base change of the group scheme Φ.

As in Remark 2.4 this group scheme is related to Φ. Indeed, since $-15=5(\sqrt{-3})^2$, its base change to the ring $\mathbf{Z}[\zeta_3,\frac{1}{15}]$ is isomorphic to the base change of the $\mathbf{Z}[\frac{1}{15}]$-group scheme Φ.

In this paper we abuse notation somewhat and denote the various base changes of the group scheme Φ described in Remarks 2.4 and 2.5 by Φ.

3. Proof of Theorem 1.2.

Put $\eta = \frac{1+\sqrt{5}}{2}$ and $F = \mathbf{Q}(\sqrt{5})$. Let $\underline{C}$ be the category of finite flat commutative 2-power order group schemes G over the ring $\mathbf{Z}[\eta, \frac{1}{3}]$ for which $(\sigma - \mathrm{id})^2 = 0$ on $G(\overline{F})$ for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$ in the inertia group of any of the primes lying over 3. Morphisms are morphisms of group schemes.

The category $\underline{C}$ has good stability properties. Duals and subquotients of objects in $\underline{C}$ are again objects of $\underline{C}$. An object G is simple if and ony if the Galois action on its group of points $G(\overline{F})$ is irreducible. For two objects G, G' in $\underline{C}$, the group $\mathrm{Ext}^1(G, G')$ classifies extensions of G by G' in the category of group schemes over $\mathbf{Z}[\eta, \frac{1}{3}]$. The subset $\mathrm{Ext}^1_{\underline{C}}(G, G')$ of such extensions that are themselves objects in $\underline{C}$, is a subgroup. To any exact sequence $0 \longrightarrow G \longrightarrow G' \longrightarrow G'' \longrightarrow 0$ of group schemes in $\underline{C}$ and any H in $\underline{C}$ there is associated a long exact sequence of the form

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_{\underline{C}}(H, G) \longrightarrow \mathrm{Hom}_{\underline{C}}(H, G') \longrightarrow \mathrm{Hom}_{\underline{C}}(H, G'') \longrightarrow \\ \longrightarrow \mathrm{Ext}^1_{\underline{C}}(H, G) \longrightarrow \mathrm{Ext}^1_{\underline{C}}(H, G') \longrightarrow \mathrm{Ext}^1_{\underline{C}}(H, G''). \end{aligned}$$

There is an analogous contravariant exact sequence. For all objects G, H the group $\mathrm{Hom}_{\underline{C}}(H, G)$ is equal to the group $\mathrm{Hom}(H, G)$ of *all* group scheme morphisms $H \longrightarrow G$. In general, the group $\mathrm{Ext}^1_{\underline{C}}(H, G)$ is strictly smaller than the group $\mathrm{Ext}^1(H, G)$ of *all* extensions of H by G. The two extension groups are equal when the Galois action on the points of G and H is unramified at 3. This happens for instance when both G and H are isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2.

The group schemes Φ and G_ε for $\varepsilon \in \mathbf{Z}[\eta, \frac{1}{3}]^*$ defined in section 2, are objects of $\underline{C}$.

Proposition 3.1. *The only simple objects in the category $\underline{C}$ are $\mathbf{Z}/2\mathbf{Z}$ and μ_2.*

Proof. Let G be a simple object. Then G is killed by 2. We multiply G by the group schemes G_ε that were discussed in section 2. The result is still an object of $\underline{C}$ that is killed by 2. The field K generated by the points of G is a Galois extension of F. The square roots of the generators -1, η and 3 of the group $\mathbf{Z}[\eta, \frac{1}{3}]^*$ are in K. Since $(\sigma - \mathrm{id})^2 = 0$ on $G(\overline{F})$ for all σ in any of the inertia subgroups of $\mathrm{Gal}(\overline{F}/F)$ of the primes lying over 3, the field K is tamely ramified at 3 with ramification index ≤ 2. By Fontaine [5, Cor.3.3.2] the root discriminant of K is therefore at most $4\sqrt{15} = 15.49\ldots$. Odlyzko's discriminant bounds [7] imply $[K : \mathbf{Q}] < 76$. We have the inclusions

$$\mathbf{Q} \overset{2}{\subset} F \overset{8}{\subset} k \overset{\leq 4}{\subset} K,$$

where k denotes the field $F(\sqrt{-3}, i, \sqrt{\eta})$. We show that the index of the rightmost inclusion cannot be 3. Note that the unique prime over 3 ramifies in $F \subset k$, so that the extension $k \subset K$ is unramified outside 2. Since η^3 is congruent to 1 modulo $(1 + i)^2$, the relative discriminant of k over $F(\sqrt{-3}, i)$ divides 2. Therefore the root discriminant of k is at most $\sqrt{2} \cdot \sqrt{60} = 10.95\ldots$. Odlyzko's bounds imply that any unramified extension of the latter field has degree $< 26/16$ and hence is trivial. There are two primes lying over 2 in $F(\zeta_3)$, generated by $\zeta_3 + \eta$ and $\zeta_3^{-1} + \eta$ respectively. Since the extension $F(\zeta_3) \subset k$ is totally ramified at both primes over 2, there are also precisely two primes in k lying over 2. The residue fields are both equal to $\mathbf{F}_4$. One checks that the product of the two multiplicative groups is generated by the global units ζ_3 and η. Therefore class field theory implies that the field k does not admit any odd degree non-trivial extension inside K. In particular $[K : k]$ cannot be 3.

It follows that $\mathrm{Gal}(K/F)$ is a 2-group. Therefore it fixes some non-zero point P of the 2-group scheme G we started with. Since G is simple, $G(\overline{F})$ must be generated by P. Therefore G has order 2. Since 2 is prime in the ring $\mathbf{Z}[\eta, \frac{1}{3}]$, the theorem by Oort-Tate [10] implies that G is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2, as required.

Proposition 3.2. *The ring $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$ is an unramified quadratic extension of $\mathbf{Z}[\eta, \frac{1}{3}]$. It does itself not admit any non-trivial 2-power degree unramified Galois extension.*

Proof. Clearly the ring $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$ is an unramified quadratic extension of $\mathbf{Z}[\eta, \frac{1}{3}]$. The quotient field H of the maximal 2-power degree unramified Galois extension of $\mathbf{Z}[\eta, \frac{1}{3}]$ is an extension of F that is unramified outside 3 and the infinite primes. Let $\pi = \mathrm{Gal}(H/K)$. By class field theory, the maximal *abelian* quotient of π is isomorphic to the multiplicative group $\mathbf{F}_9^* \times \mathbf{R}^*/\mathbf{R}^*_{>0} \times \mathbf{R}^*/\mathbf{R}^*_{>0}$ modulo the image of the global units of $\mathbf{Z}[\eta]$. It is easy to see that the units -1 and η of $\mathbf{Z}[\eta]$ generate a subgroup of index 2. Therefore π/π' has order 2. Group theory implies then that π itself is also cyclic of order 2. This proves the proposition.

Let $\omega_3 : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathbf{F}_2$ denote the restriction of the unique Dirichlet character of $\mathbf{Q}$ of conductor 3.

Corollary 3.3. *The $\mathbf{F}_2$-vector space $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ of extensions of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\eta, \frac{1}{3}]$ has dimension 2. It is generated by the class of $\mathbf{Z}/4\mathbf{Z}$ and by an extension killed by 2 on which the Galois group acts via matrices of the form*

$$\begin{pmatrix} 1 & \omega_3 \\ 0 & 1 \end{pmatrix}.$$

Proof. The action of the Galois group on the points of an étale group scheme is unramified and étale group schemes are characterized by this action. The corollary follows from the fact that the maximal unramified 2-power degree Galois extension of $\mathbf{Z}[\eta, \frac{1}{3}]$ is the ring $\mathbf{Z}[\eta, \frac{1}{3}, \zeta_3]$.

Corollary 3.4. *Any extension of group schemes $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\eta, \frac{1}{3}]$ becomes constant over $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$. Any extension of group schemes μ_2 over $\mathbf{Z}[\eta, \frac{1}{3}]$ becomes diagonalizable over $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$.*

Proof. This follows inductively from Prop. 3.2 and Cartier duality.

The group of upper triangular 3×3-matrices over $\mathbf{F}_2$ is isomorphic to the dihedral group D_4. Consider a subgroup

$$\Gamma \subset \{\begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{F}_2\}.$$

The maps $\Gamma \longrightarrow \mathbf{F}_2$ given by $\gamma \mapsto a$ and $\gamma \mapsto b$ are group homomorphisms. The following elementary lemma is repeatedly used in the sequel.

Lemma 3.5. *Let Γ be as above and let $N \subset \Gamma$ be a normal subgroup of order at most 2. Then either $a(N) = b(N) = 0$ or one of a, b vanishes on Γ.*

Proof. If neither a nor b vanishes on Γ, then Γ must contain a matrix of the form

$$\begin{pmatrix} 1 & 1 & c \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

This matrix has order 4. It follows that Γ is either the full dihedral group or its unique cyclic subgroup of order 4. Either group has a unique normal subgroup of order 2. It is given by $a = b = 0$.

This proves the lemma.

Let Φ denote the group scheme over $\mathbf{Z}[\eta, \frac{1}{3}]$ that was introduced in Remark 2.4. It is an object of the category $\underline{C}$. The action of $\mathrm{Gal}(\overline{F}/F)$ on the points of Φ is through the character ω_3.

Proposition 3.6. *We have*

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

Proof. By Cartier duality it suffices to show that $\mathrm{Ext}^1_{\underline{C}}(\Phi, \mathbf{Z}/2\mathbf{Z})$ vanishes. Consider an extension in the category $\underline{C}$

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

Then G is killed by 4. The extension gives rise to an extension of the form

$$0 \longrightarrow C \longrightarrow G \longrightarrow \mu_2 \longrightarrow 0.$$

where C is an extension of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$. If $C(\overline{F})$ were cyclic, any automorphism of $G(\overline{F})$ would necessarily act trivially on $G(\overline{F})$ modulo the subgroup $2C(\overline{F})$. Since the Galois action on $\Phi(\overline{F})$ is non-trivial, this cannot happen. Therefore C is killed by 2. It follows that G is killed by 2 over the completion at the prime 2. This implies that G itself is also killed by 2. By Remark 2.4 the Galois group acts on $G(\overline{F})$ through matrices of the form

$$\begin{pmatrix} 1 & \psi & a \\ 0 & 1 & \omega_3 \\ 0 & 0 & 1 \end{pmatrix}.$$

Since C is étale, the character $\psi : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathbf{F}_2$ is unramified outside 3. Since G is an object of $\underline{C}$, any prime over 3 is tamely ramified with inertia group of order ≤ 2. Therefore Lemma 3.5 applies with Γ equal to the decomposition group of a prime over 3 and N its inertia subgroup: since $\omega_3(N) \neq 0$, we have $\psi(\Gamma) = 0$. It follows that ψ is unramified at all finite primes. Since the narrow class number of F is 1, class field theory implies $\psi = 0$.

To finish the proof, we consider the exact sequence

$$\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z}) \xrightarrow{g} \mathrm{Ext}^1(\mu_2,\mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1(\Phi,\mathbf{Z}/2\mathbf{Z}) \xrightarrow{h} \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z}).$$

The map h sends the class of G to the class of the extension determined by ψ. By Remark 2.4 the map g is an isomorphism of two groups of order 2. It follows that h is injective. This implies the proposition.

Proposition 3.7. *The natural maps*

$$\begin{aligned}\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z},\Phi) &\longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mu_2),\\ \mathrm{Ext}^1_{\underline{C}}(\Phi,\mu_2) &\longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mu_2)\end{aligned}$$

are both zero.

Proof. By Cartier duality it suffices to deal with the first map. Since the Galois covariants of $\mathrm{Hom}_{\mathrm{ab}}(\Phi(\overline{E}),\mathbf{Z}/2\mathbf{Z})$ have order 2, Lemma 2.1 implies that $\mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z},\Phi)$ is generated by the extensions that are killed by 2 and by the image of the class of $\mathbf{Z}/4\mathbf{Z}$. The latter is mapped to zero because the sequence

$$\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z},\Phi) \longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mu_2).$$

is exact. Therefore it suffices to show that any extension in $\underline{C}$ of the form

$$0 \longrightarrow \Phi \longrightarrow G \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0,$$

that is *killed by* 2, maps to zero in $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z},\mu_2)$.

The Galois group acts on the points of G via matrices of the form

$$\begin{pmatrix} 1 & \omega_3 & a\\ 0 & 1 & \psi\\ 0 & 0 & 1\end{pmatrix}$$

The homomorphism $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z},\Phi) \longrightarrow \mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z},\mu_2)$ maps G to the quotient of G by the subgroup scheme $\mathbf{Z}/2\mathbf{Z}$ of Φ. This is an extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_2. By Proposition 2.2 it is a group scheme of the form G_ε for some ε in $\mathbf{Z}[\eta,\frac{1}{3}]^* = \langle -1,3,\eta\rangle$. We want to show that the corresponding character, i.e. the character ψ given by $(-1)^{\psi(\sigma)} = \sigma(\sqrt{\varepsilon})/\sqrt{\varepsilon}$, vanishes.

Let K denote the field generated by the points of G and let $\Gamma \subset \mathrm{Gal}(K/F)$ denote a decomposition group of a prime over 3. Since G is an object of $\underline{C}$, the ramification indices of the primes over 3 are at most 2. Therefore Lemma 3.5 applies to Γ with N equal to its inertia subgroup: since ω_3 is ramified at 3, the character ψ is trivial on Γ. We conclude that 3 splits in $F(\sqrt{\varepsilon})$, so that ε is a square modulo 3.

Since $\varepsilon = \pm\eta$ are not squares in the residue field $\mathbf{F}_9$, we have therefore $\varepsilon = \pm 1$. If $\varepsilon = -1$, then the field K is a quadratic extension of $F(i,\sqrt{-3})$. Locally at 2 the extension of $\mathbf{Z}/2\mathbf{Z}$ by Φ looks like

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

Therefore the ramification index of the prime 2 in the extension $F \subset K$ is equal to 2. It follows that K is everywhere unramified over $F(i, \sqrt{-3}) = \mathbf{Q}(i, \sqrt{-3}, \sqrt{5})$. A standard computation involving Odlyzko's discriminant bounds shows that the latter field does not admit any non-trivial everywhere unramified extension. Contradiction. It follows that $\varepsilon = 1$ and hence $\psi = 0$ as required.

This proves the proposition.

Next we compute the long exact sequences that we obtain by applying the bifunctor $\mathrm{Hom}_{\underline{C}}(-,-)$, in both arguments, to the exact sequence $0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow \Phi \longrightarrow \mu_2 \longrightarrow 0$. By Corollary 3.3 and Propositions 3.6 and 3.7 we obtain the following commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & & & 0 \arrow[d] \\
 & & 0 \arrow[r] \arrow[d] & \mathbf{F}_2 \arrow[d] \\
 & 0 \arrow[r] \arrow[d] & \mathrm{Ext}^1_{\underline{C}}(\Phi, \Phi) \arrow[r] \arrow[d] & \mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \Phi) \arrow[d] \\
0 \arrow[r] & \mathbf{F}_2 \arrow[r] & \mathrm{Ext}^1_{\underline{C}}(\Phi, \mu_2) \arrow[r] & 0
\end{tikzcd}$$

Here the "$\mathbf{F}_2$" in the upper right corner is the image of the map from $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ to $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$. It is the image of the class of $\mathbf{Z}/4\mathbf{Z}$. It is also the unique non-split extension of μ_2 by $\mathbf{Z}/4\mathbf{Z}$. Similarly, the "$\mathbf{F}_2$" in the lower left corner denotes the extension of Φ by μ_2 that is the image of the class of μ_4 in $\mathrm{Ext}^1(\mu_2, \mu_2)$. It is also the unique non-split extension of μ_4 by $\mathbf{Z}/2\mathbf{Z}$. It follows at once that in the category $\underline{C}$ there is at most one non-trivial extension of Φ by itself. We prove the following stronger statement.

Proposition 3.8. *We have*

$$\mathrm{Ext}^1_{\underline{C}}(\Phi, \Phi) \;=\; 0.$$

Proof. If a non-trivial extension exists, it maps to the image of the class of $\mathbf{Z}/4\mathbf{Z}$ in $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$ and to the image of μ_4 in $\mathrm{Ext}^1_{\underline{C}}(\Phi, \mu_2)$. This means that the group $G(\overline{F})$ of a non-trivial extension

$$0 \longrightarrow \Phi \longrightarrow G \longrightarrow \Phi \longrightarrow 0,$$

is of type 4×4. It follows that $\Phi(\overline{F})$ is precisely equal to $2G(\overline{F})$. Proposition 3.7 implies that the natural map $\mathrm{Ext}^1_{\underline{C}}(\Phi, \Phi) \longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ is *zero.* Therefore Corollary 3.3 and its Cartier dual show that we have an extension of the form

$$0 \longrightarrow \mathbf{Z}/4\mathbf{Z} \longrightarrow G \longrightarrow \mu_4 \longrightarrow 0$$

The Galois group acts on the points of G via matrices of the form

$$\begin{pmatrix} 1 & a \\ 0 & \omega_4 \end{pmatrix}$$

where ω_4 is the character that gives the action on the group μ_4 of 4th roots of unity and $a : \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathbf{Z}/4\mathbf{Z}$ is a 1-cocycle with the property that the restriction of a to the absolute Galois group of $F(i)$ is a character satisfying $2a = \omega_3$. In particular, a has order 4 and the field K generated by the points of G contains $F(i)$ and has degree 8 over F.

Since the extension $0 \to \mathbf{Z}/4\mathbf{Z} \to G \to \mu_4 \to 0$ is split over the completion of O_F at 2, the prime $1+i$ of $F(i)$ is split in K. In particular, the extension $F(i) \subset K$ is unramified outside 3. Since $F(i)$ admits no non-trivial everywhere unramified extensions, class field theory implies that $\mathrm{Gal}(K/F(i))$ is a quotient of the multiplicative group $(O_{F(i)}/3O_{F(i)})^*$ by the subgroup generated by $O^*_{F(i)}$ and by the generator $1+i$ of the prime lying over 2. There are two primes lying over 3, each with residue field $\mathbf{F}_9$. One checks that the quotient of $\mathbf{F}_9^* \times \mathbf{F}_9^*$ by the global unit η and the element $1+i$, has order 2 rather than 4. It follows that $[K : F] \neq 8$ and we obtain a contradiction.

It follows that $\mathrm{Ext}^1_{\underline{C}}(\Phi, \Phi)$ is trivial, as required.

Proof of Theorem 1.2. Let A be a semistable abelian variety over $F = \mathbf{Q}(\sqrt{5})$ with good reduction outside 3. A result by Grothendieck [6, Cor.3.5.2] implies that for any σ in an inertia group of a prime lying over 3, the endomorphism $(\sigma - \mathrm{id})^2$ acts as zero on the 2^n-torsion subgroup schemes $A[2^n]$ for $n \geq 1$. Therefore the latter are objects of the category $\underline{C}$. Proposition 3.6 implies that each $A[2^n]$ admits a filtration of the form

$$0 \underbrace{\subset}_{\mu_2\text{'s}} M_n \underbrace{\subset}_{\Phi\text{'s}} N_n \underbrace{\subset}_{\mathbf{Z}/2\mathbf{Z}\text{'s}} A[2^n]$$

where M_n is filtered by copies of μ_2, the quotient N_n/M_n is filtered by copies of Φ and $A[2^n]/N_n$ is filtered by copies of $\mathbf{Z}/2\mathbf{Z}$.

By Corollary 3.4 the étale group schemes $M_n^\vee$ and $A[2^n]/N_n$ become *constant* over the ring $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$. Choose a residue field $\mathbf{F}_q$ of this ring. The groups of points of $A[2^n]/N_n$ and $M_n^\vee$ map injectively to the group of $\mathbf{F}_q$-rational points of the abelian varieties A/N_n and A^{dual}/N'_n respectively. Here $N'_n = \ker(A[2^n]^\vee \to M_n^\vee)$.

The abelian varieties A/N_n and A^{dual}/N'_n are all isogenous to A. Therefore they have the same number of points as A over $\mathbf{F}_q$. It follows that $\#M_n$ and $\#(A[2^n]/N_n)$ are at most $\#A(\mathbf{F}_q)$. In particular, they remain bounded as n grows. By Proposition 3.8 the group schemes N_n/M_n are killed by 2. Therefore $A[2^n]$ is killed by some positive integer that does not depend on n. This is impossible unless $A = 0$.

This proves Theorem 1.2.

4. Proof of Theorem 1.3.

Let $\underline{B}$ be the category of finite flat commutative 2-power order group schemes over $\mathbf{Z}[\frac{1}{15}]$ on which $(\sigma - \mathrm{id})^2 = 0$ for all σ in the inertia subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ of any of the primes lying over 3 or 5. We write S for the set of primes $\{3, 5\}$. The category $\underline{B}$ enjoys the same stability properties as the category $\underline{C}$ of the previous section.

The following group theoretical fact is used in the proof of Prop. 4.2. We only apply it for $n = 3$.

Lemma 4.1. *Let $n \geq 3$. Then the symmetric group S_n is not the commutator subgroup of any group.*

Proof. Let G be a group and let G' be its commutator subgroup. Conjugation gives rise to a homomorphism $G \longrightarrow \mathrm{Aut}(G')$. On the one hand it maps G' to the commutator subgroup of $\mathrm{Aut}(G')$. On the other hand its image is the group $\mathrm{Inn}(G')$ of inner automorphisms of G'. Therefore, if a group H is the commutator subgroup of some group, we must have $\mathrm{Inn}(H) \subset \mathrm{Aut}(H)'$.

This condition is not satisfied for $H = S_n$ when $n \geq 3$. We leave the verification to the reader.

Proposition 4.2. *The only simple objects in the category $\underline{B}$ are $\mathbf{Z}/2\mathbf{Z}$ and μ_2.*

Proof. Let G be a simple object. As in the proof of Prop. 3.1, we multiply G by the group schemes G_ε of section 2, where ε runs through the group $\mathbf{Z}[\frac{1}{15}]^*$ modulo squares. Let K be the field generated by the points of G. Put $\Gamma = \mathrm{Gal}(K/\mathbf{Q})$. The square roots of -1, 3 and 5 are contained in K. The field K is tamely ramified at 3 and 5 with ramification index at most 2. By Fontaine's theorem [5, Cor.3.3.2] the root discriminant of K is therefore strictly smaller than $4\sqrt{15} = 15.49\ldots$. Odlyzko's discriminant bounds [7] imply $[K : \mathbf{Q}] < 76$. We have the inclusions

$$\mathbf{Q} \overset{8}{\subset} k \overset{\leq 9}{\subset} K.$$

where $k = \mathbf{Q}(\sqrt{5}, \sqrt{-3}, i)$. The extension $k \subset K$ is unramified outside 2. Therefore, by the Kronecker-Weber Theorem any larger extension inside K that is *abelian* over $\mathbf{Q}$, necessarily contains $\mathbf{Q}(\zeta_8)$. Since the root discriminant of $\mathbf{Q}(\zeta_8)$ is equal to 4, this is impossible. Therefore k is the maximal abelian extension of $\mathbf{Q}$ inside K and $\mathrm{Gal}(K/k)$ is equal to the commutator subgroup Γ'. This group is solvable and we study Γ'/Γ''. We already saw in the proof of Proposition 3.7 that k admits no non-trivial unramified extensions. In k there are two primes lying over 2. Writing $\eta = (1 + \sqrt{5})/2$, one prime contains $\zeta_3 + \eta$ while the other contains $\zeta_3^{-1} + \eta$. Their product is $(1 + i)$. Since the global units ζ_3 and η generate the group $(O_k/(1 + i)O_k)^* \cong \mathbf{F}_4^* \times \mathbf{F}_4^*$, class field theory implies that $[\Gamma' : \Gamma'']$ is a power of 2.

If $[\Gamma' : \Gamma''] = 1$, 4 or 8, it is immediate that Γ is a 2-group. If $[\Gamma' : \Gamma''] = 2$, we have $\#\Gamma'' \leq 4$. If $\#\Gamma'' = 3$, we have $\Gamma' \cong S_3$ which is impossible by Lemma 4.1. Therefore $\#\Gamma''$ is necessarily a power of 2 and Γ is a 2-group. So Γ has fixed points in the irreducible 2-power order Galois module $G(\overline{F})$ we started with. It follows that G has order 2. By the Oort-Tate Theorem [10] the group scheme G is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2 as required.

Since the Galois extension $\mathbf{Q} \subset \mathbf{Q}(\zeta_{15})$ is *not* cyclic, the same is true for the maximal 2-power degree unramified Galois extension of $\mathbf{Z}[\frac{1}{15}]$. As a consequence the group $\mathrm{Ext}^1_{\mathbf{Z}[\frac{1}{15}]}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ is relatively large. It has order 8. This affects the size of other extension groups, in particular the ones involving the group scheme Φ of section 2. A computation similar to the one performed in the proof of Prop. 3.8 shows that $\mathrm{Ext}^1_{\underline{B}}(\Phi, \Phi)$ has dimension 2 over $\mathbf{F}_2$. It is generated by the 4-torsion of the Jacobian of the modular curve $X_0(15)$ and an unramified quadratic twist of $\Phi \times \Phi$.

Since it is essential for our method that $\mathrm{Ext}^1_{\underline{B}}(\Phi,\Phi)$ be 1-dimensional, we make a base change. We move over to the ring $\mathbf{Z}[\zeta_3,\frac{1}{15}]$ and modify the category $\underline{B}$ accordingly. Put $E=\mathbf{Q}(\zeta_3)$ and let S denote the set of $\mathbf{Z}[\zeta_3]$-primes $\{\sqrt{-3},5\}$.

Definition. Let $\underline{D}$ be the category of commutative finite flat 2-power order group schemes over $\mathbf{Z}[\zeta_3,\frac{1}{15}]$ with the property that $(\sigma-\mathrm{id})^2=0$ on $G(\overline{\mathbf{Q}})$ for all σ contained in the inertia subgroup of $\mathrm{Gal}(\overline{E}/E)$ of any of the primes lying over primes in S.

The category $\underline{D}$ has the same stability properties as the category $\underline{C}$ of the previous section. The group schemes Φ and G_ε for $\varepsilon\in\mathbf{Z}[\zeta_3,\frac{1}{15}]^*$ of section 2 are objects of $\underline{D}$.

Proposition 4.3. *Let R denote the ring of integers of the ray class field of conductor $5\sqrt{-3}$ of $E=\mathbf{Q}(\zeta_3)$. Then the ring $R[\frac{1}{15}]$ is an unramified cyclic degree 8 extension of $\mathbf{Z}[\zeta_3,\frac{1}{15}]$. It does itself not admit any non-trivial 2-power degree unramified Galois extension.*

Proof. Let π denote the Galois group of the maximal unramified 2-power degree extension of $\mathbf{Z}[\zeta_3,\frac{1}{15}]$. Then π/π' is isomorphic to the ray class group of E of conductor $5\sqrt{-3}$. This shows that $R[\frac{1}{15}]$ is the maximal unramified *abelian* 2-power degree extension of $\mathbf{Z}[\zeta_3,\frac{1}{15}]$. This ray class group is isomorphic to $\mathbf{F}_3^*\times\mathbf{F}_{25}^*$ modulo the global unit $-\zeta_3$. Therefore it is *cyclic* and group theory implies then that π itself is also cyclic. It follows that $R[\frac{1}{15}]$ does not admit any non-trivial 2-power degree unramified Galois extension, as required.

Corollary 4.4. *The $\mathbf{F}_2$-vector space $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z})$ of extensions of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\zeta_3,\frac{1}{15}]$ has dimension 2. It is generated by $\mathbf{Z}/4\mathbf{Z}$ and an extension killed by 2 on which the Galois group acts via matrices of the form*

$$\begin{pmatrix}1 & \chi_5\\ 0 & 1\end{pmatrix}.$$

Here $\chi_5:\mathrm{Gal}(\overline{E}/E)\longrightarrow\mathbf{F}_2$ is the restriction of the unique quadratic Dirichlet character of conductor 5. It corresponds to the extension $E\subset E(\sqrt{5})$.

Proof. It suffices to observe that $E(\sqrt{5})$ is the unique quadratic extension of E that is unramified outside S. Now apply Prop.4.3.

Corollary 4.5. *Any extension of group schemes $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\zeta_3,\frac{1}{15}]$ is constant over $R[\frac{1}{15}]$. Similarly, any extension of group schemes μ_2 over $\mathbf{Z}[\zeta_3,\frac{1}{15}]$ is diagonalizable over $R[\frac{1}{15}]$.*

Proof. This follows from Proposition 4.3 and Cartier duality.

Let Φ denote the group scheme over $\mathbf{Z}[\zeta_3,\frac{1}{5}]$ that was introduced in Remark 2.5. It is an object of the category $\underline{D}$. The action of $\mathrm{Gal}(\overline{E}/E)$ on the points of Φ is through the character χ_5. The following proposition is analogous to Proposition 3.6.

Proposition 4.6. *We have*

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

Proof. By Cartier duality it suffices to show that the left hand side group vanishes. Consider an extension in the category $\underline{D}$

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

It gives rise to an extension

$$0 \longrightarrow C \longrightarrow G \longrightarrow \mu_2 \longrightarrow 0.$$

where C is an extension of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$. If $C(\overline{E})$ were cyclic, then any automorphism of $G(\overline{E})$ necessarily acts trivially on $G(\overline{E})$ modulo the subgroup $2C(\overline{E})$. Since the Galois action on $\Phi(\overline{E})$ is non-trivial, this cannot happen. Therefore C and hence G itself are killed by 2. So the Galois group acts through matrices of the form

$$\begin{pmatrix} 1 & \psi & a \\ 0 & 1 & \chi_5 \\ 0 & 0 & 1 \end{pmatrix}$$

Here ψ is a character of $\mathrm{Gal}(\overline{E}/E)$. Since C is étale, ψ is unramified outside $\sqrt{-3}$ and 5. We apply Lemma 3.5 first with Γ equal to a decomposition group of a prime over 5 and N its inertia subgroup. Note that $\#N \leq 2$ because G is an object of $\underline{D}$. We find that $\Gamma \subset \ker \psi$. Then we apply Lemma 3.5 to the decomposition group of a prime over $\sqrt{-3}$ and its inertia subgroup and we see that ψ is unramified at $\sqrt{-3}$.

So, ψ is everywhere unramified. Therefore it is zero. Consider the exact sequence

$$\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{g} \mathrm{Ext}^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1(\Phi, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{h} \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}).$$

The map h sends the class of G to the class of the extension determined by ψ. By Remark 2.5 the map g is an isomorphism of two groups of order 2. It follows that h is injective. Now the proposition follows.

The following proposition is analogous to Proposition 3.7. The group scheme G_{-1} was discussed in section 2. See the example there.

Proposition 4.7. *The images of both natural maps*

$$\begin{aligned} \mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z}, \Phi) &\longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2), \\ \mathrm{Ext}^1_{\underline{D}}(\Phi, \mu_2) &\longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2) \end{aligned}$$

are contained in the subgroup generated by the class $[G_{-1}]$.

Proof. By Cartier duality it suffices to give a proof for the first map. Since the Galois covariants of $\mathrm{Hom}_{\mathrm{ab}}(\Phi(\overline{E}), \mathbf{Z}/2\mathbf{Z})$ have order 2, Lemma 2.1 implies that $\mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$ is generated by the extensions that are killed by 2 and by the image of the class of $\mathbf{Z}/4\mathbf{Z}$. The latter is mapped to zero because the sequence

$$\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z}, \Phi) \longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2).$$

is exact. Therefore it suffices to show that any extension in $\underline{D}$ of the form

$$0 \longrightarrow \Phi \longrightarrow G \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0,$$

that is *killed by* 2, maps to the subgroup generated by $[G_{-1}]$ in $\mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$.

The Galois group acts on the points of G via matrices of the form

$$\begin{pmatrix} 1 & \chi_5 & a \\ 0 & 1 & \psi \\ 0 & 0 & 1 \end{pmatrix}.$$

The extension G is mapped to the class of G_ε in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$, where ε is a unit in $\mathbf{Z}[\zeta_3, \frac{1}{15}] = \langle -1, \sqrt{-3}, 5\rangle$ and the corresponding quadratic character is ψ. Since G is an object of $\underline{D}$, the inertia subgroup of any prime lying over $\sqrt{5}$ has order ≤ 2 and Lemma 3.5 applies to the decomposition group. As χ_5 is ramified, we deduce that the prime $\sqrt{5}$ splits in the field cut out by ψ. Since $\varepsilon = \pm\sqrt{-3}$ are not squares in the residue field $\mathbf{F}_{25}$, we have $\varepsilon = \pm 1$. The class in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ associated to $\varepsilon = -1$ is precisely $[G_{-1}]$.

This proves the proposition.

Remark 4.8. If there were no group scheme H in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ that maps to the class $[G_{-1}]$ in $\mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$, then the proof of Prop. 4.11 below would be trivial. However, such a group scheme does exist and is unique. The Galois group acts on its points through matrices of the form

$$\begin{pmatrix} 1 & \chi_5 & a \\ 0 & 1 & \omega_2 \\ 0 & 0 & 1 \end{pmatrix},$$

where $\omega_2 : \mathrm{Gal}(\overline{E}/E) \longrightarrow \mathbf{F}_2$ is the character corresponding to the field $E(i)$. It follows from the proof of Proposition 4.6 that the field K generated by the points of H is a quadratic extension of $E(i, \sqrt{5})$, unramified outside the primes lying over 3. There is only one such field. It is the ray class field of conductor $\sqrt{-3}$ of the field $\mathbf{Q}(\sqrt{-5}, \zeta_3)$.

Next we compute the long exact sequences that we obtain by applying the bifunctor $\mathrm{Hom}_{\underline{D}}(-,-)$, in both arguments, to the exact sequence $0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow \Phi \longrightarrow \mu_2 \longrightarrow 0$. As a consequence of the previous propositions, we have the following commutative diagram with exact rows and columns

$$\begin{tikzcd}
 & & & 0 \arrow[d] \\
 & & 0 \arrow[r] \arrow[d] & \mathbf{F}_2 \arrow[d] \\
 & 0 \arrow[r] \arrow[d] & \mathrm{Ext}^1_{\underline{D}}(\Phi, \Phi) \arrow[r] \arrow[d] & \mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z}, \Phi) \arrow[d] \\
0 \arrow[r] & \mathbf{F}_2 \arrow[r] & \mathrm{Ext}^1_{\underline{D}}(\Phi, \mu_2) \arrow[r] & \mathbf{F}_2
\end{tikzcd}$$

Here the "$\mathbf{F}_2$" in the upper right corner denotes the extension of $\mathbf{Z}/2\mathbf{Z}$ by Φ that is the image of the class of $\mathbf{Z}/4\mathbf{Z}$ in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z})$. It is also the unique non-split extension of $\mathbf{Z}/4\mathbf{Z}$ by μ_2. Similarly, the "$\mathbf{F}_2$" in the lower left corner denotes the extension of Φ by μ_2 that is the image of the class of μ_4 in $\mathrm{Ext}^1(\mu_2,\mu_2)$. It is also the unique non-split extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_4. The "$\mathbf{F}_2$" in the lower right corner is the extension $[G_{-1}]$ in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mu_2)$.

It follows that the $\mathbf{F}_2$-dimension of $\mathrm{Ext}^1_{\underline{D}}(\Phi,\Phi)$ is at most 2. On the other hand the dimension is at least 1, because the 4-torsion of the elliptic curve $Y^2+XY+Y=X^3+X^2$ of section 2, is a non-trivial extension of Φ by Φ in $\underline{D}$. We now proceed to show that $\mathrm{Ext}^1_{\underline{D}}(\Phi,\Phi)$ has dimension exactly 1.

Lemma 4.9. *Let G be an extension of Φ by Φ. Then the underlying group structure of $G(\overline{E})$ is not of type $4\times 2\times 2$.*

Proof. Suppose it is. Let $e_1\in G(\overline{E})$ be a point of order 4. Choose e_2 of order 2 so that $2e_1$ and e_2 are a basis for the group of points of the subspace $\Phi(\overline{E})$ of $G(\overline{E})$. Finally, choose $e_3\in G(\overline{E})$ of order 2 so that e_1,e_3 are a basis for the group $G(\overline{E})/\Phi(\overline{E})$. Every point in the $\Phi(\overline{E})$-coset of e_3 has order 2, while the points in the cosets of e_1 and e_1+e_3 all have order 4. This implies that $\mathrm{Gal}(\overline{E}/E)$ preserves the coset of e_3 and switches those of e_1 and e_1+e_3. Since $\Phi(\overline{E})$ is generated by $2e_1$ and e_2, it follows that $\mathrm{Gal}(\overline{E}/E)$ fixes $2e_1$ and hence switches e_2 and $2e_1+e_2$.

Over $\mathbf{Z}_2$ the group scheme Φ is a split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$ and the group scheme $G/\Phi\cong\Phi$ admits a unique morphism onto its maximal étale quotient $\mathbf{Z}/2\mathbf{Z}$. Let N denote the quotient of the kernel of the composition $G\to G/\Phi\to\mathbf{Z}/2\mathbf{Z}$ by the connected component of the subgroup scheme Φ of G. Let E_2 be the completion of E at 2. For any embedding $\overline{E}\hookrightarrow\overline{E}_2$, either e_1 or e_1+e_3 is contained in $N(\overline{E}_2)$. In the first case the natural map $\langle e_1\rangle\to N(\overline{E}_2)$ is an isomorphism. In the second case the map $\langle e_1+e_3\rangle\to N(\overline{E}_2)$ is an isomorphism. This shows that the group $N(\overline{E}_2)$ is cyclic of order 4. On the other hand, there is an exact sequence of $\mathbf{Z}_2$-group schemes

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

Since this sequence is split over $\mathbf{Z}_2$, the group scheme N is killed by 2. Contradiction.

This proves the lemma.

Corollary 4.10. *The group $\mathrm{Ext}^1_{\underline{D}}(\Phi,\Phi)$ is generated by the subgroup of extensions that are killed by 2 and by the extension of Φ by Φ realized by the 4-torsion of the elliptic curve with Weierstrass equation $Y^2+XY+Y=X^3+X^2$.*

Proof. The index "[2]" indicates the subgroup of extensions that are killed by 2. The square

$$\begin{tikzcd}
\mathrm{Ext}^1_{\underline{D},[2]}(\Phi,\Phi) \arrow[r, hook] \arrow[d, "\subset"] & \mathrm{Ext}^1_{\underline{D},[2]}(\mathbf{Z}/2\mathbf{Z},\Phi) \arrow[d, "\subset"] \\
\mathrm{Ext}^1_{\underline{D}}(\Phi,\Phi) \arrow[r, hook] & \mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z},\Phi)
\end{tikzcd}$$

is Cartesian. This follows from Lemma 4.9 and the fact that extensions in $\mathrm{Ext}^1_{\underline{D}}(\Phi,\Phi)$ with underlying group of type 4×4, map to extensions in $\mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z},\Phi)$ that are not killed by 2. It follows that the induced map between the cokernels of the vertical maps is injective We already saw in the proof Proposition 4.7 that Lemma 2.1 implies that the cokernel of the rightmost arrow has order 2. This proves the corollary

Proposition 4.11. *We have*

$$\dim_{\mathbf{F}_2}\mathrm{Ext}^1_{\underline{D}}(\Phi,\Phi) \;=\; 1.$$

Proof. By Lemma 4.9 and Corollary 4.10 it suffices to show that extensions in $\underline{D}$ of the form

$$0 \longrightarrow \Phi \longrightarrow G \longrightarrow \Phi \longrightarrow 0,$$

that are *killed by* 2 are necessarily split.

Let G be such an extension. The map $\mathrm{Ext}^1_{\underline{D}}(\Phi,\Phi) \longrightarrow \mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z},\Phi)$ sends G to the kernel of the composed morphism $G \to \Phi \to \mu_2$. The 2-dimensional $\mathbf{F}_2$-vector space $\mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z},\Phi)$ is generated by the class of the group scheme H of Remark 4.8 and by the image of $\mathbf{Z}/4\mathbf{Z}$ under the natural map $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z},\mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z},\Phi)$. The only non-trivial extension class $\mathrm{Ext}^1_{\underline{D}}(\mathbf{Z}/2\mathbf{Z},\Phi)$ that is killed by 2, is the one represented by H. It follows that the class of G maps to the class of H. Similarly, the map $\mathrm{Ext}^1_{\underline{D}}(\Phi,\Phi) \longrightarrow \mathrm{Ext}^1_{\underline{D}}(\Phi,\mu_2)$ sends G to its quotient by the subgroup scheme $\mathbf{Z}/2\mathbf{Z}$ of its subgroup scheme Φ. The class of G maps to the class of the Cartier dual $H^\vee$ in $\mathrm{Ext}^1_{\underline{D}}(\Phi,\mu_2)$.

Let $\{e_1,e_2,e_3\}$ be a basis of $H^\vee(\overline{E})$ with the property that $\{e_1\}$ and $\{e_1,e_2\}$ are bases of its unqiue 1- and 2-dimensional sub-Galois modules respectively. Then the Galois group acts on $H^\vee(\overline{E})$ through matrices of the form

$$\begin{pmatrix} 1 & \omega_2 & a+\mu\omega_2+\lambda\chi_5+\chi_5\omega_2 \\ 0 & 1 & \chi_5 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \text{for certain } \lambda,\mu\in\mathbf{F}_2.$$

This follows from a short computation using the 3×3 matrix that describes the Galois action on $H(\overline{E})$ given in Remark 4.8. It follows that the Galois group acts on $G(\overline{E})$ through matrices of the form

$$\begin{pmatrix} 1 & \chi_5 & a & b \\ 0 & 1 & \omega_2 & a+\mu\omega_2+\lambda\chi_5+\chi_5\omega_2 \\ 0 & 0 & 1 & \chi_5 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad \text{for certain } \lambda,\mu\in\mathbf{F}_2.$$

Let L be the field generated by the points of G. It contains the field K generated by the points of H (or equivalently of $H^\vee$).

Claim. *We have* $L = K$.

Since G is an object of the category $\underline{D}$ that is killed by 2, the ramification indices over E of the primes of L lying over $\sqrt{-3}$ and 5 are at most 2. Let O_2 be the completion of

$\mathbf{Z}[\zeta_3]$ at 2. Over O_2 the group scheme Φ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mu_2$. This implies that the ramification indices of the primes in L lying over 2 are at most and hence equal to 2. It follows that $E(\sqrt{5}, i) \subset L$ is an abelian exponent 2 extension that is *unramified* outside the primes lying over 3. We saw already in the proof of Proposition 3.7 that $E(\sqrt{5}, i) = \mathbf{Q}(\sqrt{-3}, \sqrt{5}, i)$ admits no non-trivial unramified extensions. The two primes of $E(\sqrt{5}, i)$ lying over 3 have residue fields isomorphic to $\mathbf{F}_9$. Since the quotient of $\mathbf{F}_9^* \times \mathbf{F}_9^*$ by the global unit $\eta = (1+\sqrt{5})/2$ is cyclic, class field theory implies that L is a cyclic extension of $E(\sqrt{5}, i)$. It follows that L has degree 2 over $E(\sqrt{5}, i)$ and hence $L = K$ as required.

As a consequence the map

$$\begin{pmatrix} 1 & \chi_5 & a & b \\ 0 & 1 & \omega_2 & a + \mu\omega_2 + \lambda\chi_5 + \chi_5\omega_2 \\ 0 & 0 & 1 & \chi_5 \\ 0 & 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & \chi_5 & a \\ 0 & 1 & \omega_2 \\ 0 & 0 & 1 \end{pmatrix}$$

is an isomorphism of groups. The fact that the 3×3-matrices with $\omega_2 = 0$ have order 2 implies the same for the 4×4-matrices and this easily implies that $\lambda = 0$. The subgroup $\mathrm{Gal}(K/F(\sqrt{5}))$ of $\mathrm{Gal}(K/E)$ consists of automorphisms whose corresponding matrices have $\chi_5 = 0$. One checks that these are the matrices

$$\begin{pmatrix} 1 & 0 & \multicolumn{2}{c}{M} \\ 0 & 1 & & \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

with

$$M = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & \mu+1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & \beta \\ 1 & \mu \end{pmatrix}, \quad \begin{pmatrix} 1 & \beta+\mu+1 \\ 1 & \mu+1 \end{pmatrix}$$

for some $\beta \in \mathbf{F}_2$. Since the rightmost two matrices have the same determinant, we see that the number of automorphisms $\sigma \in \mathrm{Gal}(K/E(\sqrt{5}))$ for which the rank of the 4×4-matrix corresponding to $\sigma - \mathrm{id}$ is equal to 2, is *odd.*

Let $\Gamma = \mathrm{Gal}(K/E)$. Recall that Γ is isomorphic to the dihedral group of order 8.

Claim. *The decomposition subgroup $\Gamma_2 \subset \Gamma$ of any prime lying over 2 has order 2.*

Proof of the claim. Since 2 splits in $E(\sqrt{5})$ and is ramified in K, the group Γ_2 has order 2 or 4. Suppose that $\#\Gamma_2 = 4$. Then $\Gamma_2 = \mathrm{Gal}(K/E(\sqrt{5}))$ and as we have seen above, the number of automorphisms $\sigma \in \Gamma_2$ for which the rank of the 4×4-matrix corresponding to $\sigma - \mathrm{id}$ is equal to 2, is *odd.*

On the other hand, let O_2 denote the completion of $\mathbf{Z}[\zeta_3]$ at 2. Over O_2 we have $\Phi \cong \mathbf{Z}/2\mathbf{Z} \times \mu_2$. Therefore $\Gamma_2 = \mathrm{Gal}(\overline{E}_2/E_2)$ acts on the points of G through matrices of the form

$$\begin{pmatrix} 1 & 0 & \gamma & 0 \\ 0 & 1 & \omega_2 & \gamma' \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Here γ and γ' are unramified characters. If one of γ, γ' is trivial, then all $\sigma \in \mathrm{Gal}(L/E(\sqrt{5}))$ have the property that the rank of the matrix corresponding to $\sigma - \mathrm{id}$ is at most 1. This is a contradiction. If *both* γ, γ' are non-trivial, then they are equal and Γ_2 acts through matrices of the form

$$\begin{pmatrix} 1 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{M}} \\ 0 & 1 & & \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

with

$$M = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Since exactly two of these matrices are invertible, exactly *two* $\sigma \in \Gamma_2$ have the property that the rank of the 4×4-matrix corresponding to $\sigma - \mathrm{id}$ is equal to 2. Contradiction. So we have $\#\Gamma_2 = 2$ and the claim follows.

The second claim implies that the two primes over 2 in $E(i, \sqrt{5})$ split in the quadratic extension K. But they don't. Indeed, consider the element $\sqrt{-3} + \sqrt{-5}$ of the subfield $E(\sqrt{-5})$. Since its norm to E is -2, it generates one of the prime ideals over 2. The other is generated by $\sqrt{-3} - \sqrt{-5}$. Since both primes are principal ideals, they split in the Hilbert class field $E(\sqrt{5}, i)$ of $E(\sqrt{-5})$. If they were even to split in K, then both primes would admit generators that are congruent to 1 (mod $\sqrt{-3}$). This follows from Remark 4.8: the field K is the ray class field of $E(\sqrt{-5})$ of conductor $\sqrt{-3}$. In other words, we would have $u(\sqrt{-3} + \sqrt{-5}) \equiv 1 \pmod{\sqrt{-3}}$ for some unit u in $E(\sqrt{-5})$. Since the unit group of $E(\sqrt{-5})$ is generated by -1 and $4 + \sqrt{15} = 4 + \sqrt{-3}\sqrt{-5}$, this implies that

$$\pm(4 + \sqrt{-3}\sqrt{-5})^m(\sqrt{-3} + \sqrt{-5}) \equiv 1 \pmod{\sqrt{-3}}, \qquad \text{for some } m \in \mathbf{Z}.$$

However, the left hand side is congruent to $\pm\sqrt{-5}$ modulo $\sqrt{-3}$, so that this is impossible for any $a \in \mathbf{Z}$.

This proves the proposition.

Proof of Theorem 1.3. Let A be a semistable abelian variety over $\mathbf{Q}$ with good reduction outside 15. By Grothendieck [6, Cor.3.5.2], for every $n \geq 1$ the 2^n-torsion subgroup schemes $A[2^n]$ are objects of the category $\underline{B}$ over the ring $\mathbf{Z}[\frac{1}{15}]$. Proposition 4.2 implies then that for every $n \geq 1$, the subgroup scheme $A[2^n]$ admits a filtration with simple subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2. We now make a base change to the ring $\mathbf{Z}[\zeta_3, \frac{1}{15}]$. The group schemes $A[2^n]$ are objects of the category $\underline{D}$. By Remark 2.5 and Proposition 4.7 we obtain for any $n \geq 1$ over $\mathbf{Z}[\zeta_3, \frac{1}{15}]$ a filtration of $A[2^n]$ as follows.

$$0 \underbrace{\subset}_{\mu_2\text{'s}} M_n \underbrace{\subset}_{\Phi\text{'s}} N_n \underbrace{\subset}_{\mathbf{Z}/2\mathbf{Z}\text{'s}} A[2^n]$$

where M_n is filtered by copies of μ_2, the quotient N_n/M_n is filtered by copies of the group scheme Φ and $A[2^n]/N_n$ is filtered by copies of $\mathbf{Z}/2\mathbf{Z}$.

By Corollary 4.5 the étale group schemes $M_n^\vee$ and $A[2^n]/N_n$ become *constant* over the ring $R[\frac{1}{15}]$. Therefore, for every residue field $\mathbf{F}_q$ of this ring, the groups of points of $M_n^\vee$

and $A[2^n]/N_n$ map injectively to the group of $\mathbf{F}_q$-rational points of the abelian varieties A/N_n and A^{dual}/N'_n. Here $N'_n = \ker(A[2^n]^\vee \to M_n^\vee)$. As in the proof of Theorem 1.2 it follows that $\#M_n$ and $\#(A[2^n]/N_n)$ remain bounded as n grows.

Let J denote the elliptic curve given by the Weierstrass equation $Y^2 + XY + Y = X^3 + X^2$. Then the group scheme $J[2]$ is isomorphic to Φ and $J[4]$ is a non-trivial extension in $\underline{D}$ of Φ by Φ. It is unique by Proposition 4.11. Since $\text{End}(\Phi)$ is isomorphic to the finite field $\mathbf{F}_2$, one proves by induction [9, section 8] that any object in $\underline{D}$ that admits a filtration with flat closed subgroup schemes with successive quotients isomorphic to Φ, is isomorphic to

$$\bigoplus_{i=1}^{t} J[2^{m_i}],$$

for certain integers $m_i > 0$. We apply this to the subquotients N_n/M_n of $A[2^n]$. For every $n \geq 0$ the underlying group of $A[2^n]$ is isomorphic to $(\mathbf{Z}/2^n\mathbf{Z})^{2g}$ where $g = \dim A$. This implies that for all $n \geq 0$ there are morphisms of group schemes

$$A[2^n] \quad \xrightarrow{f_n} \quad J[2^n]^g$$

whose kernels and cokernels are bounded as n grows. The morphisms f_n are not necessarily compatible, but there is a *cofinal* compatible system. Taking the limit we obtain an exact sequence of 2-divisible groups

$$0 \longrightarrow H \longrightarrow A_{\text{div}} \longrightarrow J^g_{\text{div}} \longrightarrow 0.$$

where H is a finite 2-power order subgroup scheme of A. By Faltings' theorem [4] the abelian varieties A and J^g are isogenous over E. Lemmas 4.12 and 4.13 below imply that A and J^g are also isogenous over $\mathbf{Q}$. Since J is isogenous to the Jacobian of the modular curve $X_0(15)$, Theorem 1.3 follows.

Lemma 4.12. *Let Γ be a group and let M and N be $\mathbf{Z}$-torsionfree $\mathbf{Z}[\Gamma]$-modules. Let H be a subgroup of Γ of finite index and let $I \subset \Gamma$ be a subset for which*

- *for every $\sigma \in I$ the element $(\sigma - 1)^2$ annihilates M and N;*
- *the group Γ is generated by H and I.*

Then every H-linear morphism $f : M \longrightarrow N$ is actually Γ-linear.

Proof. Let $f : M \longrightarrow N$ be H-linear. Let $\sigma \in I$. Then $\sigma^k \in H$ for some positive integer k. We have

$$\sigma^k = (1 + (\sigma - 1))^k \equiv 1 + k(\sigma - 1) \ (\text{mod } (\sigma - 1)^2), \qquad \text{in the ring } \mathbf{Z}[\Gamma].$$

Let $f : M \longrightarrow N$ be H-linear and let $m \in M$. We have $f((1-k)m) = (1-k)f(m)$ and $f(\sigma^k m) = \sigma^k f(m)$. Since $(\sigma - 1)^2$ kills both M and N, it follows that $kf(\sigma m) = k\sigma f(m)$. Since N is torsion-free, it follows that $f(\sigma m) = \sigma f(m)$. This implies that f is Γ-linear, as required.

Proposition 4.13. *Let F be a number field and let A, B be two semi-stable abelian varieties. Let K be a finite extension of F that does not contain any proper subextension* *that is unramified outside the set S of primes of bad reduction of A and B. Then A and B are isogenous over K if and only if they are isogenous over F.*

Proof. Pick a prime l. Any K-isogeny $A \longrightarrow B$ induces a Galois isomorphism between the Tate modules. More precisely, it gives rise to an isomorphism $f : V_l(A) \longrightarrow V_l(B)$ of $\mathbf{Q}_l[H]$-modules. Here H denotes $\mathrm{Gal}(\overline{F}/K)$. By assumption, the union I of the inertia groups in $G = \mathrm{Gal}(\overline{F}/F)$ of any of the primes lying over S has the property that I and H generate G. Since A and B are semi-stable abelian varieties, Grothendieck's result [6, Cor.3.5.2] implies that the conditions of Lemma 4.9 are both satisfied. Therefore $f : V_l(A) \longrightarrow V_l(B)$ is G-linear. Faltings' theorem implies then that A and B are isogenous over F.

Bibliography

[1] Birch, B. and Kuyk, W. Eds.: *Modular functions in one variable* IV. Lecture Notes in Math. **476**, Springer-Verlag, New York 1975.

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

[3] Dieulefait, L.: Remarks on Serre's modularity conjecture, http://arxiv.org/abs/math/0603439.

[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] Grothendieck, A.: Modèles de Néron et monodromie, Exp IX in *Groupes de monodromie en géométrie algébrique*, SGA 7, Part I, Lecture Notes in Mathematics **288** (1971) Springer-Verlag, New York.

[7] Odlyzko, A.M.: Unconditional bounds for discriminants, 1976. `http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table2`

[8] Schoof, R.: Abelian varieties over cyclotomic fields with good reduction everywhere, *Math. Annalen* **325** (2003), 413–448.

[9] Schoof, R.: Abelian varieties over **Q** with bad reduction in one prime only, *Compositio Math.* **141** (2005), 847–868.

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