On the modular curve $X_0(23)$

René Schoof

Abstract. The Jacobian $J_0(23)$ of the modular curve $X_0(23)$ is a semi-stable abelian variety over $\mathbf{Q}$ with good reduction outside 23. It is simple. We prove that every simple semi-stable abelian variety over $\mathbf{Q}$ with good reduction outside 23 is isogenous over $\mathbf{Q}$ to $J_0(23)$.

2010 Mathematics Subject Classification. Primary 14L15; Secondary 11G18, 11R37.
Keywords. Group schemes, modular curves, algebraic number fields

1. Introduction

The modular curve $X_0(23)$ parametrizes elliptic curves together with a subgroup of order 23. It has genus 2 and is defined over $\mathbf{Q}$. An explicit equation for $X_0(23)$ is given by

$$y^2 = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7).$$

Its Jacobian variety $J_0(23)$ is a simple semi-stable abelian variety over $\mathbf{Q}$ admitting good reduction at every prime different from 23. Our main result is that it is the only such abelian variety.

Theorem 1.1. *Every simple semi-stable abelian variety over* $\mathbf{Q}$ *with good reduction outside* 23 *is isogenous over* $\mathbf{Q}$ *to* $J_0(23)$.

Our result follows from a study of the 2-power order torsion points of semi-stable abelian varieties A over $\mathbf{Q}$ with good reduction outside 23. The first sections of this paper also apply to primes p different from 23. For any odd prime p we study the category $\underline{C}$ of finite flat commutative 2-power order group schemes G over $\mathbf{Z}[\frac{1}{p}]$ with the property that for each σ in the inertia group of any of the primes lying over p, the endomorphism $(\sigma - 1)^2$ annihilates the group of points of G. By a theorem of Grothendieck, for every $k \geq 1$, the subgroup schemes of 2^k-torsion points of semi-stable abelian varieties A over $\mathbf{Q}$ with good reduction outside p are objects of $\underline{C}$. In particular, the subgroup schemes of 2^k-torsion points of the Jacobian $J_0(p)$ of the modular curve $X_0(p)$ are objects of $\underline{C}$. Theorems 3.7 and 4.4 give a rough classification of the objects in $\underline{C}$.

For $p = 23$ it follows from the classification that the 2-divisible group of a semi-stable abelian variety A with good reduction outside 23 is isogenous to a product of copies of the 2-divisible group of $J_0(23)$. Faltings' theorem implies then that A is isogenous to a power of $J_0(23)$. So, when A is simple, it is isogenous to $J_0(23)$.

In our proof an important role is played by the delicate structure of the group scheme $J_0(23)[2]$ of the 2-torsion points of $J_0(23)$. In section 4 we show that this order 16 group scheme is an extension of $V^\vee$ by V

$$0 \longrightarrow V \longrightarrow J_0(23)[2] \longrightarrow V^\vee \longrightarrow 0.$$

Here V denotes the constant group scheme $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ twisted by the action of $\Delta = \mathrm{Gal}(H/\mathbf{Q})$, where H is the Hilbert class field of $\mathbf{Q}(\sqrt{-23})$. The group Δ is isomorphic to the symmetric group S_3 and the group scheme $V^\vee$ is the Cartier dual of V.

We show that the extension does *not split* over $\mathbf{Z}[\frac{1}{23}]$. The group scheme $J_0(23)[2]$ even has irreducible features in the sense that its endomorphism ring R over $\mathbf{Z}[\frac{1}{23}]$ is a field. In fact, the Hecke algebra $\mathbf{T}$ is isomorphic to $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$ and the natural map from $\mathbf{T}/2\mathbf{T} \cong \mathbf{F}_4$ to R is a ring isomorphism. On the other hand the extension splits over $\mathbf{Q}$ and over all completions of $\mathbf{Z}[\frac{1}{23}]$.

The paper is organized as follows. We describe in sections 2–4 the objects of the category $\underline{C}$ as precisely as we can. In section 2 we construct for $p \equiv \pm 1 \pmod 8$ the unique non-split extension Φ of μ_2 by $\mathbf{Z}/2\mathbf{Z}$ over the ring $\mathbf{Z}[\frac{1}{p}]$. The group scheme Φ is an object of $\underline{C}$. In sections 3 and 4 we make more assumptions on the prime p. These are satisfied by $p = 23$ and probably by infinitely many other primes. We construct the simple group schemes V and $V^\vee$ and the unique non-split extension Ψ of $V^\vee$ by V over the ring $\mathbf{Z}[\frac{1}{p}]$. The group schemes V, $V^\vee$ and Ψ are objects of $\underline{C}$. In section 2–4 we determine the various possible extensions of the group schemes $\mathbf{Z}/2\mathbf{Z}$, μ_2, Φ, V, $V^\vee$ and Ψ by one another. The main results are Theorems 2.7, 3.7, 4.4 and 4.8.

In section 5 we specialize to the case $p = 23$. In this case the group scheme Ψ is isomorphic to $J_0(23)[2]$. We show that the simple objects in the category $\underline{C}$ are the group schemes $\mathbf{Z}/2\mathbf{Z}$, μ_2, V and $V^\vee$. For $p = 23$, Theorems 2.7, 3.7, 4.4 and 4.8 lead to a classification of the objects of $\underline{C}$, which is fine enough for our purposes. Finally, in section 6 we consider the modular curve $X_0(23)$ and prove Theorem 1.1.

I thank Dick Gross and Harvard university for their hospitality in the spring of 2012 and Brian Conrad for explaining to me how to deal with the spectral sequence of Prop. 3.5.

2. The category $\underline{C}$ and the group schemes $\mathbf{Z}/2\mathbf{Z}$ and μ_2.

In this section p is an odd prime. Let $\underline{Gr}$ be the category of finite flat commutative 2-power order group schemes over the ring $\mathbf{Z}[\frac{1}{p}]$. For every abelian variety A over $\mathbf{Q}$ with good reduction outside p, the group schemes $A[2^k]$ of 2^k-torsion points, are objects of $\underline{Gr}$. So are the constant group schemes $\mathbf{Z}/2^k\mathbf{Z}$ and their Cartier duals μ_{2^k}. The group schemes $\mathbf{Z}/2\mathbf{Z}$ and μ_2 are *simple* objects of $\underline{C}$.

In this section we study various extensions of the group schemes $\mathbf{Z}/2\mathbf{Z}$ and μ_2 by one another. Group schemes that are successive extensions of copies of $\mathbf{Z}/2\mathbf{Z}$

make up a full subcategory of $\underline{Gr}$. The same is true for the group schemes that are successive extensions of copies of μ_2. These categories are abelian. In order to describe them, we let F be the maximal 2-power degree subfield of $\mathbf{Q}(\zeta_p)$ and put $\pi = \mathrm{Gal}(F/\mathbf{Q})$.

Proposition 2.1. *The functor $G \mapsto G(\overline{\mathbf{Q}})$ is an equivalence of categories between the full subcategory of $\underline{Gr}$ of group schemes that are successive extensions of $\mathbf{Z}/2\mathbf{Z}$ and the category of finite $\mathbf{Z}_2[\pi]$-modules. In particular, any object G becomes constant over the ring $O_F[\frac{1}{p}]$.*

Similarly, the functor $G \mapsto \mathrm{Hom}(G^\vee(\overline{\mathbf{Q}}), \mathbf{Q}/\mathbf{Z})$ is an equivalence of categories between the full subcategory of $\underline{Gr}$ of group schemes that are successive extensions of μ_2 and the category of finite $\mathbf{Z}_2[\pi]$-modules. In particular, any object G becomes diagonalizable over the ring $O_F[\frac{1}{p}]$.

Proof. Let G be a successive extension of group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$. Then G is étale. The Galois group acts on $G(\overline{\mathbf{Q}})$ through the Galois group Π of the maximal 2-power degree unramified Galois extension of $\mathbf{Z}[\frac{1}{p}]$. By the Kronecker-Weber Theorem the quotient of Π by its commutator subgroup Π' is isomorphic to $\pi = \mathrm{Gal}(F/\mathbf{Q})$. Since the Galois group of $\mathbf{Q}(\zeta_p)$ over $\mathbf{Q}$ is cyclic, so is π. It follows that Π is also cyclic, so that $\Pi = \pi$. Therefore $G(\overline{\mathbf{Q}})$ is a $\mathbf{Z}_2[\pi]$-module. The result now follows from Galois theory.

The second statement follows by Cartier duality. This proves the proposition. $\square$

Corollary 2.2. *Over the ring $\mathbf{Z}[\frac{1}{p}]$ we have the following.*

(a) the group $\mathrm{Ext}^1_{\underline{Gr}}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ has $\mathbf{F}_2$-dimension 2 and is generated by the class of $\mathbf{Z}/4\mathbf{Z}$ and an étale group scheme killed by 2 on which the Galois group acts through matrices of the form

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

where $\chi_p : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{F}_2$ is the character that corresponds to the quadratic subfield of $\mathbf{Q}(\zeta_p)$;

(b) the group $\mathrm{Ext}^1_{\underline{Gr}}(\mu_2, \mu_2)$ has $\mathbf{F}_2$-dimension 2 and is generated by the class of μ_4 and a group scheme killed by 2 on which the Galois group acts as in part (a).

Proof. It is easy to determine the structure of the $\mathbf{Z}_2[\pi]$-modules of order 4. The result then follows from Proposition 2.1. $\square$

Proposition 2.3. *The group $\mathrm{Ext}^1_{\underline{Gr}}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ of extensions of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 over the ring $\mathbf{Z}[\frac{1}{p}]$ has dimension 3. It is generated by a group scheme with trivial Galois action and underlying group cyclic of order 4 and by the extensions*

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

with $u = -1$ or p.

Proof. This is Kummer theory. See [11, Prop. 2.2] for the proof and for the definition of the group scheme G_u. Recall that G_u is an order 4 group scheme that is killed by 2. The Galois group acts on its points through matrices of the form

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

where for $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ the entry $\psi(\sigma) \in \mathbf{F}_2$ is given by $\sigma(\sqrt{u})/\sqrt{u} = (-1)^{\psi(\sigma)}$. □

The group schemes described in Proposition 2.3 play a minor role in the proof of the main result of this paper. On the other hand the extension that appears in the next proposition is important.

Proposition 2.4. *If* $p \equiv \pm 3 \pmod 8$, *any extension*

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

splits over $\mathbf{Z}[\frac{1}{p}]$. *If* $p \equiv \pm 1 \pmod 8$, *there exist a unique non-split extension. This group scheme is killed by* 2 *and the Galois group acts on its points through matrices of the form*

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

Here χ_p *is the character of Corollary 2.2.*

Proof. By [11, Prop. 2.3] the group $\mathrm{Ext}^1_{\underline{Gr}}(\mu_2, \mathbf{Z}/2\mathbf{Z})$ is isomorphic to the kernel of the homomorphism

$$\mathbf{Z}[\tfrac{1}{p}]^*/\mathbf{Z}[\tfrac{1}{p}]^{*2} \longrightarrow \mathbf{Q}_2^*/\mathbf{Q}_2^{*2}.$$

The group on the left is generated by -1 and p. The kernel is trivial when $p \equiv \pm 3 \pmod 8$, while it has order 2 when $p \equiv \pm 1 \pmod 8$. □

Definition. For $p \equiv \pm 1 \pmod 8$, let Φ denote the non-trivial extension of Proposition 2.4:

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

By uniqueness, the group scheme Φ is self-dual. Since $\mathbf{Z}/2\mathbf{Z}$ is the unique closed subgroup scheme of Φ of order 2 and since there are no non-zero homomorphisms $\mu_2 \longrightarrow \mathbf{Z}/2\mathbf{Z}$, the ring $\mathrm{End}(\Phi)$ is isomorphic to $\mathbf{F}_2$.

Applying the functor $\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z}, -)$ to the exact sequence $0 \to \mathbf{Z}/2\mathbf{Z} \to \Phi \to \mu_2 \to 0$, we obtain the exact sequence

$$0 \longrightarrow \mathrm{Hom}(\mathbf{Z}/2\mathbf{Z}, \mu_2) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$$

The image of the unique non-zero morphism $\mathbf{Z}/2\mathbf{Z} \to \mu_2$ is an extension of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$ that is killed by 2. It is the one described in Corollary 2.2 (a). Therefore the image of $\mathrm{Ext}^1_{\underline{Gr}}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ inside $\mathrm{Ext}^1_{\underline{Gr}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$ has $\mathbf{F}_2$-dimension 1. It is generated by the image of the class of $\mathbf{Z}/4\mathbf{Z}$.

Definition. For $p \equiv \pm 1 \pmod 8$, let Υ be the extension

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

in $\mathrm{Ext}^1_{\underline{Gr}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$ that is the image of the class of $\mathbf{Z}/4\mathbf{Z}$ in $\mathrm{Ext}^1_{\underline{Gr}}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$. A consideration of the Cartesian diagram

$$\begin{array}{ccc} \mathbf{Z}/2\mathbf{Z} & \longrightarrow & \mathbf{Z}/4\mathbf{Z} \\ \downarrow & & \downarrow \\ \Phi & \longrightarrow & \Upsilon \end{array}$$

shows that the group scheme Υ is also an extension of μ_2 by $\mathbf{Z}/4\mathbf{Z}$. Similarly, the image of the map $\mathrm{Ext}^1_{\underline{Gr}}(\mu_2, \mu_2) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(\Phi, \mu_2)$ is generated by the Cartier dual $\Upsilon^\vee$ of Υ. The group scheme $\Upsilon^\vee$ is also an extension of μ_4 by $\mathbf{Z}/2\mathbf{Z}$.

Definition. Let $\underline{C}$ be the full subcategory of those objects G of the category $\underline{Gr}$ that have the property that for every σ in an inertia subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ of any of the primes lying over p, the endomorphism $(\sigma - 1)^2$ acts as zero on the group of points $G(\overline{\mathbf{Q}})$.

When A is a semistable abelian variety over $\mathbf{Q}$ with good reduction outside p, a theorem of A. Grothendieck [5, Cor.3.5.2] asserts that for every $k \geq 1$, the group schemes $A[2^k]$ are actually objects of $\underline{C}$. So are the constant group schemes $\mathbf{Z}/2^k\mathbf{Z}$, their Cartier duals μ_{2^k}, the group schemes G_u of Proposition 2.3 and the group schemes Φ and Υ introduced above.

The category $\underline{C}$ is not abelian, but it has good stability properties. Closed flat subgroup schemes of objects in $\underline{C}$ are again objects of $\underline{C}$ and so are quotients by such subgroup schemes. The Cartier dual $G^\vee$ of an object G in $\underline{C}$ is again an object in $\underline{C}$. An object G is simple if and only if the Galois action on its group of points $G(\overline{\mathbf{Q}})$ is irreducible. For two objects G, G' in $\underline{C}$, the group $\mathrm{Ext}^1_{\underline{Gr}}(G, G')$ classifies extensions of G by G' in the category $\underline{Gr}$. The subset $\mathrm{Ext}^1_{\underline{C}}(G, G')$ of such extensions that are themselves objects in $\underline{C}$, is a subgroup [10, section 2]. In general, the group $\mathrm{Ext}^1_{\underline{C}}(H, G)$ is strictly smaller than the group $\mathrm{Ext}^1_{\underline{Gr}}(H, G)$ 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 p. This happens for instance when both G and H are isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2.

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

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

There is an analogous contravariant exact sequence.

Proposition 2.5. *Let $p \equiv \pm 1 \pmod 8$ be prime. Then*

(a) we have

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

(b) we have

$$\dim_{\mathbf{F}_2} \mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \Phi) \;=\; \dim_{\mathbf{F}_2} \mathrm{Ext}^1_{\underline{C}}(\Phi, \mu_2) \;=\; \begin{cases} 2, & \textit{if } p \equiv 1 \pmod 8; \\ 1, & \textit{if } p \equiv -1 \pmod 8). \end{cases}$$

Proof. (a) See [11, Prop.3.6]. By Cartier duality it suffices to prove that the first group is zero. Suppose we have an extension in the category $\underline{C}$

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

The composite morphism $G \to \Phi \to \mu_2$ gives rise to an exact sequence 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 $\mathbf{Z}/2\mathbf{Z}$. As in [11, Prop.3.6] one shows that C is killed by 2. It follows that G is killed by 2 and that the Galois group acts on $G(\overline{\mathbf{Q}})$ through matrices of the form

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

Since C is étale, ψ is unramified at 2. Since G is an object of $\underline{C}$ that is killed by 2, we have $\sigma^2 = 1$ for each σ in the inertia group of any of the primes lying over p. Therefore the ramification index of p is at most 2. By [11, Lemma 3.5] the character ψ is then also unramified at p. It follows that ψ is everywhere unramified and hence trivial. Therefore the map h in the exact sequence

$$\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{g} \mathrm{Ext}^1_{\underline{C}}(\mu_2, \mathbf{Z}/2\mathbf{Z}) \to \mathrm{Ext}^1_{\underline{C}}(\Phi, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{h} \mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$$

maps the extension class of G to zero. Since the map g is an isomorphism, h is injective and the result follows.

(b) By Cartier duality it suffices to deal with the group $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$. By the exactness of the Ext-sequence, the extension Υ of $\mathbf{Z}/2\mathbf{Z}$ by Φ defined above generates the kernel of the natural map

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

Since Υ is not killed by 2, the map

$$\mathrm{Ext}^1_{\underline{C},[2]}(\mathbf{Z}/2\mathbf{Z}, \Phi) \overset{\phi}{\hookrightarrow} \mathrm{Ext}^1_{\underline{C},[2]}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$$

is injective. Here $\mathrm{Ext}^1_{\underline{C},[2]}(\mathbf{Z}/2\mathbf{Z}, \Phi)$ denotes the subgroup of extensions of $\mathbf{Z}/2\mathbf{Z}$ by Φ that are killed by 2. By [11, Lemma 2.1] it has index ≤ 2 inside $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$. The existence of the group scheme Υ shows that the index is *equal* to 2. It suffices therefore to show that $\mathrm{Ext}^1_{\underline{C},[2]}(\mathbf{Z}/2\mathbf{Z}, \Phi)$ has $\mathbf{F}_2$-dimension 1 or 0 depending on whether $p \equiv 1 \pmod 8$ or not. Proposition 2.4 implies then that $\mathrm{Ext}^1_{\underline{C},[2]}(\mathbf{Z}/2\mathbf{Z},\Phi)$ has $\mathbf{F}_2$-dimension at most 1.

In order to decide what the precise dimension is, consider an extension

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

with G killed by 2. The Galois group acts on $G(\overline{\mathbf{Q}})$ through matrices of the form

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

and ϕ maps the class of G to the extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 that is determined by ψ. Since G is an object of $\underline{C}$, it follows from [11, Lemma 3.5] that ψ is unramified at p. By Prop. 2.3 we either have $\psi = 0$ or ψ cuts out the field $\mathbf{Q}(i)$. In the first case G is split by the injectivity of ϕ. In the second case we note that over $\mathbf{Z}_2$ the group scheme Φ is isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mu_2$. It follows that the ramification indices of the primes lying over 2 is at most 2. Therefore $a : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(i,\sqrt{p})) \longrightarrow \mathbf{F}_2$ is everywhere unramified. Since a is non-trivial, this means that $\mathbf{Q}(i,\sqrt{p})$ admits an unramified quadratic extension. This is the case if and only if $p \equiv 1 \pmod 8$. See for instance [6, section 8].

This proves the proposition when $p \equiv -1 \pmod 8$. The fact that for $p \equiv 1 \pmod 8$, the category $\underline{C}$ actually contains a non-split extension of $\mathbf{Z}/2\mathbf{Z}$ by Φ that is killed by 2 is not relevant for the proof of the main result of this paper. It follows from the description of 2-power order group schemes over $\mathbf{Z}[\frac{1}{p}]$ given in [9, Prop.2.3]. $\square$

Proposition 2.6. *Suppose that* $p \equiv \pm 1 \pmod 8$. *Then the extension* Υ *of* $\mathbf{Z}/2\mathbf{Z}$ *by* Φ *is in the image of the natural map*

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

if and only if $p \equiv \pm 1 \pmod{16}$.

Proof. Let G be an extension in $\mathrm{Ext}^1_{\underline{C}}(\Phi,\Phi)$ that is mapped to Υ in $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z},\Phi)$. Consider the maps in the following diagram

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

The extension Υ in $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z},\Phi)$ is mapped to zero in $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z},\mu_2)$. It follows from the exactness of the Ext-sequence that the leftmost vertical arrow maps the class of G into the image of $\mathrm{Ext}^1_{\underline{C}}(\mu_2,\mu_2) \longrightarrow \mathrm{Ext}^1_{\underline{C}}(\Phi,\mu_2)$. Therefore it maps the extension G to $\Upsilon^\vee$. This means that G admits a surjective morphism onto $\Upsilon^\vee$ and hence onto μ_4. The kernel of this morphism is $\mathbf{Z}/4\mathbf{Z}$ or a twist of $\mathbf{Z}/4\mathbf{Z}$ by the quadratic character χ_p. In the second case one checks that a generator σ of the inertia group of a prime over p does not satisfy $(\sigma - \mathrm{id})^2 = 0$. Since G is an object of $\underline{C}$, this is impossible. Therefore the group scheme G is an extension of μ_4 by $\mathbf{Z}/4\mathbf{Z}$:

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

The group scheme G is killed by 4 and the Galois group acts on $G(\overline{\mathbf{Q}})$ through matrices of the form

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

where $\omega_2 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \{\pm 1\}$ is the character that corresponds to the field $\mathbf{Q}(i)$ and $a : G_{\mathbf{Q}} \longrightarrow \mathbf{Z}/4\mathbf{Z}$ is a 1-cocycle whose restriction to $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(i))$ is a character satisfying $2a = \chi_p$. In particular, a has order 4.

Let K be the field generated by the points of G. The extension $\mathbf{Q}(i) \subset K$ is cyclic of degree 4. Since the connected component splits any extension $0 \to \mathbf{Z}/4\mathbf{Z} \to G \to \mu_4 \to 0$ over $\mathbf{Z}_2$, the extension $\mathbf{Q}(i) \subset K$ is unramified outside p and the prime $\pi = i + 1$ splits in K. Since K is Galois over $\mathbf{Q}$, Kummer theory implies that $K = \mathbf{Q}(i, \sqrt[4]{\pm p})$, where the sign is chosen so that $\pm p \equiv 1 \pmod 8$. The prime $1 + i$ splits in K if and only if $\pm p$ is square in $\mathbf{Q}_2(i)$. This happens if and only if $\pm p \equiv 1 \pmod{\pi^7}$. In other words, if and only if $p \equiv \pm 1 \pmod{16}$.

This proves the proposition. □

Theorem 2.7. *If $p \equiv 7 \pmod{16}$ then $\mathrm{Ext}^1_{\underline{C}}(\Phi, \Phi)$ vanishes.*

Proof. Let G be an object in $\mathrm{Ext}^1_{\underline{C}}(\Phi, \Phi)$. By Proposition 2.5 (a) the map

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

is injective. Since $p \equiv 7 \pmod 8$, Proposition 2.5 (b) implies that the group $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$ is generated by the extension Υ. Therefore G is split if and only if it is *not* mapped to the extension Υ in $\mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, \Phi)$. The result now follows from Proposition 2.6. □

This leads to an alternative proof of the following result [10].

Corollary 2.8. *There does not exist a non-zero semistable abelian variety over $\mathbf{Q}$ with good reduction outside 7.*

Proof. Using the methods of [10, section 6] or of section 5 of the present paper it is easy to prove that for $p = 7$ the only simple objects in the category $\underline{C}$ are the group schemes $\mathbf{Z}/2\mathbf{Z}$ and μ_2. We leave this to the reader. Now let A be a semistable abelian variety over $\mathbf{Q}$ with good reduction outside 7. For every $n \geq 1$ the group scheme $A[2^n]$ is an object of the category $\underline{C}$. Therefore it admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2. The results of this section imply then that $A[2^n]$ admits a filtration by closed flat subgroup schemes

$$0 \underbrace{\hookrightarrow}_{\mu_2\text{'s}} G_{n,1} \underbrace{\hookrightarrow}_{\Phi\text{'s}} G_{n,2} \underbrace{\hookrightarrow}_{\mathbf{Z}/2\mathbf{Z}\text{'s}} A[2^n]$$

with the property that $G_{n,1}$ admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to μ_2, the quotient $A[2^n]/G_{n,2}$ admits such a filtration with successive subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$ and the group scheme $G_{n,2}/G_{n,1}$ admits such a filtration with successive subquotients isomorphic to Φ. By Theorem 2.7 the subquotient $G_{n,2}/G_{n,1}$ is actually a *direct product* of group schemes isomorphic to Φ. Just as in [10, section 7] or section 6 of the present paper one shows that the orders of the group schemes $G_{n,1}$, $G_{n,2}/G_{n,1}$, $A[2^n]/G_{n,2}$ and hence of $A[2^n]$ remain bounded as $n \longrightarrow \infty$. This is impossible unless $A = 0$. $\square$

3. The group scheme V and its Cartier dual.

In sections 3 and 4 we make the following assumptions on the prime p:

Assumption 3.1. *We assume that*

- $p \equiv -1 \pmod 8$*;*
- $\mathbf{Q}(\sqrt{-p})$ *admits a unique unramified cyclic degree* 3 *extension* H*;*
- *the prime* 2 *splits into a product of two prime ideals* $\mathfrak{q}$ *and* $\overline{\mathfrak{q}}$ *of the ring of integers* O_H*;*
- *the ray class groups of* H *of conductors* $\mathfrak{q}^2$*,* $\overline{\mathfrak{q}}^2$ *and* $\sqrt{-p}$ *all have odd order.*

In section 5 we show that the prime $p = 23$ satisfies the assumptions. But so do $p = 31$, 199, ... and probably infinitely many others.

By class field theory the assumptions imply several things. First of all, the 3-part of the class group of $\mathbf{Q}(\sqrt{-p})$ is a non-trivial cyclic group. The Galois group $\Delta = \mathrm{Gal}(H/\mathbf{Q})$ is isomorphic to $S_3 \cong \mathrm{GL}_2(\mathbf{F}_2)$. The class number of H is odd. The residue fields of $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ are isomorphic to $\mathbf{F}_8$. Since the 2-parts of the ray class groups of conductor $\mathfrak{q}^2$ and $\overline{\mathfrak{q}}^2$ are both trivial and since the $\mathbf{F}_2$-dimension of $O_H^*/{O_H^*}^2$ is 3, the 2-part of the ray class group of conductor $(4) = \mathfrak{q}^2\overline{\mathfrak{q}}^2$ of H is an $\mathbf{F}_2$-vector space of dimension at most 3. On the other hand, the ray class field of conductor (4) of H contains the field $H(\sqrt{\varepsilon} : \varepsilon \in O_H^*\}$. Since the latter field has degree 8 over H, this inclusion is actually an equality.

Under Assumption 3.1 we construct two more simple objects in the category $\underline{C}$ that was introduced in section 2.

Definition. Let $\tau \in \Delta \cong S_3$ be an element of order 3 and let W denote the quotient of $\mathbf{Z}_2[\Delta]$ by the two-sided ideal generated by the τ-norm $\tau^2 + \tau + 1$. We define V to be the étale group scheme over $\mathbf{Z}[\frac{1}{p}]$ with Galois module $V(\overline{\mathbf{Q}})$ isomorphic to $W/2W$. The Galois modules $V(\overline{\mathbf{Q}})$ and $V^\vee(\overline{\mathbf{Q}})$ are isomorphic.

The Δ-action on $W/2W$ is irreducible and unramified outside p. Since the prime $\sqrt{-p}$ is principal, it splits in H. It follows that the inertia subgroups of Δ of the primes over p in $\mathrm{Gal}(H/\mathbf{Q})$ have order 2, so that their elements σ satisfy

$\sigma^2 = \mathrm{id}$. Therefore the group scheme V and its Cartier dual $V^\vee$ are objects of the category $\underline{C}$. They are both simple.

Group schemes that are successive extensions of copies of V make up a full subcategory of $\underline{Gr}$. The same is true for the group schemes that are successive extensions of copies of $V^\vee$. These categories are actually abelian subcategories of the category $\underline{C}$. The following proposition is analogous to Proposition 2.1.

Proposition 3.2. *The functor that associates to a finite abelian* 2*-group* A *the unique étale group scheme over* $\mathbf{Z}[\frac{1}{p}]$ *with associated Galois module* $A \otimes W$ *is an equivalence between the category of finite abelian* 2*-groups and the full subcategory of* $\underline{Gr}$ *whose objects are finite group schemes that are successive extensions of the group scheme* V*. In particular, any such group scheme becomes constant over the ring* $O_H[\frac{1}{p}]$*.*

Similarly, the functor that associates to a finite abelian 2*-group* A *the Cartier dual of the unique étale group scheme over* $\mathbf{Z}[\frac{1}{p}]$ *with associated Galois module* $\mathrm{Hom}(A, \mathbf{Q}/\mathbf{Z}) \otimes W$ *is an equivalence between the category of finite abelian* 2*-groups and the full subcategory of* $\underline{Gr}$ *whose objects are finite group schemes that are successive extensions of the group scheme* $V^\vee$*. In particular, any such group scheme becomes diagonalizable over the ring* $O_H[\frac{1}{p}]$*.*

Proof. By Galois theory, it suffices to show that a group scheme G in $\underline{C}$ that is a successive extension of the group scheme V has a Galois module of the form $A \otimes W$ for some finite 2-group A. Such a group scheme G is étale. The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/H)$ acts its points through a 2-group Π. The maximal abelian quotient Π/Π' is a quotient of the maximal abelian 2-extension of H that is unramified outside the primes lying over p. By Assumption 3.1, this extension is trivial, so that Π/Π' and hence Π are trivial. It follows that $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $G(\overline{\mathbf{Q}})$ through its quotient $\Delta = \mathrm{Gal}(H/\mathbf{Q})$. Therefore $G(\overline{\mathbf{Q}})$ is a $\mathbf{Z}_2[\Delta]$-module.

Let $\tau \in \Delta \cong S_3$ be an automorphism of order 3. Then $G(\overline{\mathbf{Q}})$ is a direct product of the τ-invariants and the kernel of the τ-norm $\tau^2 + \tau + 1$. Since $G(\overline{\mathbf{Q}})$ is a successive extension of copies of $V(\overline{\mathbf{Q}})$, the submodule of τ-invariants is zero and hence $G(\overline{\mathbf{Q}})$ is killed by the τ-norm. It follows that $G(\overline{\mathbf{Q}})$ is a module over the ring $\mathbf{Z}_2[\Delta]$ modulo the two-sided ideal generated by the τ-norm.

The reduction homomorphism $\mathrm{GL}_2(\mathbf{Z}_2) \longrightarrow \mathrm{GL}_2(\mathbf{F}_2) \cong \Delta$ has a section that is unique up to conjugation. The induced natural map $\mathbf{Z}_2[\Delta] \longrightarrow \mathrm{End}(\mathbf{Z}_2 \times \mathbf{Z}_2)$ gives rise to an isomorphism of $\mathbf{Z}_2[\Delta]/(\tau^2+\tau+1)$ with the ring of 2×2 matrices over $\mathbf{Z}_2$. By Morita equivalence, the functor $A \mapsto A \otimes W$ is an equivalence of categories from the category of finite abelian 2-groups to the category of finite modules over this matrix ring. Therefore $G(\overline{\mathbf{Q}})$ is of the form $A \otimes W$ for some finite 2-group A. The result now follows from Galois theory.

The second statement follows by Cartier duality. This proves the proposition. $\square$

Example 3.3. *Both groups* $\mathrm{Hom}(V, V)$ *and* $\mathrm{Hom}(V^\vee, V^\vee)$ *are isomorphic to* $\mathbf{F}_2$*. The group* $\mathrm{Ext}^1_{\underline{Gr}}(V, V)$ *of extensions of* V *by itself over* $\mathbf{Z}[\frac{1}{p}]$ *has order* 2*. It is generated by the étale group scheme with associated Galois module* $W/4W = \mathbf{Z}/4\mathbf{Z}[\Delta]/(\tau^2 + \tau + 1)$*.*

Proposition 3.4. *Over the ring* $\mathbf{Z}[\frac{1}{p}]$ *we have*

$$\mathrm{Hom}(V^\vee, V) = 0 \quad \textit{and} \quad \mathrm{Hom}(V, V^\vee) = \mathbf{F}_2.$$

Proof. Since $V^\vee$ is local over $\mathbf{Z}_2$, while V is étale, we have $\mathrm{Hom}(V^\vee, V) = 0$. In order to compute $\mathrm{Hom}(V, V^\vee)$, we note that $O_H[\frac{1}{p}]$ is Galois over $\mathbf{Z}[\frac{1}{p}]$ with Galois group Δ. We have

$$\mathrm{Hom}_{\underline{Gr}}(V, V^\vee) \;\cong\; \mathrm{Hom}_{O_H[\frac{1}{p}]}(V, V^\vee)^\Delta \;=\; \mathrm{Hom}_\Delta(V(\overline{\mathbf{Q}}), V^\vee(\overline{\mathbf{Q}})) \;=\; \mathbf{F}_2.$$

The equalities follow from Schur's Lemma and the fact that the group schemes V and $V^\vee$ are isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and $\mu_2 \times \mu_2$ respectively and that $\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ is $\mathbf{F}_2$ over $O_H[\frac{1}{p}]$. □

Proposition 3.5. *Over the ring* $\mathbf{Z}[\frac{1}{p}]$ *we have the following.*

(a) Extensions of $\mathbf{Z}/2\mathbf{Z}$ *and* V *by one another are necessarily split; extensions of* μ_2 *and* $V^\vee$ *by one another are necessarily split.*

(b) We have

$$\mathrm{Ext}^1_{\underline{Gr}}(\mu_2, V) \;=\; \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, \mathbf{Z}/2\mathbf{Z}) \;=\; 0.$$

(c) We have

$$\mathrm{Ext}^1_{\underline{C}}(V, \mu_2) \;=\; \mathrm{Ext}^1_{\underline{C}}(\mathbf{Z}/2\mathbf{Z}, V^\vee) \;=\; \mathbf{F}_2.$$

Proof. First we observe that all extensions G that appear in this proposition are annihilated by 2. Indeed, the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $G(\overline{\mathbf{Q}})$ through a group that is an extension of $\Delta \cong S_3$ by a 2-group. Let τ be an element of order 3 in this group. Then $G(\overline{\mathbf{Q}})$ is a $\mathbf{Z}_2[\tau]$-module. It is therefore a direct sum of the τ-invariants and of the elements killed by the τ-norm. Since τ acts trivially on the points of μ_2 and $\mathbf{Z}/2\mathbf{Z}$, while the module $V(\overline{\mathbf{Q}}) \cong V^\vee(\overline{\mathbf{Q}})$ is killed by the τ-norm, we see that G is killed by 2.

(a) By Cartier duality it suffices to study extensions G of the étale group schemes $\mathbf{Z}/2\mathbf{Z}$ and V by one another. By Assumption 3.1, the ray class field of conductor $\sqrt{-p}$ of H has odd degree over H. This implies that the Galois group acts on $G(\overline{\mathbf{Q}})$ through $\Delta = \mathrm{Gal}(H/\mathbf{Q}) \cong S_3$. As we explained above, the τ-module $G(\overline{\mathbf{Q}})$ is a direct product of the τ-invariants and the kernel of the τ-norm, each of which are Δ-modules. It follows that the Δ-module $G(\overline{\mathbf{Q}})$ is isomorphic to the product of $V(\overline{\mathbf{Q}})$ and $\mathbf{Z}/2\mathbf{Z}$. So the extension splits.

(b) By Cartier duality it suffices to show that any extension

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow V^\vee \longrightarrow 0$$

is split over the ring $\mathbf{Z}[\frac{1}{p}]$. Such an extension is split over $\mathbf{Z}_2$ by the connected component. Therefore the action of $\mathrm{Gal}(\mathbf{Q}/H)$ on $G(\overline{\mathbf{Q}})$ is unramified outside p. By Assumption 3.1, the ray class group of H of conductor $\sqrt{-p}$ has odd order. It follows that $\mathrm{Gal}(\overline{\mathbf{Q}}/H)$ acts trivially on the points of G. Therefore, the extension also splits over $\mathbf{Z}[\frac{1}{2p}]$. The Mayer-Vietoris sequence [9, Cor. 2.4] shows then that $\mathrm{Ext}^1_{\underline{Gr}}(V^\vee, \mathbf{Z}/2\mathbf{Z})$ vanishes, as required.

(c) By Cartier duality it suffices to determine the extensions

$$0 \longrightarrow \mu_2 \longrightarrow G \longrightarrow V \longrightarrow 0$$

in the category $\underline{C}$. Let S be the étale extension $O_H[\frac{1}{p}]$ of $\mathbf{Z}[\frac{1}{p}]$. Then $f : \mathrm{Spec}(S) \longrightarrow \mathrm{Spec}(\mathbf{Z}[\frac{1}{p}])$ is Galois with Galois group $\Delta \cong S_3$ and the groups $\mathrm{Ext}^q_S(V, \mu_2)$ have a natural $\mathbf{F}_2[\Delta]$-structure. Using the fact that f^* maps injective abelian fppf sheaves on $\mathrm{Spec}(\mathbf{Z}[\frac{1}{p}])$ to injective abelian fppf sheaves on $\mathrm{Spec}(S)$, one shows that the functor $\mathrm{Hom}_S(V, -)$ from the category of abelian fppf sheaves on $\mathrm{Spec}(\mathbf{Z}[\frac{1}{p}])$ to the category of $\mathbf{F}_2[\Delta]$-modules carries injective objects to induced $\mathbf{F}_2[\Delta]$-modules. Therefore there is a Grothendieck spectral sequence

$$H^p(\Delta, \mathrm{Ext}^q_S(V, \mu_2)) \;\Rightarrow\; \mathrm{Ext}^{p+q}_{\underline{Gr}}(V, \mu_2).$$

Since the group scheme V is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ over S, the Δ-module $\mathrm{Hom}_S(V, \mu_2)$ is isomorphic to the cohomologically trivial Δ-module $V^\vee(\overline{\mathbf{Q}})$. Therefore the exactness of the sequence of low degree terms gives rise to a natural isomorphism

$$\mathrm{Ext}^1_{\underline{Gr}}(V, \mu_2)) \;\cong\; \mathrm{Ext}^1_S(V, \mu_2)^\Delta.$$

The composition of the functor $\mathrm{Hom}_S(\mathbf{Z}/2\mathbf{Z}, -)$ from the category of abelian fppf-sheaves on $\mathrm{Spec}(\mathbf{Z}[\frac{1}{p}])$ to the category of $\mathbf{F}_2[\Delta]$-modules and the functor $\mathrm{Hom}_{ab}(V(\overline{\mathbf{Q}}), -)$ from the category of $\mathbf{F}_2[\Delta]$-modules to itself is equal to the functor $\mathrm{Hom}_S(V, -)$. Since the functor $\mathrm{Hom}_{ab}(V(\overline{\mathbf{Q}}), -)$ is exact, the Grothendieck spectral sequence degenerates and there is a natural isomorphism of $\mathbf{F}_2[\Delta]$-modules

$$\mathrm{Hom}_{\mathrm{ab}}(V(\overline{\mathbf{Q}}), \mathrm{Ext}^q_S(\mathbf{Z}/2\mathbf{Z}, \mu_2)) \;\cong\; \mathrm{Ext}^q_S(V, \mu_2).$$

Therefore we have functorial isomorphisms

$$\mathrm{Ext}^1_{\underline{Gr}}(V, \mu_2)) \;\cong\; \mathrm{Ext}^1_S(V, \mu_2))^\Delta \;\cong\; \mathrm{Hom}_\Delta(V(\overline{\mathbf{Q}}), \mathrm{Ext}^1_S(\mathbf{Z}/2\mathbf{Z}, \mu_2)).$$

Since the class number of H is odd, the long exact sequence of flat cohomology groups of the exact sequence $0 \to \mu_2 \to \mathbf{G}_m \to \mathbf{G}_m \to 0$ of fppf sheaves and Kummer theory lead to the following exact sequence of $\mathbf{F}_2[\Delta]$-modules [10, proof of Prop. 4.2]:

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

Here an extension E of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 is mapped to a unit $u \in S^*$ that generates the quadratic extension of S that is generated by the points of E. Since $\mathrm{Hom}_\Delta(V(\overline{\mathbf{Q}}), \{\pm 1\}) = 0$, we have an isomorphism

$$\mathrm{Ext}^1_{\underline{Gr}}(V, \mu_2) \;\cong\; \mathrm{Hom}_\Delta(V(\overline{\mathbf{Q}}), S^*/S^{*2}).$$

Since all extensions in the group $\mathrm{Ext}^1_{\underline{Gr}}(V,\mu_2)$ are killed by 2, the extensions in the subgroup $\mathrm{Ext}^1_{\underline{C}}(V,\mu_2)\subset \mathrm{Ext}^1_{\underline{Gr}}(V,\mu_2)$ have the property that the inertia subgroups of the primes over p have order at most 2. Therefore the points of such extensions generate a field extension of H that is unramified at the primes over p. It follows that the units $u\in S^*$ can be taken in the subgroup $O_H^*\subset S^*$. Therefore the following diagram is commutative

$$\begin{array}{ccc}
\mathrm{Ext}^1_{\underline{C}}(V,\mu_2)) & \xrightarrow{\cong} & \mathrm{Hom}_\Delta(V(\overline{\mathbf{Q}}),O_H^*/{O_H^*}^2) \\
\downarrow\subset & & \downarrow\subset \\
\mathrm{Ext}^1_{\underline{Gr}}(V,\mu_2)) & \xrightarrow{\cong} & \mathrm{Hom}_\Delta(V(\overline{\mathbf{Q}}),S^*/S^{*2}).
\end{array}$$

Finally, since $O_H^*/{O_H}^{*2}$ is isomorphic to the $\mathbf{F}_2[\Delta]$-module $V(\overline{\mathbf{Q}})\times\mathbf{F}_2$, we have

$$\mathrm{Hom}_\Delta(V(\overline{\mathbf{Q}}),O_H^*/{O_H^*}^2)\;\cong\;\mathrm{Hom}_\Delta(V(\overline{\mathbf{Q}}),V(\overline{\mathbf{Q}})\times\mathbf{F}_2)\;\cong\;\mathrm{End}_\Delta(V(\overline{\mathbf{Q}}))\;=\;\mathbf{F}_2.$$

This proves (c). □

Proposition 3.5 implies that in the category $\underline{C}$ there is a unique non-split extension

$$0\longrightarrow\mu_2\longrightarrow G\longrightarrow V\longrightarrow 0.$$

Since V is isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ over O_H, the points of G generate the extension $L=H(\sqrt{u}\,:\,u\in O_{H,1}^*)$. Here $O_{H,1}^*$ is the subgroup of units whose norm to $\mathbf{Q}(\sqrt{-p})$ is equal to 1. The Galois group $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to the symmetric group S_4.

Proposition 3.6. *We have*

(a)

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

(b) We have

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

Proof. (a) By Proposition 3.5 the outer terms of the exact sequence

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

vanish. Therefore, so does the term in the middle. This proves (a).

(b) By Cartier duality it suffices to show that any extension of the form

$$0\longrightarrow\Phi\longrightarrow G\longrightarrow V\longrightarrow 0$$

splits. Let L be the number field generated by the points of G. Then $\mathrm{Gal}(L/\mathbf{Q})$ is an extension of $\Delta=\mathrm{Gal}(H/\mathbf{Q})\cong S_3$ by the finite exponent 2-group $\mathrm{Gal}(L/H)$. Let $\tau\in\mathrm{Gal}(L/\mathbf{Q})$ be an automorphism of order 3. Since $G(\overline{\mathbf{Q}})$ is a $\mathbf{Z}_2[\tau]$-module, it is a product of the kernels of the τ-norm and of $\tau-1$. Since $\Phi(\overline{\mathbf{Q}})$ is killed by $\tau-1$ and $V(\overline{\mathbf{Q}})$ is killed by the τ-norm, the group scheme G is killed by 2.

Since G is an object of the category $\underline{C}$, the extension $H \subset L$ is unramified outside the primes $\mathfrak{q}$ of O_H that lie over 2. Over the completion $O_{\mathfrak{q}}$ of O_H, the group scheme G is an extension of $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}\times\mu_2$. It follows that over $O_{\mathfrak{q}}$ the group scheme is an extension of an étale group scheme by μ_2. Therefore the kernel of $\sigma - \mathrm{id}$ is an $\mathbf{F}_2$-vector space of dimension at least 3. Moreover, by Kummer theory, the local Galois extension is the composite of quadratic extensions of $O_{\mathfrak{q}}$ generated by the square roots of certain units of $O_{\mathfrak{q}}$. It follows that the conductor of the local extension divides $\mathfrak{q}^2$. Therefore the conductor of L over H divides $\mathfrak{q}^2\overline{\mathfrak{q}}^2 = (4)$.

On the other hand, the group $G(\overline{\mathbf{Q}})$ is a 4-dimensional $\mathbf{F}_2$-vector space on which $\mathrm{Gal}(L/\mathbf{Q})$ acts through a subgroup of the group of invertible 4×4-matrices of the form

$$\begin{pmatrix} 1 & \chi_{abcd} & * & * \\ 0 & 1 & * & * \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$$

Here $\chi_{abcd} = 1$ when the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has order 2 and is 0 otherwise. In other words, $\chi : \mathrm{GL}_2(\mathbf{F}_2) \longrightarrow \mathbf{F}_2$ is the composition of the isomorphism $\mathrm{GL}_2(\mathbf{F}_2) \cong S_3$ with the sign homomorphism $S_3 \longrightarrow \mathbf{F}_2$.

The group $\Delta \cong \mathrm{GL}_2(\mathbf{F}_2)$ acts by conjugation on the additive group of 2×2-matrices indicated by $\begin{pmatrix} * & * \\ * & * \end{pmatrix}$. This 4-dimensional $\mathbf{F}_2[\Delta]$-module is isomorphic to $M = \mathrm{Hom}(V(\overline{\mathbf{Q}}), \Phi(\overline{\mathbf{Q}}))$. The 'Kummer map'

$$\mathrm{Gal}(L/H) \longrightarrow \mathrm{Hom}(V(\overline{\mathbf{Q}}), \Phi(\overline{\mathbf{Q}})),$$

is given by $\sigma \mapsto f_\sigma$ where $f_\sigma(P) = \sigma(P') - P'$, where P' is any point in $G(\overline{\mathbf{Q}})$ that is mapped to $P \in V(\overline{\mathbf{Q}})$. It is injective and Δ-linear. Since $\mathrm{Gal}(L/H)$ has order at most $\#(O_H^*/(O_H^*)^2) = 8$, it is isomorphic to a proper Δ-submodule of M.

The Δ-module M is killed by the τ-norm. Therefore it is isomorphic to the product of two copies of the $\mathbf{F}_2[\Delta]$-module $\mathbf{F}_2[\Delta]/(\tau^2+\tau+1)$. The module M admits precisely three proper non-zero submodules. They all have order 4 and are given by

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

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

and

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

The non-zero matrices in first two submodules all have rank 2. Therefore the 4×4 matrices that describe the action of $\sigma - \mathrm{id}$ for $\sigma \in \mathrm{Gal}(L/H)$ on $G(\overline{\mathbf{Q}})$ are either zero or have 2-dimensional kernels. By Assumption 3.1 made on the prime p at the beginning of this section, the field L is contained in the degree 8 extension $H(\sqrt{u} : u \in O_H^*)$ of H. In particular, the extension $H \subset L$ is totally ramified at both primes over 2. It follows that the inertia subgroup of $\mathrm{Gal}(L/\mathbf{Q})$ of both primes is equal to $\mathrm{Gal}(L/H)$.

Therefore the kernel of $\sigma - \mathrm{id}$ is at least 3-dimensional and the first two submodules cannot be the image of $\mathrm{Gal}(L/H)$. It follows that $\mathrm{Gal}(L/H)$ is contained in the third submodule. The fact that the bottom rows of the 2×2-matrices in this module are all zero, means that the second arrow in the exact sequence

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

maps the class of the extension G to an extension of V by μ_2 that is *split* as a Galois module. By the proof of Prop. 3.5 the only non-trivial extension V by μ_2 over $\mathbf{Z}[\frac{1}{p}]$ is *not split* as a Galois module. Therefore the second arrow is zero. Since $\mathrm{Ext}^1_{\underline{C}}(V, \mathbf{Z}/2\mathbf{Z}) = 0$ by Prop. 3.5 (a), it follows that $\mathrm{Ext}^1_{\underline{C}}(V, \Phi)$ vanishes, as required. □

We now obtain a rough description of the objects of a certain subcategory of the category $\underline{C}$.

Theorem 3.7. *Let p be a prime number that satisfies the hypothesis made at the beginning of this section. Let G be an object of the category $\underline{C}$ and suppose that it admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to one of the simple group schemes $\mathbf{Z}/2\mathbf{Z}$, μ_2, V or $V^\vee$. Then G admits a filtration with closed flat subgroup schemes of the form*

$$0 \hookrightarrow G_1 \hookrightarrow G_2 \hookrightarrow G,$$

where G_1 becomes diagonalizable and the quotient G/G_2 becomes constant over the ring $\mathbf{Z}[\frac{1+\sqrt{-p}}{2}, \frac{1}{p}]$. Moreover, we have

$$G_2/G_1 \cong E \times E',$$

where E' admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to Φ and E admits such a filtration with successive subquotients isomorphic to V or $V^\vee$.

Proof. Let G be an object of the category $\underline{C}$ admitting such a filtration. By Propositions 2.5 and 3.5 any extension of the form

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

where G' is one of the group schemes Φ, V or $V^\vee$ splits. This fact and its dual version imply that G admits a filtration by closed flat subgroup schemes of the form

$$0 \underbrace{\hookrightarrow}_{\mu_2\text{'s}} G_1 \hookrightarrow G_2 \underbrace{\hookrightarrow}_{\mathbf{Z}/2\mathbf{Z}\text{'s}} G,$$

where G/G_2 is an extension of copies of $\mathbf{Z}/2\mathbf{Z}$, the group scheme G_1 is an extension of copies of μ_2 and G_2/G_1 admits a filtration by closed flat subgroup schemes with successive subquotients isomorphic to Φ, V or $V^\vee$. By Prop. 2.1 the group scheme G/G_2 becomes constant and G_1 becomes diagonalizable over $\mathbf{Z}[\frac{1+\sqrt{-p}}{2}, \frac{1}{p}]$. By Proposition 3.6 the group scheme G_2/G_1 is of the form $E \times E'$, where E' admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to Φ and E admits such a filtration with successive subquotients isomorphic to V or $V^\vee$. This proves the theorem. $\square$

4. The group scheme Ψ.

In this section we also make the Assumptions 3.1 on the prime p. We construct a non-split extension Ψ of the group scheme $V^\vee$ by V over $\mathbf{Z}[\frac{1}{p}]$. Here V is the étale order 4 group scheme that was constructed in section 3. The extension Ψ is unique. It is killed by 2 and it is self-dual. We show that its ring of endomorphisms is a finite field with 4 elements.

In section 5 we show that for $p = 23$ the group scheme Ψ is isomorphic to the subscheme of 2-torsion points of the Jacobian of the modular curve $X_0(23)$.

Proposition 4.1. *Let V be the étale group scheme constructed in section 3. We have*

$$\mathrm{Ext}^1_{\underline{Gr}}(V^\vee, V) \;=\; \mathbf{F}_2.$$

The unique non-split extension

$$0 \longrightarrow V \longrightarrow \Psi \longrightarrow V^\vee \longrightarrow 0$$

is split over $\mathbf{Q}$ as well as over $\mathbf{Z}_l$ for all primes l of $\mathbf{Z}[\frac{1}{p}]$.

Proof. By Assumption 3.1 the field $\mathbf{Q}(\sqrt{-p})$ admits a unique unramified cyclic cubic extension H. The group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on the points of V through $\Delta = \mathrm{Gal}(H/\mathbf{Q}) \cong S_3$. Consider an extension

$$0 \longrightarrow V \longrightarrow G \longrightarrow V^\vee \longrightarrow 0.$$

The sequence is split over $\mathbf{Z}_2$ by the connected component. It follows that G is killed by 2. Let L be the extension generated by the points of G. Since G is an object of $\underline{C}$, the extension $H \subset L$ is abelian of 2-power degree and is everywhere unramified. So, by the Assumptions 3.1 we have $L = H$. This implies that $G(\overline{\mathbf{Q}})$ is an $\mathbf{F}_2[\Delta]$-module killed by the τ-norm, where $\tau \in \Delta$ has order 3. Since $\mathbf{F}_2[\Delta]/(\tau^2 + \tau + 1)$ is isomorphic to the ring of 2×2-matrices over $\mathbf{F}_2$, Morita equivalence implies that the Galois module $G(\overline{\mathbf{Q}})$ is split. So G is split over $\mathbf{Q}$ and over $\mathbf{Z}_l$ for every prime l of $\mathbf{Z}[\frac{1}{p}]$.

This fact and the triviality of both $\mathrm{Hom}_{\mathbf{Z}_2}(V^\vee, V)$ and $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{p}]}(V^\vee, V)$ imply that the Mayer-Vietoris exact sequence [9, Cor. 2.4] becomes the short exact sequence

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, V) \longrightarrow \mathrm{Hom}_{\mathbf{Q}_2}(V^\vee, V) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, V) \longrightarrow 0$$

Since $V(\overline{\mathbf{Q}})$ and $V^\vee\overline{\mathbf{Q}})$ are isomorphic Δ-modules, Schur's Lemma implies that the group $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, V)$ has order 2. By the Assumptions 3.1 the prime 2 *splits* in $\mathbf{Q}(\sqrt{-p})$ but not in H. Therefore the local Galois group is the subgroup of Δ generated by an element τ of order 3. The ring $\mathbf{F}_2[\tau]$ acts on $V(\overline{\mathbf{Q}})$ through its quotient $\mathbf{F}_2[\tau]/(\tau^2+\tau+1) \cong \mathbf{F}_4$. Therefore $\mathrm{Hom}_{\mathbf{Q}_2}(V^\vee, V)$ is a 1-dimensional $\mathbf{F}_4$-vector space.

The exactness of the sequence implies then that $\mathrm{Ext}^1_{\mathbf{Z}[\frac{1}{p}]}(V^\vee, V) \cong \mathbf{F}_4/\mathbf{F}_2 \cong \mathbf{F}_2$ as required. □

Definition. Let Ψ denote the unique non-split extension of $V^\vee$ by V. The group scheme Ψ is an object of $\underline{C}$. It is self-dual and has order 16. Its points generate the Hilbert class field H of $\mathbf{Q}(\sqrt{23})$.

Proposition 4.2. *Over the ring* $\mathbf{Z}[\frac{1}{p}]$ *we have*

(a) $\mathrm{Hom}(\Psi, V) = \mathrm{Hom}(V^\vee, \Psi) = 0$*;*

(b) The $\mathbf{F}_2$*-dimension of* $\mathrm{Hom}(V, \Psi) \cong \mathrm{Hom}(\Psi, V^\vee)$ *is equal to* 2.

Proof. (a) We apply the functor $\mathrm{Hom}(V^\vee, -)$ to the exact sequence

$$0 \longrightarrow V \longrightarrow \Psi \longrightarrow V^\vee \longrightarrow 0.$$

By Prop. 3.4 we have $\mathrm{Hom}(V^\vee, V) = 0$. Therefore we obtain the exact sequence

$$0 \longrightarrow \mathrm{Hom}(V^\vee, \Psi) \xrightarrow{\phi} \mathrm{Hom}(V^\vee, V^\vee) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, V).$$

By Schur's Lemma the group $\mathrm{Hom}(V^\vee, V^\vee)$ is an $\mathbf{F}_2$-vector space of dimension 1, generated by the identity. The identity is mapped to the class of the extension Ψ in $\mathrm{Ext}^1_{\underline{Gr}}(V^\vee, V)$. Therefore the second arrow is injective and ϕ must be zero. This implies that $\mathrm{Hom}(V^\vee, \Psi)$ is zero as required. The fact that $\mathrm{Hom}(\Psi, V)$ vanishes follows by Cartier duality.

To prove (b) we apply the functor $\mathrm{Hom}(-, V^\vee)$ to the exact sequence $0 \longrightarrow V \longrightarrow \Psi \longrightarrow V^\vee \longrightarrow 0$. We obtain the exact sequence

$$0 \longrightarrow \mathrm{Hom}(V^\vee, V^\vee) \longrightarrow \mathrm{Hom}(\Psi, V^\vee) \longrightarrow \mathrm{Hom}(V, V^\vee) \xrightarrow{\phi} \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, V^\vee).$$

Since Ψ is split over $\mathbf{Q}$, it is killed by 2. Consideration of the Galois modules shows that the image under ϕ of the non-trivial homomorphism $V \longrightarrow V^\vee$ is an extension of $V^\vee$ by $V^\vee$ that is also killed by 2. The only non-trivial extension of $V^\vee$ by itself is dual to the group scheme of Example 3.3 and is *not* killed by 2. Therefore the map ϕ must be zero. By Example 3.3 and Prop. 3.4 both groups $\mathrm{Hom}(V^\vee, V^\vee)$ and $\mathrm{Hom}(V, V^\vee)$ have order 2. This implies that the order of $\mathrm{Hom}(\Psi, V^\vee)$ and hence of $\mathrm{Hom}(V, \Psi)$ has to be 4, as required. □

Proposition 4.3. *We have*

$$\mathrm{Ext}^1_{\underline{Gr}}(\Psi, V) \;=\; \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, \Psi) \;=\; 0.$$

Proof. By Cartier duality it suffices to prove that any extension of the form

$$0 \longrightarrow V \longrightarrow G \longrightarrow \Psi \longrightarrow 0$$

is split. Let C denote the kernel of the composite morphism $G \longrightarrow \Psi \longrightarrow V^\vee$. Then the order 64 group scheme G sits in an exact sequence

$$0 \longrightarrow C \longrightarrow G \longrightarrow V^\vee \longrightarrow 0,$$

where C is an extension of V by V. By Example 3.3 the extension C is either split or it is a twist of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$. In order to decide this, we first compute $\mathrm{Ext}^1_{\underline{Gr}}(V^\vee, C)$.

Claim. The following natural sequence is exact:

$$0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, C) \longrightarrow \mathrm{Hom}_{\mathbf{Q}_2}(V^\vee, C) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, C) \longrightarrow 0.$$

Proof of the claim. This is the Mayer-Vietoris exact sequence [9, Cor. 2.4]. Indeed, since C is étale, there are no non-zero homomorphisms $V^\vee \longrightarrow C$ over $\mathbf{Z}_2$. Therefore there are none over $\mathbf{Z}[\frac{1}{p}]$. Since $V^\vee$ is connected and C is étale, we have $\mathrm{Ext}^1_{\mathbf{Z}_2}(V^\vee, C) = 0$. It remains to show that $\mathrm{Ext}^1_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, C)$ is zero. For any extension G of $V^\vee$ by C, the Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/H)$ acts through a 2-group on $G(\overline{\mathbf{Q}})$. Since the extension G of $V^\vee$ by C is split over $\mathbf{Z}_2$, the group scheme G is killed by 2 or 4, depending on whether C is split or not.

The Galois action on $G(\overline{\mathbf{Q}})$ is unramified outside p. By the Assumptions 3.1, the field H admits no quadratic extensions that are unramified outside the primes lying over p. The action of $\mathrm{Gal}(\overline{\mathbf{Q}}/H)$ on $G(\overline{\mathbf{Q}})$ is therefore trivial. It follows that $G(\overline{\mathbf{Q}})$ is a module over the ring $\mathbf{Z}_2[\Delta]$. Writing τ for an order 3 element in Δ, the Δ-module $G(\overline{\mathbf{Q}})$ is killed by the τ-norm. Therefore it is a module over $\mathbf{Z}_2[\Delta]/(\tau^2+\tau+1)$, which is isomorphic to the ring of 2×2-matrices over $\mathbf{Z}_2$. Morita equivalence implies then that the extension G of $V^\vee$ by C is split over $\mathbf{Z}[\frac{1}{2p}]$.

This proves the claim.

We now show that the group scheme C is a split extension of V by V. Suppose not. Then Example 3.3 shows that $C(\overline{\mathbf{Q}})$ is isomorphic to $\mathbf{Z}/4\mathbf{Z}[\Delta]/(\tau^2+\tau+1)$. It follows that the group $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, C)$ is isomorphic to $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, V) = \mathbf{F}_2$. By the Assumptions 3.1 the prime 2 is split in $\mathbf{Q}(\sqrt{-p})$ but not in H. Therefore we have $\mathrm{Hom}_{\mathbf{Q}_2}(V^\vee, C) = \mathrm{Hom}_{\mathbf{Q}_2}(V^\vee, V) \cong \mathbf{F}_4$. It follows from the exactness of the sequence in the claim that the group $\mathrm{Ext}^1_{\underline{Gr}}(V^\vee, C)$ has order 2.

Then we apply the functor $\mathrm{Hom}(V^\vee, -)$ to the exact sequence $0 \longrightarrow V \longrightarrow C \longrightarrow V \longrightarrow 0$. Since $\mathrm{Hom}(V^\vee, V)$ vanishes, we obtain the exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, V) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, C) \xrightarrow{\psi} \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, V)$$

By Proposition 4.1 all three groups have order 2, so that the map ψ is zero. But this is impossible, since it maps the class of G to the class of Ψ, which is certainly not trivial. We conclude that C is a split extension of V by V. Finally we apply the functor $\mathrm{Hom}(-, V)$ to the exact sequence

$$0 \longrightarrow V \longrightarrow \Psi \longrightarrow V^\vee \longrightarrow 0$$

and we obtain the exact sequence

$$0 \longrightarrow \mathrm{Hom}(V, V) \xrightarrow{\phi} \mathrm{Ext}^1_{\underline{Gr}}(V^\vee, V) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(\Psi, V) \longrightarrow \mathrm{Ext}^1_{\underline{Gr}}(V, V).$$

Proposition 4.1 implies that ϕ is an isomorphism. This shows that the map $\mathrm{Ext}^1_{\underline{C}}(\Psi, V) \longrightarrow \mathrm{Ext}^1_{\underline{C}}(V, V)$ is injective. Since it maps the class of G to the class of the split extension C, the extension G is split.

This proves the proposition. □

Theorem 4.4. *Let p be a prime satisfying the Assumptions 3.1. Let G be an object of the category $\underline{C}$. Suppose that G admits a filtration with flat closed subgroup schemes and successive subquotients isomorphic to either V or $V^\vee$. Then G admits a filtration*

$$0 \hookrightarrow H_1 \hookrightarrow H_2 \hookrightarrow G,$$

where G/H_2 becomes constant and H_1 becomes diagonalizable over the ring $O_H[\frac{1}{p}]$ and where the group scheme H_2/H_1 admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to Ψ.

Proof. By Proposition 4.3 the group scheme G admits a filtration

$$0 \underbrace{\hookrightarrow}_{V^\vee\text{'s}} H_1 \underbrace{\hookrightarrow}_{\Psi\text{'s}} H_2 \underbrace{\hookrightarrow}_{V\text{'s}} G.$$

where G/H_2 is an extension of copies of V, the group scheme H_1 is an extension of copies of $V^\vee$ and H_2/H_1 admits a filtration by closed flat subgroup schemes with successive subquotients isomorphic to Ψ. By Prop. 3.2 the group scheme G/H_2 becomes constant over the ring $O_H[\frac{1}{p}]$ and H_1 becomes diagonalizable over $O_H[\frac{1}{p}]$. This proves the theorem. □

Proposition 4.5. *The ring $\mathrm{End}(\Psi)$ is a field with 4 elements.*

Proof. We apply the functor $\mathrm{Hom}(\Psi, -)$ to the exact sequence

$$0 \longrightarrow V \longrightarrow \Psi \longrightarrow V^\vee \longrightarrow 0.$$

and consider the exact sequence of $\mathrm{Ext}^1_{\underline{Gr}}$-groups. By Proposition 4.2 the group $\mathrm{Hom}(\Psi, V)$ is zero and the $\mathbf{F}_2$-dimension of $\mathrm{Hom}(\Psi, V^\vee)$ is 2. By Proposition 4.3 the group $\mathrm{Ext}^1_{\underline{Gr}}(\Psi, V)$ is zero. It follows that $\mathrm{End}(\Psi)$ has order 4.

It remains to show that $\mathrm{End}(\Psi)$ is a field. Since $V(\overline{\mathbf{Q}}) \cong V^\vee(\overline{\mathbf{Q}})$, the Galois module $\Psi(\overline{\mathbf{Q}})$ is isomorphic to $V(\overline{\mathbf{Q}}) \times V(\overline{\mathbf{Q}})$. It has precisely three proper submodules. They all have order 4 and are isomorphic to $V(\overline{\mathbf{Q}})$. Their Zariski closures are three distinct proper closed flat subgroup schemes G of Ψ. Since by Proposition 4.2 we have $\mathrm{Hom}(V^\vee, \Psi) = 0$, each subgroup scheme G is isomorphic to V and has the property that Ψ/G is isomorphic to $V^\vee$.

Now let $f : \Psi \longrightarrow \Psi$ be an endomorphism. If f is zero on $\Psi(\overline{\mathbf{Q}})$, then it is zero. Similarly, if it induces an automorphism of $\Psi(\overline{\mathbf{Q}})$, then it is itself also an automorphism. Suppose therefore that f is not zero and is not an automorphism. Then its kernel on $\Psi(\overline{\mathbf{Q}})$ is one of the three proper submodules and therefore $f : \Psi \longrightarrow \Psi$ is zero on one of the three subgroup schemes G above. It follows that f factors through $\Psi/G \cong V^\vee$ and hence induces a morphism $V^\vee \longrightarrow \Psi$, which is necessarily zero. Contradiction.

This proves the proposition. $\square$

Lemma 4.6. *Let p be a prime satisfying the Assumptions 3.1. Then any extension in the category $\underline{C}$*

$$0 \longrightarrow \Psi \longrightarrow G \longrightarrow V \longrightarrow 0,$$

that is killed by 2, is split.

Proof. We apply the functor $\mathrm{Hom}(V, -)$ to the exact sequence

$$0 \longrightarrow V \longrightarrow \Psi \longrightarrow V^\vee \longrightarrow 0.$$

Proposition 4.2 implies then that we have the following exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_{\underline{C}}(V, V) \longrightarrow \mathrm{Ext}^1_{\underline{C}}(V, \Psi) \xrightarrow{\phi} \mathrm{Ext}^1_{\underline{C}}(V, V^\vee).$$

By Example 3.5 the unique non-split extension of V by V is *not* killed by 2. Therefore the restriction of ϕ to the subgroup $\mathrm{Ext}^1_{\underline{C},[2]}(V, \Psi)$ of extensions of V by Ψ that are killed by 2, is injective. Let W in $\mathrm{Ext}^1_{\underline{C}}(V, V^\vee)$ be the image under ϕ of the class of G. Since G is killed by 2, so is W. If W is a split extension of V by $V^\vee$, we are done. So, suppose it is not. We now derive a contradiction from this assumption.

We have the exact sequence

$$0 \longrightarrow V^\vee \longrightarrow W \longrightarrow V \longrightarrow 0.$$

First we observe that W is determined by its Galois module. Indeed, the étale extension $S = O_H[\frac{1}{p}]$ of $\mathbf{Z}[\frac{1}{p}]$ is Galois with group Δ. Just like in the proof of Proposition 3.5, the functor $\mathrm{Hom}_S(V, -)$ from the category of fppf sheaves over $\mathrm{Spec}(\mathbf{Z}[\frac{1}{p}])$ to the category of $\mathbf{F}_2[\Delta]$-modules sends injective objects to induced $\mathbf{F}_2[\Delta]$-modules. Therefore we have the spectral sequence

$$H^p(\Delta, \mathrm{Ext}^q_S(V, V^\vee)) \Longrightarrow \mathrm{Ext}^{p+q}_{\underline{Gr}}(V, V^\vee).$$

Since $\mathrm{Hom}(V, V^\vee) \cong \mathrm{End}(V)$ is a cohomologically trivial Δ-module, the exact sequence of low degree terms shows that the natural map

$$\mathrm{Ext}^1_{\underline{Gr}}(V, V^\vee) \hookrightarrow \mathrm{Ext}^1_{O_H[\frac{1}{p}]}(V, V^\vee)$$

is injective. Over the ring $O_H[\frac{1}{p}]$ the group schemes V and $V^\vee$ are isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ and $\mu_2 \times \mu_2$ respectively. Since extensions of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 are determined by their Galois modules, we see that the same is true for W.

The Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on the points of W. By Kummer theory it acts through $\pi = \mathrm{Gal}(L/\mathbf{Q})$ where $L = H(\sqrt{u} : u \in O_H^*)$. The Kummer map

$$\mathrm{Gal}(L/H) \longrightarrow \mathrm{Hom}(V(\overline{\mathbf{Q}}), V^\vee(\overline{\mathbf{Q}})),$$

is given by $\sigma \mapsto f_\sigma$ where $f_\sigma(P) = \sigma(P') - P'$, where P' is any point in $W(\overline{\mathbf{Q}})$ that is mapped to $P \in V(\overline{\mathbf{Q}})$. It is injective and Δ-linear. Since the non-split extension W is determined by its Galois module, the group $\mathrm{Gal}(L/H)$ is therefore isomorphic to a *non-zero* $\mathbf{F}_2[\Delta]$-submodule of $\mathrm{Hom}(V(\overline{\mathbf{Q}}), V^\vee(\overline{\mathbf{Q}}))$.

Claim. There is a natural exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_{\underline{Gr},[2]}(W,V) \longrightarrow \mathrm{Ext}^1_{\mathbf{Z}[\frac{1}{2p}],[2]}(W,V) \longrightarrow \mathrm{Ext}^1_{\mathbf{Q}_2,[2]}(W,V).$$

Proof of the claim. For each of the rings $R = \mathbf{Z}[\frac{1}{p}]$, $\mathbf{Z}[\frac{1}{2p}]$, $\mathbf{Z}_2$ and $\mathbf{Q}_2$ consider the exact sequence

$$0 \longrightarrow \mathrm{Hom}_R(V,V) \xrightarrow{\phi} \mathrm{Hom}_R(W,V) \longrightarrow \mathrm{Hom}_R(V^\vee,V)$$

Since V is étale and $V^\vee$ is connected, the right hand side group vanishes for $R = \mathbf{Z}_2$ and hence for $R = \mathbf{Z}[\frac{1}{p}]$. Over the rings $R = \mathbf{Z}[\frac{1}{2p}]$ or $\mathbf{Q}_2$ the group schemes W, V and $V^\vee$ are étale and we identify them with their Galois modules. By Assumption 3.1 the primes over 2 are totally ramified in $H \subset L$. Therefore the decomposition subgroup of π of each of the primes lying over 2 is equal to $N = \mathrm{Gal}(L/\mathbf{Q}(\sqrt{-p}))$ and we have $\mathrm{Gal}(L/H) \subset N$.

Let σ be a non-identity automorphism in $\mathrm{Gal}(L/H)$ and let $f \in \mathrm{Hom}_R(W,V)$. Then f and $\sigma - \mathrm{id}$ commute. Since $\sigma - \mathrm{id}$ induces the zero map on the quotient V of W, we have that $f(\sigma - \mathrm{id}) = (\sigma - \mathrm{id})f = 0$ on W. The image of $\sigma - \mathrm{id}$ is a non-trivial submodule of $V^\vee$. Therefore $\ker f \cap V^\vee \neq 0$. Since for both rings R, the Galois module $V^\vee$ is irreducible, $V^\vee$ is contained in the kernel of f. This means that f is in the image of ϕ.

We conclude that for all four rings R the homomorphism ϕ is a bijection. It follows then from Example 3.3 that the order of $\mathrm{Hom}_R(W,V)$ is equal to 2, 2, 4 and 4 for $R = \mathbf{Z}[\frac{1}{p}]$, $\mathbf{Z}[\frac{1}{2p}]$, $\mathbf{Z}_2$ and $\mathbf{Q}_2$ respectively. This implies that the 'Hom part' of the Mayer-Vietoris exact sequence [9, Cor. 2.4] associated to W and V is exact. The rest of the sequence only involves Ext-groups and is almost the sequence that we are looking for. It remains exact when we replace the Ext-groups by their subgroups of extensions that are killed by 2. Finally, since the leftmost and rightmost terms of the exact sequence

$$\mathrm{Ext}^1_{\mathbf{Z}_2,[2]}(V,V) \longrightarrow \mathrm{Ext}^1_{\mathbf{Z}_2,[2]}(W,V) \longrightarrow \mathrm{Ext}^1_{\mathbf{Z}_2,[2]}(V^\vee,V),$$

are zero, we have that $\mathrm{Ext}^1_{\mathbf{Z}_2,[2]}(W,V) = 0$ and we recover the exact sequence of the claim.

The exact sequence of low degree terms of the spectral sequence

$$H^p(\pi, \mathrm{Ext}^q(W(\overline{\mathbf{Q}}), V(\overline{\mathbf{Q}}))) \implies \mathrm{Ext}^{p+q}_{\mathrm{ab}}(W(\overline{\mathbf{Q}}), V(\overline{\mathbf{Q}}))$$

gives rise to the natural isomorphism

$$H^1(\pi, \mathrm{Hom}(W(\overline{\mathbf{Q}}), V(\overline{\mathbf{Q}}))) \;\cong\; \mathrm{Ext}^1_{\mathbf{Z}[\frac{1}{2p}],[2]}(W,V).$$

There is a similar isomorphism for the normal subgroup N of π and the following diagram commutes

$$\begin{array}{ccc} H^1(\pi, \mathrm{Hom}(W(\overline{\mathbf{Q}}), V(\overline{\mathbf{Q}}))) & \stackrel{\mathrm{Res}}{\longrightarrow} & H^1(N, \mathrm{Hom}(W(\overline{\mathbf{Q}}), V(\overline{\mathbf{Q}}))) \\ \downarrow\cong & & \downarrow\cong \\ \mathrm{Ext}^1_{\mathbf{Z}[\frac{1}{2p}],[2]}(W,V) & \longrightarrow & \mathrm{Ext}^1_{\mathbf{Q}_2,[2]}(W,V), \end{array}$$

the Hochschild-Serre spectral sequence and the exact sequence of the claim provide us with an isomorphism

$$\mathrm{Ext}^1_{\underline{Gr},[2]}(W,V) \;\cong\; H^1(\pi/N, \mathrm{Hom}_N(W(\overline{\mathbf{Q}}), V(\overline{\mathbf{Q}}))).$$

Since $\mathrm{Hom}_N(W(\overline{\mathbf{Q}}), V(\overline{\mathbf{Q}}) = \mathrm{Hom}_{\mathbf{Q}_2}(W,V) = \mathrm{Hom}_{\mathbf{Q}_2}(V,V) = \mathbf{F}_4$, we find

$$\mathrm{Ext}^1_{\underline{Gr},[2]}(W,V) \;\cong\; H^1(\pi/N, \mathbf{F}_4).$$

Here $\mathbf{F}_4 = \mathbf{F}_2[\tau]/(\tau^2+\tau+1)$. The group π/N acts on $\mathbf{F}_4$ by conjugation. An easy computation shows that $H^1(\pi/N, \mathbf{F}_4) = 0$ and hence

$$\mathrm{Ext}^1_{\underline{Gr},[2]}(W,V) = 0.$$

This leads to a contradiction. Indeed, the homomorphism

$$\mathrm{Ext}^1_{\underline{Gr},[2]}(W,V) \longrightarrow \mathrm{Ext}^1_{\underline{Gr},[2]}(V^\vee,V)$$

maps the class of G to the class of Ψ and is hence *surjective* onto the order 2-group $\mathrm{Ext}^1_{\underline{Gr},[2]}(V^\vee,V)$. It follows that W must be split. This proves the lemma. □

Corollary 4.7. *Under Assumption 3.1 on the prime p, the groups* $\mathrm{Ext}^1_{\underline{C}}(V,\Psi)$ *and* $\mathrm{Ext}^1_{\underline{C}}(\Psi,V^\vee)$ *are* 1*-dimensional vector spaces over the field* $\mathrm{End}(\Psi) \cong \mathbf{F}_4$.

Proof. By Lemma 4.6 the group $\mathrm{Ext}^1_{\underline{C},[2]}(V,\Psi)$ is trivial. It follows therefore from [11, Lemma 2.1] that the natural map

$$\mathrm{Ext}^1_{\underline{C}}(V,\Psi) \;\hookrightarrow\; \mathrm{Hom}(V(\overline{\mathbf{Q}}), \Psi(\overline{\mathbf{Q}}))^\Delta$$

is injective. Since the Galois module $\Psi(\overline{\mathbf{Q}})$ is isomorphic to $V(\overline{\mathbf{Q}})^2$, the group on the right is $(\mathrm{End}(V(\overline{\mathbf{Q}})) \times \mathrm{End}(V(\overline{\mathbf{Q}})))^\Delta$. Since the Δ-invariants of $\mathrm{End}(V(\overline{\mathbf{Q}}))$ are isomorphic to $\mathbf{F}_2$, we conclude that $\#\mathrm{Ext}^1_{\underline{C}}(V,\Psi) \le 4$. By Proposition 4.5, the ring $\mathrm{End}(\Psi)$ is isomorphic to $\mathbf{F}_4$. It follows that $\mathrm{Ext}^1_{\underline{C}}(V,\Psi)$ is an $\mathbf{F}_4$-vector space of dimension ≤ 1. By Proposition 4.2 the natural map $\mathrm{Ext}^1_{\underline{C}}(V,V) \hookrightarrow \mathrm{Ext}^1_{\underline{C}}(V,\Psi)$ is injective. It follows from Example 3.3 that $\mathrm{Ext}^1_{\underline{C}}(V,\Psi)$ is not zero and we are done. The statement concerning $\mathrm{Ext}^1_{\underline{C}}(\Psi,V^\vee)$ follows by Cartier duality. This proves the corollary. □

Theorem 4.8. *Under the Assumptions 3.1, the group* $\mathrm{Ext}^1_{\underline{C}}(\Psi,\Psi)$ *is a vector space over the field* $\mathrm{End}(\Psi)\cong \mathbf{F}_4$ *of dimension* ≤ 1.

Proof. By Proposition 4.3 the group $\mathrm{Ext}^1_{\underline{C}}(V^\vee,\Psi)$ vanishes. Therefore the natural map

$$\mathrm{Ext}^1_{\underline{C}}(\Psi,\Psi) \hookrightarrow \mathrm{Ext}^1_{\underline{C}}(V,\Psi)$$

is injective. The result now follows from Corollary 4.7. $\square$

5. The simple objects of the category $\underline{C}$.

In this section we let $p=23$. We show that in this case the simple objects of the category $\underline{C}$ introduced in section 2 are $\mathbf{Z}/2\mathbf{Z}$, μ_2 and the group schemes V and $V^\vee$ introduced in section 3. It is not very useful and we do indeed make no use of it, but the reader may verify that the Hopf algebra of V is equal to $\mathbf{Z}[\frac{1}{23}][X]/(X(X^3-X-1))$ with addition formula

$$x+y+\frac{2xy}{23}\left(35+4(x+y)-18(x^2+y^2)+9xy-6(x^2y+xy^2)+4x^2y^2\right).$$

The points of this group scheme generate the Hilbert class field H of $\mathbf{Q}(\sqrt{-23})$.

Proposition 5.1. *Let G be a simple object of the category $\underline{C}$ introduced in section 2. Then its points are rational over the Hilbert class field H of* $\mathbf{Q}(\sqrt{-23})$.

Proof. Let G be a simple 2-power order group scheme in the category $\underline{C}$. Then G is killed by 2. The action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on $G(\overline{\mathbf{Q}})$ is unramified outside 2, p and ∞. Let L be the number field generated by the points of G and let $\pi=\mathrm{Gal}(L/\mathbf{Q})$. Since G is an object of $\underline{C}$ that is killed by 2, the field L is at most tamely ramified of index ≤ 2 at the primes lying over p. By the theorems of Fontaine [3] or Abrashkin [1], the higher ramification subgroups of π at the primes over 2 are trivial when their index in Fontaine's higher numbering [3, p.515] exceeds 2. An easy computation [3, Cor.3.3.2] shows that the root discriminant of L is at most $4\sqrt{23}=19.18\ldots$

Examples of Galois extensions of $\mathbf{Q}$ satisfying the same restrictions on the ramification groups are $\mathbf{Q}(i)$ and H. Both fields are in fact generated by the points of an object in the category $\underline{C}$. The restrictions on the ramification groups behave well under composition. Therefore there is a *maximal* field inside $\overline{\mathbf{Q}}$ satisfying the restrictions. We call this field L again. It contains $H(i)$. The root discriminant of L satisfies the same inequality. Therefore Odlyzko's discriminant bounds [8] imply the inequality $[L:\mathbf{Q}]<300$ and hence $[L:H(i)]\leq 24$. It follows that the group $\pi=\mathrm{Gal}(L/\mathbf{Q})$ is solvable.

The Galois group of $\mathbf{Q}(\zeta_8)$ over $\mathbf{Q}(i)$ is the higher ramification subgroup of $\mathrm{Gal}(\mathbf{Q}(\zeta_8)/\mathbf{Q})$ of index 3 in Fontaine's upper numbering. Therefore the field $\mathbf{Q}(\zeta_8)$ does not satisfy the conditions on the ramification at the prime lying over 2. So by the Kronecker-Weber Theorem the field $F=\mathbf{Q}(i,\sqrt{-23})$ is the maximal abelian extension of $\mathbf{Q}$ inside L and hence $\mathrm{Gal}(L/F)$ is equal to the commutator subgroup π' of π.

We have the following inclusions

$$\mathbf{Q} \underset{4}{\subsetneq} F \underset{3}{\subsetneq} H(i) \underset{\leq 24}{\subset} L.$$

The Galois group of $H(i)$ over $\mathbf{Q}$ is isomorphic to $S_3 \times C_2$.

Claim. The maximal abelian extension of F inside L is $H(i)$ and hence the group $\mathrm{Gal}(L/H(i))$ is equal to π''.

Proof of the claim. Clearly $H(i)$ is an abelian extension of F. We show that $H(i)$ is the maximal such extension inside L. Since F is ramified at 23, the extension $F \subset L$ is unramified at 23 and hence is unramified outside 2. The root discriminant of F is equal to $2\sqrt{23} = 9.59\ldots$. By Odlyzko's bounds any everywhere unramified extension of F has degree at most 20 over $\mathbf{Q}$. Since $H(i)$ is everywhere unramfied over F and since $[H(i) : \mathbf{Q}] = 12$, the field $H(i)$ admits no non-trivial everywhere unramified extensions and must be the maximal everywhere unramified extension of F inside L. The two primes over 2 in F have residue fields isomorphic to $\mathbf{F}_2$. The ray class group of F of conductor $(1+i)^3$ is equal to $(O_F/(1+i)^3 O_F)^*$ modulo the group $O_F^* = \langle i, \eta \rangle$. Here η is the unit given by

$$\eta = \frac{5+\sqrt{23}}{1-i} = \frac{5-\sqrt{-23}}{2} + \frac{5+\sqrt{-23}}{2} i.$$

The square of η is equal to $i\varepsilon$ where $\varepsilon = 24 - 5\sqrt{23}$ is a fundamental unit of the real quadratic field $\mathbf{Q}(\sqrt{23})$. A short computation shows that the units i and η *generate* the group $(O_F/(1+i)^3 O_F)^*$. This means that the ray class field of F of conductor $(1+i)^3$ is equal to F itself. Any quadratic extension of F of conductor divisible by $(1+i)^4 = (4)$ is too ramified at the primes over 2, in the sense that its Galois group over $\mathbf{Q}$ admits non-trivial ramification subgroups of upper index exceeding 2. It follows that a quadratic extension of conductor divisible by $(1+i)^4$ cannot be contained in L. We conclude that the maximal abelian extension of F inside L is equal to $H(i)$ and hence that the Galois group $\mathrm{Gal}(L/H(i))$ is equal to π''. This proves the claim.

We proceed by determining the maximal abelian extension of $H(i)$ inside L. We know that $H(i) \subset L$ is unramified outside 2 and we already saw that $H(i)$ admits no non-trivial everywhere unramified extension inside L. The two primes in $H(i)$ lying over 2 have residue fields isomorphic to $\mathbf{F}_8$ and the action of $\mathrm{Gal}(H(i)/\mathbf{Q})$ on $\mathbf{F}_8^* \times \mathbf{F}_8^*$ is irreducible. A short computation shows that global units provided by the zeroes of $T^3 - T + 1$ generate a non-zero $\mathrm{Gal}(H(i)/\mathbf{Q})$-submodule. Therefore the ray class group of $H(i)$ of conductor $(1+i)$ is trivial. Class field theory implies then that π''/π''' is a 2-group. Since $[L : H(i)] \leq 24$, it has order ≤ 16.

The rest of the argument is a group theoretic exercise: if π is a finite group with $\pi/\pi'' \cong S_3 \times C_2$ and for which $\#\pi'' \leq 24$ and π''/π''' is a 2-group, then π'' is a 2-group. The proposition now follows from the fact that $\mathrm{Gal}(L/H)$ is also a 2-group and therefore it has non-zero fixed points in the 2-group $G(\overline{\mathbf{Q}})$. Since G is simple, $G(\overline{\mathbf{Q}})$ is therefore fixed by $\mathrm{Gal}(L/H)$ as required. $\square$

Theorem 5.2. *The only simple group schemes in the category $\underline{C}$ are μ_2, $\mathbf{Z}/2\mathbf{Z}$, V and its Cartier dual $V^\vee$.*

Proof. Let G be a simple object. Then G is killed by 2. By Proposition 5.1, the group $G(\overline{\mathbf{Q}})$ is a simple $\mathbf{F}_2[\Delta]$-module. Recall that $\Delta = \mathrm{Gal}(H/\mathbf{Q})$ is isomorphic to S_3. So either $G(\overline{\mathbf{Q}})$ has order 2 and trivial Galois action or it has order 4 with irreducible Galois action. In the first case the Oort-Tate theorem implies that we have $G \cong \mathbf{Z}/2\mathbf{Z}$ or $G \cong \mu_2$. In the second case, the action of the local Galois group at the primes over 2 is also irreducible. This follows from the fact that the primes over 2 are inert in the cubic extension $\mathbf{Q}(\sqrt{-23}) \subset H$. Therefore G is either étale or local over $\mathbf{Z}_2$. If G is étale, Galois theory implies $G \cong V$. If G is local, we twist the Galois action with the 2-dimensional representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Gal}(H/\mathbf{Q}) \cong \mathrm{GL}_2(\mathbf{F}_2)$. Then $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts trivially on the points of the twisted group scheme $G(\rho)$. Let M be the Zariski closure of one of the subgroups of order 2. An application of the Oort-Tate theorem over the ring $\mathbf{Z}[\frac{1}{23}]$ shows that both M and the quotient $G(\rho)/M$ are isomorphic to μ_2. This leads to an exact sequence of group schemes over $\mathbf{Z}[\frac{1}{23}]$ of the form

$$0 \longrightarrow \mu_2 \longrightarrow G(\rho) \longrightarrow \mu_2 \longrightarrow 0.$$

It follows that the Cartier dual $G(\rho)^\vee$ is étale. Since it is killed by 2 and has trivial Galois action, we must have $G(\rho)^\vee \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Therefore G is dual to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ twisted by ρ. So G is isomorphic to $V^\vee$.

This proves the theorem. □

The next proposition shows that Assumption 3.1 is satisfied for $p = 23$.

Proposition 5.3. *Let H denote the Hilbert class field of $\mathbf{Q}(\sqrt{-23})$. Then*

(a) the ray class field of H of conductor $\sqrt{-23}$ is equal to H;

(b) let $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ denote the primes over 2 in H. Then the ray class fields of conductors $\mathfrak{q}^2$ and $\overline{\mathfrak{q}}^2$ are both equal to H.

Proof. A standard computation employing Odlyzko's bounds shows that the only unramified extension of H is H itself. We leave this to the reader. For $a = (-3+\sqrt{-23})/2$ the cubic polynomial $f(X) = X^3 + aX^2 - (a+3)X + 1$ has discriminant 1. Its zeroes are units contained in H.

(a) The prime $\sqrt{-23}$ of $\mathbf{Q}(\sqrt{-23})$ is principal and splits in H. Therefore there are three primes lying over 23 in H corresponding to the three linear factors of the polynomial $f \pmod{\sqrt{23}}$. We have

$$f(X) \equiv X^3 - \tfrac{3}{2}X^2 - \tfrac{3}{2}X + 1 \equiv (X-2)(X-12)(X-22) \pmod{\sqrt{-23}}$$

The zeroes 2, 12, 22 are a square, a square and a non-square respectively in $\mathbf{F}_{23}$. This means that the images of the zeroes of f in the 3-dimensional $\mathbf{F}_2$-vector space

$$(O_H/(\sqrt{-23}))^*/(O_H/(\sqrt{-23}))^{*2}$$

are the cyclic permutations of the vector $(0,0,1)$. It follows that the ray class group of conductor $\sqrt{-23}$ is trivial.

(b) Both primes $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ have residue field $\mathbf{F}_8$. Let $\mathfrak{q}$ be the prime over 2 that divides a. Since $(a) = \mathfrak{q}^3$, we have

$$f(X) \equiv X^3 + X + 1 \pmod{\mathfrak{q}^2}.$$

It follows that the images of the zeroes of f in the order 7 group $(O_H/(2))^*$ generate the whole group. This means that the ray class group of conductor $\mathfrak{q}$ is trivial. Finally we compute the ray class group of conductor $\mathfrak{q}^2$. The seventh power of any unit $\varepsilon \in O_H^*$ is congruent to 1 (mod 2). We have $(-1)^7 \equiv 1 + 2 \cdot 1 \pmod{\mathfrak{q}^2}$ and for a zero u of f we have $u^7 \equiv 1 + 2u^2 \pmod{\mathfrak{q}^2}$. Since the additive subgroup of $O_H/\mathfrak{q}$ is generated by 1 and by u and its conjugates u^2 and u^4, the ray class group of conductor $\mathfrak{q}^2$ is trivial. The same is true with the prime $\mathfrak{q}$ replaced by $\overline{\mathfrak{q}}$. This proves the proposition. □

6. The modular curve.

In this section we let $p = 23$ and we study the Jacobian $J = J_0(23)$ of the modular curve $X_0(23)$. The following equation for $X_0(23)$ was obtained by J. Gonzàlez Rovira [4, p.794]:

$$y^2 = (x^3 - x + 1)(x^3 - 8x^2 + 3x - 7).$$

This curve has genus 2 and is hyperelliptic. Since J has good reduction outside 23 and semi-stable reduction at 23, the group schemes $J[2^n]$ of 2^n-torsion points are objects of the category $\underline{C}$ introduced in section 2.

Proposition 6.1. *The group scheme $J[2]$ is isomorphic to the group scheme Ψ introduced in section 4.*

Proof. The group scheme $J[2]$ has order 16 and is an object of $\underline{C}$. Theorem 5.2 implies that it admits a filtration with flat closed subgroup schemes and successive quotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$, μ_2 or the group schemes V and $V^\vee$ introduced in section 3. Since the two points at infinity of $X_0(23)$ are rational, the points of the group $J[2](\overline{\mathbf{Q}})$ generate the same field as the zeroes of $(x^3-x+1)(x^3-8x^2+3x-7)$. A simple computation shows that this field is the Hilbert class field H of $\mathbf{Q}(\sqrt{-23})$.

Since $\mathrm{Gal}(H/\mathbf{Q})$ is not a 2-group, one of the simple group schemes V and $V^\vee$ must be a subquotient of $J[2]$. Since $J[2]$ is self-dual, so must the other. It follows that $J[2]$ is an extension of V by $V^\vee$ or the other way around. If there is a non-split exact sequence

$$0 \longrightarrow V \longrightarrow J[2] \longrightarrow V^\vee \longrightarrow 0,$$

then we are done by the uniqueness proved in Proposition 4.1. If there is no such sequence, then $J[2]$ is isomorphic to G, where G sits in an exact sequence of the form

$$0 \longrightarrow V^\vee \longrightarrow G \longrightarrow V \longrightarrow 0,$$

that may or may not be split. The Hecke algebra $\mathbf{T}$ acts on $J[2]$. It is known [7, Table B] that $\mathbf{T}$ is isomorphic to the ring $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$. Therefore $\mathbf{T}/2\mathbf{T} \cong \mathbf{F}_4$ injects into $\mathrm{End}(G)$. It follows that the ring $\mathrm{End}(G)$ is an $\mathbf{F}_4$-algebra. By Example 3.3 and Proposition 3.4 an application of the bifunctor $\mathrm{Hom}(-,-)$ to the exact sequence $0 \to V^\vee \to G \to V \to 0$ shows that $\#\mathrm{End}(G) \leq 2\cdot 2\cdot 2 = 8$. Then we must have $\#\mathrm{End}(G) = 4$ and hence $\mathrm{End}(G) \cong \mathbf{F}_4$.

However, $\mathrm{End}(G)$ cannot be a field. Indeed, let f be the the composition of morphisms

$$G \to V \longrightarrow V^\vee \hookrightarrow G,$$

where the middle arrow is the unique non-zero morphism $V \to V^\vee$. Then $f : G \longrightarrow G$ is a non-zero endomorphism whose square is zero. Contradiction.

This proves the proposition. □

Corollary 6.2. *For $p = 23$, the group $\mathrm{Ext}^1_{\underline{C}}(\Psi, \Psi)$ is a vector space over $\mathrm{End}(\Psi) \cong \mathbf{F}_4$ of dimension 1.*

Proof. By Proposition 4.8 the $\mathbf{F}_4$-dimension of $\mathrm{Ext}^1_{\underline{C}}(\Psi, \Psi)$ is at most 1. The group scheme $J[4]$ is an object of the category $\underline{C}$ that is a non-trivial extension of Ψ by Ψ. Therefore the dimension is exactly 1. □

Proof of Theorem 1.1. Let A be a semistable abelian variety over $\mathbf{Q}$ admitting good reduction outside 23. For any $n \geq 1$, the group scheme $A[2^n]$ is an object of the category $\underline{C}$. By Theorem 5.2 it admits a filtration with closed flat subgroup schemes and simple subquotients, which are isomorphic to one of the simple group schemes $\mathbf{Z}/2\mathbf{Z}$, μ_2, V and $V^\vee$.

By Theorem 3.7 the group scheme $A[2^n]$ admits therefore a filtration of the form

$$0 \hookrightarrow G_{n,1} \hookrightarrow G_{n,2} \hookrightarrow A[2^n],$$

where $G_{n,1}$ becomes diagonalizable and the group scheme $A[2^n]/G_{n,2}$ becomes constant over the ring $\mathbf{Z}[\frac{1+\sqrt{-23}}{2}, \frac{1}{23}]$. The quotient $G_{n,2}/G_{n,1}$ is isomorphic to $E_n \times E'_n$ as in Thm 3.7 and is discussed below. Let $\mathfrak{p}$ be a prime ideal of $\mathbf{Z}[\frac{1+\sqrt{-23}}{2}, \frac{1}{23}]$ not dividing $2\cdot 23$ and let $k_\mathfrak{p}$ denote its residue field. Let A' denote the abelian variety $A/G_{n,2}$. Since reduction modulo $\mathfrak{p}$ maps the group of points of the constant group scheme $A[2^n]/G_{n,2}$ *injectively* into the finite group $A'(k_\mathfrak{p})$, we see that $\#(A[2^n]/G_{n,2}) \leq \#A'(k_\mathfrak{p}) = \#A(k_\mathfrak{p})$. This shows that $\#(A[2^n]/G_{n,2})$ is bounded as n grows. Similarly, using Cartier duality, one shows that $\#G_{n,1}$ remains bounded as n grows.

By Theorem 3.7 the subquotient $G_{n,2}/G_{n,1}$ satisfies

$$G_{n,2}/G_{n,1} \;\cong\; E_n \times E'_n,$$

where E'_n is a successive extension of group schemes isomorphic to Φ and E_n admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to V or $V^\vee$. Since $23 \equiv 7 \pmod{16}$, Theorem 2.7 implies that E'_n is actually a *direct product* of group schemes isomorphic to Φ. Therefore E'_n is killed by 2 and hence $\#E'_n$ is bounded as n grows.

Theorem 4.4 implies that for each $n \geq 1$, the group scheme E_n admits a filtration of the form
$$0 \hookrightarrow H_{n,1} \hookrightarrow H_{n,2} \hookrightarrow E_n,$$
where $E_n/H_{n,2}$ becomes constant and $H_{n,1}$ becomes diagonalizable over $O_H[\frac{1}{23}]$. In addition the quotient $H_{n,2}/H_{n,1}$ admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to the group scheme Ψ. By the same arguments as above, reducing modulo a suitable prime of the ring $O_H[\frac{1}{23}]$ shows then that $\#(E_n/H_{n,2})$ and $\#H_{n,1}$ remain bounded as $n \to \infty$.

By Corollary 6.2 the group $\mathrm{Ext}^1_{\underline{C}}(\Psi, \Psi)$ is a vector space over $\mathrm{End}(\Psi) \cong \mathbf{F}_4$ of dimension 1. Indeed, it is generated by the class of $J[4]$. As in [10, section 8] one proves by induction that for every $n \geq 1$ the group scheme $H_{n,2}/H_{n,1}$ is the product of group schemes of 2-power torsion points of the abelian variety J. We have
$$H_{n,2}/H_{n,1} \;\cong\; \bigoplus_{j=1}^{t_n} J[2^{m_{n,j}}],$$
for certain non-negative integers t_n and $m_{n,j}$.

Now we let n grow. Put $g' = \dim A$. The underlying group of $A[2^n]$ is a product of $2g'$ cyclic groups of order 2^n. The orders of the group schemes $G_{n,1}$, $A[2^n]/G_{n,2}$, E'_n, $H_{n,1}$ and $E_n/H_{n,2}$ remain bounded as n grows. This implies that $\#(H_{n,2}/H_{n,1})/2^{2ng'}$ is bounded as $n \to \infty$ and hence that there are morphisms of group schemes
$$f_n : A[2^n] \longrightarrow J[2^n]^g, \qquad n \geq 1,$$
with the property that $\#\ker f_n$ and $\#\mathrm{coker}\, f_n$ remain bounded as n grows. Here g satisfies $2g = g'$. The morphisms are not necessarily compatible, but there is a cofinal compatible system. Taking the limit we obtain an exact sequence of 2-divisible groups
$$0 \longrightarrow K \longrightarrow A_{\mathrm{div}} \longrightarrow J^g_{\mathrm{div}} \longrightarrow 0.$$
Here K is a finite closed flat subgroup scheme of A. By Faltings' theorem [2] the abelian varieties A and J^g are therefore isogenous over $\mathbf{Q}$. Since A is simple, it is isogenous to J itself.

This proves Theorem 1.1.

References

[1] Abraškin, V.A.: Galois moduli of period p group schemes over a ring of Witt vectors, *Izv. Ak. Nauk USSR*, Ser. Matem., **51** (1987), 691–736. English translation in *Math. USSR Izvestiya*, **31** (1988) 1–46.

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

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

[4] Gonzalez Rovira, J.: Equations of hyperelliptic modular curves, *Annales de l'institut Fourier* **41** (1991), 779–795.

[5] 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.

[6] Hurwitz, A. Über die Anzahl der Classen binärer quadratischer Formen von negativer Determinante, *Acta Mathematica* **19** (1895), 351–384.

[7] Miyake, T.: *Modular Forms*, Springer-Verlag, New York 1989.

[8] Odlyzko, A.M.: Unconditional bounds for discriminants, manuscript 1976. Scanned version at http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table2

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

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

[11] Schoof, R.: Semistable abelian varieties with good reduction outside 15, *Manuscripta Mathematica*, 2012. To appear.

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

Dipartimento di Matematica, 2^a Università di Roma “Tor Vergata”, Via della ricerca scientifica, I-00133 Roma, ITALY

E-mail: schoof@mat.uniroma2.it