



## On the modular curve $X_0(23)$

René Schoof

Dipartimento di Matematica  
2<sup>a</sup> Università di Roma “Tor Vergata”  
I-00133 Roma ITALY  
Email: [schoof@mat.uniroma2.it](mailto:schoof@mat.uniroma2.it)

**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. We prove that it is the only simple abelian variety with this property: every semi-stable abelian variety over  $\mathbf{Q}$  with good reduction outside 23 is isogenous over  $\mathbf{Q}$  to a power of  $J_0(23)$ .

### 1. Introduction.

The modular curve  $X_0(23)$  parametrizes elliptic curves together with a subgroup of order 23. An explicit equation is given by

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

The curve  $X_0(23)$  has genus 2 and is defined over  $\mathbf{Q}$ . Its Jacobian variety  $J_0(23)$  is a semi-stable abelian variety over  $\mathbf{Q}$ , that is absolutely simple and admits good reduction at every prime different from 23. The next theorem is our main result. It 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.

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

The approach of this paper is a bit more general: we study for an odd prime  $p$  the category  $\underline{\mathcal{C}}$  of finite flat commutative 2-power order group schemes  $G$  over  $\mathbf{Z}[\frac{1}{p}]$  with the property that for each  $\sigma$  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, the 2-power order torsion points of semi-stable abelian varieties  $A$  over  $\mathbf{Q}$  with good reduction outside  $p$  are objects of  $\underline{\mathcal{C}}$ . In particular, the 2-power order torsion points of  $J_0(p)$  are objects of  $\underline{\mathcal{C}}$ . Theorems 3.7 and 4.4 give a rough classification of the objects in  $\underline{\mathcal{C}}$ .

For  $p = 23$  it follows from the classification that the 2-divisible group of a semi-stable abelian variety  $A$  as in Theorem 1.1 is isogenous to the 2-divisible group of  $J_0(23)^g$  for a suitable  $g \geq 0$ . Faltings' theorem implies then that  $A$  is isogenous to  $J_0(23)^g$ .

The main complication in our proof is 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  $\Gamma = \text{Gal}(H/\mathbf{Q})$  and  $V^\vee$  is its Cartier dual. Here  $H$  is the Hilbert class field of  $\mathbf{Q}(\sqrt{-23})$  and  $\Gamma$  is isomorphic to the symmetric group  $S_3$ .

We show that the extension does *not split* over  $\mathbf{Z}[\frac{1}{23}]$ , but does split over  $\mathbf{Q}$  and over all completions of  $\mathbf{Z}[\frac{1}{23}]$ . On the other hand, the group scheme  $J_0(23)[2]$  has irreducible features in the sense that its endomorphism ring  $R$  over  $\mathbf{Z}[\frac{1}{23}]$  is a field of 4 elements. In fact, the Hecke algebra  $\mathbf{T}$  is isomorphic to  $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$  and the natural map  $\mathbf{T}/2\mathbf{T} \longrightarrow R$  is a ring isomorphism.

The paper is organized as follows. Under certain assumptions on the prime  $p$  we describe in sections 2–4 the objects of the category  $\underline{\mathcal{C}}$  as precisely as we can. The main results are Theorems 2.7, 3.7, 4.4 and 4.8. In section 2 we construct for  $p \equiv \pm 1 \pmod{8}$  the unique non-split extension  $\Phi$  of  $\mu_2$  by  $\mathbf{Z}/2\mathbf{Z}$  over the ring  $\mathbf{Z}[\frac{1}{p}]$ . The group scheme  $\Phi$  is an object of  $\underline{\mathcal{C}}$ . In sections 3 and 4 we make more assumptions on the prime  $p$ . These are satisfied by  $p = 23$  and probably infinitely many other primes. We construct the group schemes  $V$  and  $V^\vee$  and the unique non-split extension  $\Psi$  of  $V^\vee$  by  $V$  over the ring  $\mathbf{Z}[\frac{1}{p}]$ . The group schemes  $V$ ,  $V^\vee$  and  $\Psi$  are objects of  $\underline{\mathcal{C}}$ . In section 2–4 we determine various extensions of the group schemes  $\mathbf{Z}/2\mathbf{Z}$ ,  $\mu_2$ ,  $\Phi$ ,  $V^\vee$ ,  $V$  and  $\Psi$  by one another.

In section 5 we specialize to the case  $p = 23$ . In this case the group scheme  $\Psi$  is isomorphic to  $J_0(23)[2]$ . We show that the simple objects in the category  $\underline{\mathcal{C}}$  are the group schemes  $\mathbf{Z}/2\mathbf{Z}$ ,  $\mu_2$ ,  $V$  and  $V^\vee$ . For  $p = 23$  Theorems 2.7, 3.7, 4.4 and 4.8 lead to a classification of the objects of  $\underline{\mathcal{C}}$ , which is fine enough for our purposes. Finally, in section 6 we consider the modular curve  $X_0(23)$  and prove Theorem 1.1

## 2. The category $\underline{C}$ and the group schemes $\mathbf{Z}/2\mathbf{Z}$ and $\mu_2$ .

In this section  $p$  is an odd prime.

**Definition.** Let  $\underline{C}$  be the full subcategory of the category of finite flat commutative 2-power order group schemes over the ring  $\mathbf{Z}[\frac{1}{p}]$  whose objects  $G$  have the property that for every  $\sigma$  in an inertia subgroup of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  of any of the primes lying over  $p$ , the endomorphism  $(\sigma - 1)^2$  acts as zero on the group of points  $G(\overline{\mathbf{Q}})$ .

By A. Grothendieck [5, Cor.3.5.2], for every semi-stable 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  $\underline{C}$ . So are the constant group schemes  $\mathbf{Z}/2^k\mathbf{Z}$  and their Cartier duals  $\mu_{2^k}$ . The group schemes  $\mathbf{Z}/2\mathbf{Z}$  and  $\mu_2$  are *simple* objects of  $\underline{C}$ .

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

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

There is an analogous contravariant exact sequence. In general, the group  $\text{Ext}_{\underline{C}}^1(H, G)$  is strictly smaller than the group  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(H, G)$  of *all* extensions of  $H$  by  $G$ . The two extension groups are equal when the Galois action on the points of  $G$  and  $H$  is unramified at  $p$ . This happens for instance when both  $G$  and  $H$  are isomorphic to  $\mathbf{Z}/2\mathbf{Z}$  or  $\mu_2$ .

In the rest of this section we work in the category  $\underline{C}$  and we study various extensions of the group schemes  $\mathbf{Z}/2\mathbf{Z}$  and  $\mu_2$  by one another.

**Proposition 2.1.** *Over the ring  $\mathbf{Z}[\frac{1}{p}]$  we have the following.*

- (a) *the group  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$  has dimension 2 and is generated by the class of  $\mathbf{Z}/4\mathbf{Z}$  and a 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  $\chi_p : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathbf{F}_2$  is the character that corresponds to the quadratic subfield of  $\mathbf{Q}(\zeta_p)$ ;

- (b) *the group  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mu_2, \mu_2)$  has dimension 2 and is generated by the class of  $\mu_4$  and a group scheme killed by 2 on which the Galois group acts as in part (a).*

**Proof.** Part (a) follows from Galois theory and part (b) by Cartier duality.

**Proposition 2.2.** *Let  $F$  be the maximal 2-power degree subfield of  $\mathbf{Q}(\zeta_p)$ . Any extension over  $\mathbf{Z}[\frac{1}{p}]$  of copies of  $\mathbf{Z}/2\mathbf{Z}$  becomes constant over the ring  $O_F[\frac{1}{p}]$ . Similarly, any extension over  $\mathbf{Z}[\frac{1}{p}]$  of copies of  $\mu_2$  becomes diagonalizable over the ring  $O_F[\frac{1}{p}]$ .*

**Proof.** Let  $G$  be an extension of group schemes isomorphic to  $\mathbf{Z}/2\mathbf{Z}$ . Then  $G$  is étale and becomes constant over an unramified extension of  $\mathbf{Z}[\frac{1}{p}]$ . The Galois group acts on  $G(\overline{\mathbf{Q}})$  through the Galois group  $\pi$  of the maximal 2-power degree unramified Galois extension of  $\mathbf{Z}[\frac{1}{p}]$ . By class field theory  $\pi/\pi'$  is isomorphic to  $\text{Gal}(F/\mathbf{Q})$ . Since the Galois group of  $\mathbf{Q}(\zeta_p)$  over  $\mathbf{Q}$  is cyclic, so is  $\pi/\pi'$ . It follows that  $\pi$  is also cyclic. Therefore  $O_F[\frac{1}{p}]$  is the maximal unramified 2-power degree Galois extension of  $\mathbf{Z}[\frac{1}{p}]$ . This proves the proposition.

**Proposition 2.3.** *The group  $\text{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$  of extensions by  $\mathbf{Z}/2\mathbf{Z}$  by  $\mu_2$  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 group schemes  $G_u$  with  $u = -1$  or  $p$ .*

**Proof.** This is Kummer theory. See [11, Prop. 2.2] for the proof. 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  $\sigma \in \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  the entry  $\psi(\sigma)$  is given by  $\sigma(\sqrt{u})/\sqrt{u} = (-1)^{\psi(\sigma)}$ .

The group schemes described in Proposition 2.3 play no major 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. 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*

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

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

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

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  $\Phi$  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  $\Phi$  is self-dual. It is an object of  $\underline{C}$ . Since there are no non-zero homomorphisms  $\mu_2 \rightarrow \mathbf{Z}/2\mathbf{Z}$ , the ring  $\text{End}(\Phi)$  is isomorphic to  $\mathbf{F}_2$ .

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

$$0 \rightarrow \text{Hom}(\mathbf{Z}/2\mathbf{Z}, \mu_2) \rightarrow \text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \rightarrow \text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$$

The image of the unique non-zero morphism  $\mathbf{Z}/2\mathbf{Z} \rightarrow \mu_2$  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 Proposition 2.1 (a). Therefore the image of  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$  inside  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$  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  $\Upsilon$  be the extension

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

in  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$  that is the image of the class of  $\mathbf{Z}/4\mathbf{Z}$  in  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ .

A consideration of the composite morphism  $\Upsilon \rightarrow \Phi \rightarrow \mu_2$ , shows that the group scheme  $\Upsilon$  can also be viewed as an extension of  $\mu_2$  by  $\mathbf{Z}/4\mathbf{Z}$ . Similarly, the image of the map  $\text{Ext}^1(\mu_2, \mu_2) \rightarrow \text{Ext}^1(\Phi, \mu_2)$  is generated by the Cartier dual of  $\Upsilon$ . It is an extension of  $\mu_4$  by  $\mathbf{Z}/2\mathbf{Z}$ .

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

(a) *we have*

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

(b) *we have*

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

**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

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

The composite morphism  $G \rightarrow \Phi \rightarrow \mu_2$  gives rise to an exact sequence of the form

$$0 \rightarrow C \rightarrow G \rightarrow \mu_2 \rightarrow 0.$$

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,  $\psi$  is unramified at 2. Since  $G$  is an object of  $\underline{C}$  that is killed by 2, we have  $\sigma^2 = 1$  for each  $\sigma$  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  $\psi$  is then also unramified at  $p$ . It follows that  $\psi$  is everywhere unramified and hence trivial. Therefore the map  $h$  in the exact sequence

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

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  $\mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ . The extension  $\Upsilon$  of  $\mathbf{Z}/2\mathbf{Z}$  by  $\Phi$  defined above generates the kernel of the natural map

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

By [11, Lemma 2.1] the subgroup  $\mathrm{Ext}_{\underline{C}, [2]}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$  of extensions of  $\mathbf{Z}/2\mathbf{Z}$  by  $\Phi$  that are killed by 2 has index  $\leq 2$  inside  $\mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ . The fact that the group scheme  $\Upsilon$  is *not* killed by 2 implies that the index is equal to 2. It suffices therefore to show that  $\mathrm{Ext}_{\underline{C}, [2]}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$  has  $\mathbf{F}_2$ -dimension 1 or 0 depending on whether  $p \equiv 1 \pmod{8}$  or not.

Since the class of  $\Upsilon$  generates the kernel of  $\phi$ , the map

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

is injective. 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  $\phi$  maps the class of  $G$  to the extension of  $\mathbf{Z}/2\mathbf{Z}$  by  $\mu_2$  that is determined by  $\psi$ . Since  $G$  is an object of  $\underline{C}$ , [11, Lemma 3.5] implies that  $\psi$  is unramified at  $p$ . By Prop. 2.3 we have  $\psi = 0$ , in which case  $G$  is split, or  $\psi$  cuts out the field  $\mathbf{Q}(i)$ . Over  $\mathbf{Z}_2$  the group scheme  $\Phi$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \times \mu_2$ . It follows that the ramification index of the primes lying over 2 is at most 2. It follows that  $a : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(i, \sqrt{p})) \longrightarrow \mathbf{F}_2$  is everywhere unramified. This means that  $\mathbf{Q}(i, \sqrt{p})$  admits an unramified quadratic extension. This happens if and only if  $p \equiv 1 \pmod{8}$ . See for instance [6, section 8].

This proves the proposition when  $p \equiv -1 \pmod{8}$ . To complete the proof for  $p \equiv 1 \pmod{8}$ , we first note that the unramified field extension of  $\mathbf{Q}(i, \sqrt{p})$  is unique, so that there exists at most one non-split extension of  $\mathbf{Z}/2\mathbf{Z}$  by  $\Phi$  that is killed by 2. The fact

that such an extension actually exists follows from the description of 2-power order group schemes over  $\mathbf{Z}[\frac{1}{p}]$  given in [9, Prop.2.3].

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

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

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

**Proof.** Let  $G$  be an extension in  $\mathrm{Ext}_{\underline{C}}^1(\Phi, \Phi)$  and suppose it maps to the extension  $\Upsilon$  in  $\mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ . Then the ‘dual’ homomorphism  $\mathrm{Ext}_{\underline{C}}^1(\Phi, \Phi) \hookrightarrow \mathrm{Ext}_{\underline{C}}^1(\Phi, \mu_2)$  maps  $G$  to  $\Upsilon^\vee$  in  $\mathrm{Ext}_{\underline{C}}^1(\Phi, \mu_2)$ . It follows that  $G$  is an extension of  $\mathbf{Z}/4\mathbf{Z}$  by  $\mu_4$  on which the Galois group acts through matrices of the form

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

Here  $\omega_2 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \{\pm 1\}$  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  $G$ . Then the extension  $\mathbf{Q}(i) \subset K$  is cyclic of degree 4 and is unramified outside  $p$ . Moreover, the prime  $\pi = i + 1$  splits in  $K$ . By Kummer theory we have  $K = \mathbf{Q}(i, \sqrt[4]{\pm p})$ , 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  $\mathrm{Ext}_{\underline{C}}^1(\Phi, \Phi)$  vanishes.*

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

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

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

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

**Corollary 2.8.** *There do not exist any non-zero semistable abelian varieties 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  $\mu_2$ . We leave this to the reader. Now let  $A$  be a semistable abelian variety  $A$  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 successive subquotients isomorphic

to  $\mathbf{Z}/2\mathbf{Z}$  or  $\mu_2$ . The results of this section imply then that  $A[2^n]$  admits a filtration by closed flat subgroup schemes

$$0 \begin{array}{c} \hookrightarrow \\ \underbrace{\hspace{1.5cm}} \\ \mu_2\text{'s} \end{array} G_1 \begin{array}{c} \hookrightarrow \\ \underbrace{\hspace{1.5cm}} \\ \Phi\text{'s} \end{array} G_2 \begin{array}{c} \hookrightarrow \\ \underbrace{\hspace{1.5cm}} \\ \mathbf{Z}/2\mathbf{Z}\text{'s} \end{array} A[2^n]$$

with the property that  $G_1$  admits a filtration with successive subquotients isomorphic to  $\mu_2$ , the quotient  $A[2^n]/G_2$  admits a filtration with successive subquotients isomorphic to  $\mathbf{Z}/2\mathbf{Z}$  and the group scheme  $G_2/G_1$  admits a filtration with successive subquotients isomorphic to  $\Phi$ . By Theorem 2.7 the subquotient  $G_2/G_1$  is actually a product of group schemes isomorphic to  $\Phi$ . Just as in [10, section 7] or section 6 of the present paper one shows that the orders of the group schemes  $G_1$ ,  $G_2/G_1$ ,  $A[2^n]/G_2$  and hence of  $A[2^n]$  remain bounded as  $n \rightarrow \infty$ . This is impossible unless  $A = 0$ .

### 3. The group scheme $V$ and its Cartier dual.

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

#### Assumptions.

- $p \equiv -1 \pmod{8}$ ;
- $\mathbf{Q}(\sqrt{-p})$  admits a unique unramified cyclic degree 3 extension  $H$ ;
- in  $H$  the prime 2 splits into a product of two prime ideals  $\mathfrak{p}$  and  $\bar{\mathfrak{p}}$ ;
- the ray class groups of  $H$  of conductors  $\mathfrak{p}^2$ ,  $\bar{\mathfrak{p}}^2$  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  $\Delta = \text{Gal}(H/\mathbf{Q})$  is isomorphic to  $S_3 \cong \text{GL}_2(\mathbf{F}_2)$ . The class number of  $H$  is odd. The residue fields of  $\mathfrak{p}$  and  $\bar{\mathfrak{p}}$  are isomorphic to  $\mathbf{F}_8$ . Since the 2-parts of the ray class groups of conductor  $\mathfrak{p}^2$  and  $\bar{\mathfrak{p}}^2$  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  $(4) = \mathfrak{p}^2\bar{\mathfrak{p}}^2$  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 the above assumptions we construct two more simple objects in the category  $\underline{\mathcal{C}}$  that was defined in section 2.

**Definition.** Let  $V$  be the étale group scheme  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  over  $\mathbf{Z}[\frac{1}{p}]$ , twisted by the action of  $\Delta = \text{Gal}(H/\mathbf{Q})$ .

Note that  $\Delta$  is isomorphic to  $S_3 \cong \text{GL}_2(\mathbf{F}_2)$ . Since the inertia subgroups of  $\Delta$  of the primes over 2 in  $\text{Gal}(H/\mathbf{Q})$  have order 2, every  $\sigma$  in an inertia subgroup satisfies  $\sigma^2 = \text{id}$ . Therefore the group scheme  $V$  and its Cartier dual  $V^\vee$  are objects of the category  $\underline{\mathcal{C}}$ .

**Proposition 3.1.** *Over the ring  $\mathbf{Z}[\frac{1}{p}]$  we have*

$$\text{Hom}(V, V) = \text{Hom}(V, V^\vee) = \text{Hom}(V^\vee, V^\vee) = \mathbf{F}_2,$$

but  $\text{Hom}(V^\vee, V) = 0$ .

**Proof.** For any two objects  $G, H$  of  $\underline{\mathcal{C}}$  there is a natural isomorphism

$$\text{Hom}_{\mathbf{Z}[\frac{1}{p}]}(G, H) \cong \text{Hom}_{O_H[\frac{1}{p}]}(G, H)^\Delta.$$

Over the Galois extension  $O_H[\frac{1}{p}]$  of  $\mathbf{Z}[\frac{1}{p}]$  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 over the ring  $O_H[\frac{1}{p}]$  we have

$$\text{Hom}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) = \text{Hom}(\mathbf{Z}/2\mathbf{Z}, \mu_2) = \text{Hom}(\mu_2, \mu_2) = \mathbf{F}_2,$$

but  $\text{Hom}(\mu_2, \mathbf{Z}/2\mathbf{Z}) = 0$  and since  $\Delta$  is isomorphic to  $\text{GL}_2(\mathbf{F}_2)$ , the result now follows from Schur's Lemma.

**Proposition 3.2.** *Let  $O_H$  denote the ring of integers of the unique unramified cyclic cubic extension  $H$  of  $\mathbf{Q}(\sqrt{-p})$ . Then we have the following.*

- (a) *any successive extension of group schemes isomorphic to  $V$  becomes constant over the ring  $O_H[\frac{1}{p}]$ ;*
- (b) *any successive extension of group schemes isomorphic to  $V^\vee$  becomes diagonalizable over  $O_H[\frac{1}{p}]$ .*

**Proof.** (a) Let  $G$  be a group scheme over  $\mathbf{Z}[\frac{1}{p}]$  that is a successive extension of copies of  $V$ . Then  $G$  is étale. The Galois group  $\text{Gal}(\overline{\mathbf{Q}}/H)$  acts on the points of  $G$  through a 2-group  $\pi$ . The maximal abelian quotient  $\pi/\pi'$  is a quotient of the maximal abelian 2-extension of  $H$  that is unramified outside the primes lying over  $p$ . By the assumptions on  $p$ , this extension is trivial, so that  $\pi/\pi'$  and hence  $\pi$  are trivial. This implies that  $G$  is constant over  $O_H[\frac{1}{p}]$  as required.

Part (b) follows by Cartier duality.

The reduction homomorphism  $\text{GL}_2(\mathbf{Z}_2) \longrightarrow \text{GL}_2(\mathbf{F}_2)$  admits a section. Since the group  $\Delta$  is isomorphic to  $\text{GL}_2(\mathbf{F}_2)$ , we can in this way equip  $W = \mathbf{Z}_2 \times \mathbf{Z}_2$  with the structure of a  $\Delta$ -module. For any constant 2-power order group scheme  $G$  over  $\mathbf{Z}[\frac{1}{p}]$ , the  $\Delta$ -twist of the product  $G \times G$  by the action of  $\Delta = \text{Gal}(H/\mathbf{Q})$  is the étale  $\mathbf{Z}[\frac{1}{p}]$ -group scheme, whose associated Galois module is  $G(\overline{\mathbf{Q}}) \otimes_{\mathbf{Z}_2} W$ . In a similar way one defines  $\Delta$ -twists of diagonalizable 2-power order group schemes over  $\mathbf{Z}[\frac{1}{p}]$ . The  $\Delta$ -twists are objects of the category  $\underline{\mathcal{C}}$ .

**Proposition 3.3.** *Any finite group scheme over  $\mathbf{Z}[\frac{1}{p}]$  that is a successive extension of copies of  $V$ , is isomorphic to the  $\Delta$ -twist of a product of a constant group scheme by itself. Similarly, any group scheme over  $\mathbf{Z}[\frac{1}{p}]$  that is a successive extension of copies of  $V^\vee$ , is isomorphic to the  $\Delta$ -twist of a product of a diagonalizable group scheme by itself.*

**Proof.** The second statement follows by Cartier duality. To prove the first, we observe that for any successive extension  $G$  of copies of  $V$ , the Galois group  $\text{Gal}(\overline{\mathbf{Q}}/H)$  acts on  $G(\overline{\mathbf{Q}})$  through a 2-group. Since  $V$  is étale, the action is unramified outside the primes lying over  $p$ . Therefore, by our assumptions on the prime  $p$ , the group  $\text{Gal}(\overline{\mathbf{Q}}/H)$  acts

trivially on  $G(\overline{\mathbf{Q}})$ . It follows that  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  acts through its quotient  $\Delta = \text{Gal}(H/\mathbf{Q})$  which is isomorphic to  $\text{GL}_2(\mathbf{F}_2) \cong S_3$ . Let  $\tau \in \Delta$  be an automorphism of order 3. Since  $V(\overline{\mathbf{Q}})$  is killed by the  $\tau$ -norm, so is  $G(\overline{\mathbf{Q}})$ . 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  $\tau$ -norm. The natural map  $\mathbf{Z}_2[\text{GL}_2(\mathbf{F}_2)] \rightarrow \text{End}(\mathbf{Z}_2)$  induced by a section of  $\text{GL}_2(\mathbf{Z}_2) \rightarrow \text{GL}_2(\mathbf{F}_2)$  gives rise to an isomorphism of  $\mathbf{Z}_2[\Delta]/(\tau^2 + \tau + 1)$  with the ring of  $2 \times 2$  matrices over  $\mathbf{Z}_2$ . By Morita equivalence, the category of modules over this ring is equivalent to the category of  $\mathbf{Z}_2$ -modules. Indeed, the functor that sends a  $\mathbf{Z}_2$ -module  $M$  to  $M \otimes_{\mathbf{Z}_2} W$ , where  $W$  is a free  $\mathbf{Z}_2$ -module of rank 2 equipped with the canonical  $\text{GL}_2(\mathbf{Z}_2)$ -action, is an equivalence of categories.

This proves the proposition.

**Example 3.4.** *The group  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V, V)$  of extensions of  $V$  by itself over  $\mathbf{Z}[\frac{1}{p}]$  has order 2. It is generated by the  $\Delta$ -twist of the group scheme  $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ .*

**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  $\mu_2$  and  $V^\vee$  by one another are necessarily split.*
- (b) *We have*

$$\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mu_2, V) = \text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, \mathbf{Z}/2\mathbf{Z}) = 0.$$

- (c) *We have*

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

**Proof.** First we observe that all extensions  $G$  that appear in this proposition are annihilated by 2. Indeed, the Galois group  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  acts on  $G(\overline{\mathbf{Q}})$  through a group that is an extension of  $S_3$  by a 2-group. Let  $\tau$  be a generator of a 3-Sylow subgroup of this group. Then  $G(\overline{\mathbf{Q}})$  is a  $\mathbf{Z}_2[\tau]$ -module. It is therefore a direct sum of the  $\tau$ -invariants and of the elements killed by the  $\tau$ -norm. Since  $\tau$  acts trivially on the points of  $\mu_2$  and  $\mathbf{Z}/2\mathbf{Z}$ , while the module  $V(\overline{\mathbf{Q}}) \cong V^\vee(\overline{\mathbf{Q}})$  is killed by the  $\tau$ -norm, we see that  $G$  is killed by 2.

(a) By Cartier duality it suffices to study extensions  $G$  of  $\mathbf{Z}/2\mathbf{Z}$  and  $V$  by one another. Such group schemes  $G$  are étale. By the assumptions on the prime  $p$ , the class number of  $H$  is odd. This implies that the Galois group acts on  $G(\overline{\mathbf{Q}})$  through  $\text{Gal}(H/\mathbf{Q}) \cong S_3$ . As we explained above, the  $\tau$ -module  $G(\overline{\mathbf{Q}})$  is a direct product of the  $\tau$ -invariants and the kernel of the  $\tau$ -norm, each of which are preserved by the  $S_3$ -action. It follows that the  $S_3$ -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 determine the extensions

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

over the ring  $\mathbf{Z}[\frac{1}{p}]$ . Such extensions are split over  $\mathbf{Z}_2$ . By the assumptions on  $p$ , the ray class group of  $H$  of conductor  $\sqrt{-p}$  has odd order. It follows that  $\text{Gal}(\overline{\mathbf{Q}}/H)$  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  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, \mathbf{Z}/2\mathbf{Z})$  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  $S$  is Galois over  $R$  with Galois group  $\Delta \cong S_3$  and the extension groups  $\text{Ext}_S^q(V, \mu_2)$  are  $\mathbf{F}_2[\Delta]$ -modules. Consider the spectral sequence

$$H^p(\Delta, \text{Ext}_S^q(V, \mu_2)) \Rightarrow \text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^{p+q}(V, \mu_2).$$

Over the ring  $S$  the group scheme  $V$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  and there is a spectral sequence

$$\text{Ext}_{\text{ab}}^p(V(\overline{\mathbf{Q}}), \text{Ext}_S^q(\mathbf{Z}/2\mathbf{Z}, \mu_2)) \Rightarrow \text{Ext}_S^{p+q}(V, \mu_2),$$

Since the  $\mathbf{F}_2[\Delta]$ -module  $V(\overline{\mathbf{Q}})$  is projective, the second spectral sequence degenerates. Since the  $\Delta$ -module  $\text{Hom}_S(V, \mu_2)$  is isomorphic to  $V(\overline{\mathbf{Q}})$ , it has trivial cohomology. It follows that there are natural isomorphisms

$$\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V, \mu_2) \cong \text{Ext}_S^1(V, \mu_2)^\Delta \cong \text{Hom}_\Delta(V(\overline{\mathbf{Q}}), \text{Ext}_S^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)).$$

Since the class number of  $H$  is odd, Kummer theory leads to the following exact sequence of  $\mathbf{F}_2[\Delta]$ -modules:

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

Here an extension  $E$  of  $\mathbf{Z}/2\mathbf{Z}$  by  $\mu_2$  is mapped to a unit  $u \in S^*$  that generates the quadratic extension of  $S$  that is generated by the points of  $E$ . Since  $\text{Hom}_\Delta(V(\overline{\mathbf{Q}}), \{\pm 1\}) = 0$ , we have an isomorphism

$$\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V, \mu_2) \cong \text{Hom}_\Delta(V(\overline{\mathbf{Q}}), S^*/S^{*2}).$$

Since all extensions in  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V, \mu_2)$  are killed by 2, the points of those in the subgroup  $\text{Ext}_{\underline{C}}^1(V, \mu_2)$  generate an extension of  $H$  that is unramified at the primes over  $p$ . Therefore the following diagram is commutative

$$\begin{array}{ccc} \text{Ext}_{\underline{C}}^1(V, \mu_2) & \xrightarrow{\cong} & \text{Hom}_\Delta(V(\overline{\mathbf{Q}}), O_H^*/O_H^{*2}) \\ \downarrow \subset & & \downarrow \subset \\ \text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V, \mu_2) & \xrightarrow{\cong} & \text{Hom}_\Delta(V(\overline{\mathbf{Q}}), S^*/S^{*2}) \end{array}$$

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

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

This implies (c).

Proposition 3.5 implies that there is a unique non-split extension

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

Its points generate the extension  $H(\sqrt{u} : u \in O_H^*$  of norm 1). The Galois group  $\text{Gal}(L/\mathbf{Q})$  is isomorphic to the symmetric group  $S_4$ .

**Proposition 3.6.** *We have*

(a)

$$\mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\Phi, V) = \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, \Phi) = 0.$$

(b) *We have*

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

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

$$\mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mu_2, V) \longrightarrow \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\Phi, V) \longrightarrow \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\mathbf{Z}/2\mathbf{Z}, V)$$

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

(b) By Cartier duality it suffices to consider an extension of the form

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

Let  $\tau \in \Delta = \mathrm{Gal}(H/\mathbf{Q})$  be an automorphism of order 3. Since  $G(\mathbf{Q})$  is an  $\mathbf{Z}_2[\tau]$ -module, it is a product of the kernel of the  $\tau$ -norm and of  $\tau - 1$ . Since  $\Phi$  is killed by  $\tau - 1$  and  $V$  is killed by the  $\tau$ -norm, the group scheme  $G$  is killed by 2. Since  $G$  is an object of the category  $\underline{\mathcal{C}}$ , the extension  $L$  of  $H$  generated by the points of  $G$  is unramified outside the primes over 2.

Let  $\mathfrak{p}$  be one of the primes over  $O_H$  lying over 2. Over the completion  $O_{\mathfrak{p}}$  of  $O_H$ , the group scheme  $G$  is an extension of  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  by  $\mathbf{Z}/2\mathbf{Z} \times \mu_2$ . This implies that the inertia subgroups of  $\mathrm{Gal}(L/\mathbf{Q})$  of the primes over 2 have order at most 2. Moreover, by Kummer theory, the local Galois extension is a compositum of quadratic extensions of  $O_{\mathfrak{p}}$  generated by the square roots of certain units of  $O_{\mathfrak{p}}$ . It follows that the conductor of the local extension divides  $\mathfrak{p}^2$ . It follows that the conductor of  $L$  over  $H$  divides  $\mathfrak{p}^2 \bar{\mathfrak{p}}^2 = (4)$ . By the assumptions made on the prime  $p$  at the beginning of this section, the extension  $L$  is totally ramified at both primes over 2. It follows that  $[L : H] \leq 2$ .

The ‘Kummer map’

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

given by  $\sigma \mapsto f_\sigma$  where  $f_\sigma(P) = \sigma(P) - P$  for every  $P \in V(\bar{\mathbf{Q}})$ , is injective and  $\Delta$ -equivariant. Since  $\mathrm{Gal}(L/H)$  is  $\Delta$ -invariant, while there are no non-zero  $\Delta$ -equivariant maps  $V(\bar{\mathbf{Q}}) \rightarrow \Phi(\bar{\mathbf{Q}})$ , the Kummer map must be zero. It follows that  $L = H$ .

Therefore the second arrow in the exact sequence

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

maps the class of the extension  $G$  to an extension of  $V$  by  $\mu_2$  that is split as a Galois module. Since extensions of  $V$  by  $\mu_2$  over  $\mathbf{Z}[\frac{1}{p}]$  are determined by their Galois modules, the second arrow is zero. Since  $\mathrm{Ext}_{\underline{\mathcal{C}}}^1(V, \mathbf{Z}/2\mathbf{Z}) = 0$  by Prop. 3.5 (a), it follows that  $\mathrm{Ext}_{\underline{\mathcal{C}}}^1(V, \Phi)$  vanishes, as required.

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

**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  $\underline{\mathcal{C}}$  and suppose that it admits a filtration with closed flat subgroup schemes with successive subquotients isomorphic to one of the simple group schemes  $\mathbf{Z}/2\mathbf{Z}$ ,  $\mu_2$ ,  $V$  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  $\mathbf{Z}[\frac{1+\sqrt{-p}}{2}, \frac{1}{p}]$ . In addition, we have

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

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

**Proof.** Let  $G$  be an object of the category  $\underline{\mathcal{C}}$  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  $\Phi$ ,  $V$  or  $V^\vee$  splits. This fact and its dual version imply that  $G$  admits a filtration by closed flat subgroup schemes of the form

$$0 \hookrightarrow G_1 \hookrightarrow G_2 \hookrightarrow G.$$

Here  $G/G_2$  is an extension of copies of  $\mathbf{Z}/2\mathbf{Z}$ , the group scheme  $G_1$  is an extension of copies of  $\mu_2$  and  $G_2/G_1$  admits a filtration by closed flat subgroup schemes with successive subquotients isomorphic to  $\Phi$ ,  $V$  or  $V^\vee$ . By Prop. 2.2 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  $\Phi$  and  $E$  admits a filtration with closed flat subgroup schemes and successive subquotients isomorphic to  $V$  or  $V^\vee$ . This proves the corollary.

#### 4. The group scheme $\Psi$ .

In this section we make the *same assumptions* on the prime  $p$  as in section 3. We construct a non-split extension  $\Psi$  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  $\Psi$  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  $\Psi$  is isomorphic to the subscheme of 2-torsion points of the Jacobian of the modular curve  $X_0(23)$ .

**Proposition 4.1.** *We have*

$$\mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V) = \mathbf{F}_2.$$

*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 any prime  $l$  of  $\mathbf{Z}[\frac{1}{p}]$ .*

**Proof.** By the conditions on the prime  $p$ , there is a unique unramified cyclic cubic extension  $H$  of  $\mathbf{Q}(\sqrt{-p})$ . 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 that is unramified outside  $p$ . So, by the assumptions on the prime  $p$  we have  $L = H$ . This implies that  $G(\mathbf{Q})$  is an  $\mathbf{F}_2[S_3]$ -module killed by the  $\tau$ -norm, where  $\tau \in S_3$  has order 3. It follows that the Galois module  $G(\mathbf{Q})$  is split. So  $G$  is split over  $\mathbf{Q}$  and over  $\mathbf{Z}_l$  for every  $l$  of  $\mathbf{Z}[\frac{1}{p}]$ .

The Mayer-Vietoris exact sequence [9, Cor. 2.4] associated to the exact sequence gives the exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{Hom}_{\mathbf{Z}[\frac{1}{p}]}(V^\vee, V) \longrightarrow \mathrm{Hom}_{\mathbf{Z}_2}(V^\vee, V) \times \mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, V) \longrightarrow \\ \longrightarrow \mathrm{Hom}_{\mathbf{Q}_2}(V^\vee, V) \longrightarrow \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V) \longrightarrow 0. \end{aligned}$$

The group  $\mathrm{Hom}_{\mathbf{Z}_2}(V^\vee, V)$  and hence  $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{p}]}(V^\vee, V)$  vanish. The group  $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, V)$  has order 2. Since 2 *splits* in  $\mathbf{Q}(\sqrt{-p})$  but not in  $H$ , the local Galois group is the order 3 subgroup of  $S_3$ . It follows that  $\mathrm{Hom}_{\mathbf{Q}_2}(V^\vee, V)$  has order 4. Therefore  $\mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V) \cong \mathbf{F}_2$  as required.

**Definition.** Let  $\Psi$  denote the unique non-split extension of  $V^\vee$  by  $V$ . This group scheme is an object of  $\underline{C}$ . It is self-dual and has order 16. Its points generate the field  $H$ .

**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

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

Since  $V^\vee$  is connected and  $V$  is étale, we have  $\mathrm{Hom}(V^\vee, V) = 0$ . Therefore we obtain the exact sequence

$$0 \longrightarrow \mathrm{Hom}(V^\vee, \Psi) \xrightarrow{\phi} \mathrm{Hom}(V^\vee, V^\vee) \longrightarrow \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V).$$

Since the Galois action on  $V^\vee(\overline{\mathbf{Q}})$  is irreducible, the latter maps to the extension class of  $\Psi$  in  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V)$ . It follows that the homomorphism  $\phi$  is zero. This implies that  $\text{Hom}(V^\vee, \Psi)$  is zero as required. The fact that  $\text{Hom}(\Psi, V)$  vanishes follows by Cartier duality.

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

$$0 \rightarrow \text{Hom}(V^\vee, V^\vee) \rightarrow \text{Hom}(\Psi, V^\vee) \rightarrow \text{Hom}(V, V^\vee) \xrightarrow{\phi} \text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V^\vee).$$

Since the group scheme  $\Psi$  is killed by 2, so is the image under  $\phi$  of the non-trivial homomorphism  $V \rightarrow V^\vee$ . By Prop. 3.3 the only non-trivial extension of  $V^\vee$  by itself is dual to the group scheme of Example 3.4 and is *not* killed by 2. Therefore the map  $\phi$  must be zero. By Prop. 3.1 both groups  $\text{Hom}(V^\vee, V^\vee)$  and  $\text{Hom}(V, V^\vee)$  have order 2. This implies that the order of  $\text{Hom}(\Psi, V^\vee)$  and hence of  $\text{Hom}(V, \Psi)$  has to be 4, as required.

**Proposition 4.3.** *We have*

$$\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\Psi, V) = \text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, \Psi) = 0.$$

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

$$0 \rightarrow V \rightarrow G \rightarrow \Psi \rightarrow 0$$

is split. Let  $C$  denote the kernel of the composite morphism  $G \rightarrow \Psi \rightarrow V^\vee$ . Then we have the exact sequence

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

where  $C$  is an extension of  $V$  by  $V$ . Then  $C$  is either a split extension or it is the  $\Delta$ -twist of  $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$  of Example 3.4. We compute  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, C)$ .

**Claim.** The following natural sequence is exact:

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

This follows from the Mayer-Vietoris exact sequence [9, Cor. 2.4] associated to the second exact sequence above. Indeed, since  $C$  is étale, there are no non-zero homomorphisms  $V^\vee \rightarrow C$  over  $\mathbf{Z}_2$ . Therefore there are none over  $\mathbf{Z}[\frac{1}{p}]$ . The extension  $G$  of  $V^\vee$  by  $C$  is split over  $\mathbf{Z}_2$ . It follows that  $G$  is killed by 4 and that the action of  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  on  $G(\overline{\mathbf{Q}})$  is unramified outside  $p$ . By the assumptions on the prime  $p$ , the field  $H$  admits no quadratic extensions that are unramified outside the primes lying over  $p$ . By the assumptions on the prime  $p$  made at the beginning of section , the action of  $\text{Gal}(\overline{\mathbf{Q}}/H)$  on  $G(\overline{\mathbf{Q}})$  is therefore trivial. It follows that  $G(\overline{\mathbf{Q}})$  is a module over the ring  $\mathbf{Z}_2[\Delta]/(\tau^2 + \tau + 1)$  that is killed by 4. As in the proof of Prop. 3.3 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 the group  $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, C)$  is isomorphic to  $\mathrm{Hom}_{\mathbf{Z}[\frac{1}{2p}]}(V^\vee, V) = \mathbf{F}_2$ . In addition 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 that the group  $\mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, C)$  has order 2.

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

$$0 \rightarrow \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V) \rightarrow \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, C) \xrightarrow{\psi} \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V)$$

Since all three groups have order 2, the map  $\psi$  is zero. But this is impossible, since it maps the class of  $G$  to the class of  $\Psi$ , which is certainly not trivial. This leads to a contradiction and we conclude that  $C$  is a split extension of  $V$  by  $V$ .

Finally we apply the functor  $\mathrm{Hom}(-, V)$  to the exact sequence

$$0 \rightarrow V \rightarrow \Psi \rightarrow V^\vee \rightarrow 0$$

and we obtain the exact sequence

$$0 \rightarrow \mathrm{Hom}(V, V) \xrightarrow{\phi} \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V^\vee, V) \rightarrow \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\Psi, V) \rightarrow \mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V, V).$$

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

This proves the proposition.

**Theorem 4.4.** *Let  $p$  be a prime satisfying the hypotheses formulated at the beginning of section 3. 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*

$$0 \hookrightarrow H_1 \hookrightarrow H_2 \hookrightarrow G.$$

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

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

$$0 \hookrightarrow H_1 \hookrightarrow H_2 \hookrightarrow G.$$

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  $\Psi$ . 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 corollary.

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

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

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

and consider the exact sequence of  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1$ -groups. By Prop. 4.2 the group  $\text{Hom}(\Psi, V)$  is zero and the  $\mathbf{F}_2$ -dimension of  $\text{Hom}(\Psi, V^\vee)$  is 2. By Prop. 4.3 the group  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(\Psi, V)$  is zero. It follows that  $\text{End}(\Psi)$  has order 4.

It remains to show that  $\text{End}(\Psi)$  is a field. The Galois module  $\Psi(\overline{\mathbf{Q}}) \cong V(\overline{\mathbf{Q}})^2$  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  $\Psi$ . Since by Proposition 4.2 we have  $\text{Hom}(V^\vee, \Psi) = 0$ , it follows that each subgroup scheme  $G$  is isomorphic to  $V$  and hence that  $\Psi/G$  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 submodules above 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.

**Lemma 4.6.** *Let  $p$  be a prime as in Corollary 4.4. Then any extension in the category  $\underline{\mathcal{C}}$*

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

*that is killed by 2, is split.*

**Proof.** We apply the functor  $\text{Hom}_{\underline{\mathcal{C}}}(V, -)$  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

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

Since the unique non-split extension of  $V$  by  $V$  is *not* killed by 2, the restriction of  $\phi$  to the subgroup  $\text{Ext}_{\underline{\mathcal{C}}, [2]}^1(V, \Psi)$  of extensions of  $V$  by  $\Psi$  that are killed by 2, is injective. Let  $W$  in  $\text{Ext}_{\underline{\mathcal{C}}}^1(V, V^\vee)$  be the image under  $\phi$  of the class  $G$ . Then  $W$  is killed by 2. 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.

First we observe that  $W$  is determined by its Galois module. Indeed, the spectral sequence

$$H^p(\Delta, \text{Ext}_{O_H[\frac{1}{p}]}^q(V, V^\vee)) \implies \text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^{p+q}(V, V^\vee)$$

and the fact that  $\text{Hom}(V, V^\vee) \cong \text{End}(V)$  is a cohomologically trivial  $\Delta$ -module show that the natural map  $\text{Ext}_{\mathbf{Z}[\frac{1}{p}]}^1(V, V^\vee) \hookrightarrow \text{Ext}_{O_H[\frac{1}{p}]}^1(V, V^\vee)$  is injective. Over the ring  $O_H[\frac{1}{p}]$  the group schemes  $V$  and  $V^\vee$  are isomorphic to  $\mathbf{Z}/2\mathbf{Z}$  and  $\mu_2 \times \mu_2$  respectively. Since extensions of  $\mathbf{Z}/2\mathbf{Z}$  by  $\mu_2$  are determined by their Galois modules, we see that the same is true for  $W$ .

The group scheme  $W$  is the cokernel of the composite morphism  $V \longrightarrow \Psi \longrightarrow G$ . We evaluate the Mayer-Vietoris exact sequence [9, Cor. 2.4] associated to the exact sequence

$$0 \longrightarrow V \longrightarrow G \longrightarrow W \longrightarrow 0.$$

First we compute the homomorphisms  $W \longrightarrow V$  over the base rings  $\mathbf{Z}[\frac{1}{p}]$ ,  $\mathbf{Z}[\frac{1}{2p}]$ ,  $\mathbf{Z}_2$  and  $\mathbf{Q}_2$ .

The Galois group acts on the points of  $G$  and by Kummer theory it acts through  $\pi = \text{Gal}(L/\mathbf{Q})$  where  $L = H(\sqrt{u} : u \in O_H^*)$ . Our assumptions on  $p$  imply that  $[L : H] = 8$  and that both primes of  $H$  lying over 2 are *totally ramified* in  $L$ . Since the non-split extension  $W$  is determined by its Galois module, we have  $H \neq L$  and therefore the homomorphisms factor in each case over the quotient  $V$  of  $W$ . It follows that  $\text{Hom}(W, V) = \text{Hom}(V, V)$  which is  $\mathbf{F}_2$  over the base rings  $\mathbf{Z}[\frac{1}{p}]$  and  $\mathbf{Z}[\frac{1}{2p}]$  and is  $\mathbf{F}_4$  over  $\mathbf{Z}_2$  and  $\mathbf{Q}_2$ .

Since the leftmost and rightmost terms of the exact sequence

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

are zero, we have that  $\text{Ext}_{\mathbf{Z}_2, [2]}^1(W, V) = 0$ . The Mayer-Vietoris exact sequence now becomes

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

For each prime lying over 2 the local Galois group is equal to  $N = \text{Gal}(L/\mathbf{Q}(\sqrt{-p}))$ . In particular, it is normal in  $\pi$ . Since the following diagram commutes

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

the Hochschild-Serre spectral sequence provides us with an isomorphism

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

Since  $W$  is not split, the  $N$ -invariants of  $W(\overline{\mathbf{Q}})$  constitute the submodule  $V^\vee(\overline{\mathbf{Q}})$  and any  $N$ -homomorphism  $W(\overline{\mathbf{Q}}) \longrightarrow V(\overline{\mathbf{Q}})$  factors over the quotient  $V(\overline{\mathbf{Q}})$ . Since we have  $\text{Hom}_N(V(\overline{\mathbf{Q}}), V(\overline{\mathbf{Q}})) \cong \mathbf{F}_4$ , we find

$$\text{Ext}_{\mathbf{Z}[\frac{1}{p}], [2]}^1(W, V) \cong H^1(\pi/N, \mathbf{F}_4).$$

Here  $\mathbf{F}_4$  indicates the algebra generated by  $\tau = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ . The group  $\pi/N$  acts through conjugation by the matrix  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . An easy computation shows that  $H^1(\pi/N, \mathbf{F}_4) = 0$  and hence

$$\mathrm{Ext}_{\mathbf{Z}[\frac{1}{p}], [2]}^1(W, V) = 0.$$

However, the homomorphism

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

maps the class of  $G$  to the class of  $\Psi$  and is hence *surjective* onto the order 2-group  $\mathrm{Ext}_{[2]}^1(V^\vee, V)$ . This contradiction implies that  $W$  is split. Contradiction. This proves the lemma.

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

**Proof.** Recall that by Proposition 4.5, the ring  $\mathrm{End}(\Psi)$  is isomorphic to  $\mathbf{F}_4$ . By Lemma 4.6 the group  $\mathrm{Ext}_{\underline{C}, [2]}^1(V, \Psi)$  is trivial. It follows therefore from [11, Lemma 2.1] that the natural map

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

is injective. Since the Galois module  $\Psi(\overline{\mathbf{Q}})$  is isomorphic to  $V(\overline{\mathbf{Q}})^2$ , the group on the right is dual to the  $\Delta$ -covariants of  $\mathrm{End}(V(\overline{\mathbf{Q}}))^2$ . Since the  $\Delta$ -covariants of  $\mathrm{End}(V(\overline{\mathbf{Q}}))$  are isomorphic to  $\mathbf{F}_2$ , we conclude that  $\#\mathrm{Ext}_{\underline{C}}^1(V, \Psi) \leq 4$  and that  $\mathrm{Ext}_{\underline{C}}^1(V, \Psi)$  is an  $\mathbf{F}_4$ -vector space of dimension  $\leq 1$ . Since the image of the natural map  $\mathrm{Ext}_{\underline{C}}^1(V, V) \longrightarrow \mathrm{Ext}_{\underline{C}}^1(V, \Psi)$  is not zero, the dimension is actually equal to 1. The statement concerning  $\mathrm{Ext}_{\underline{C}}^1(\Psi, V^\vee)$  follows by Cartier duality. This proves the corollary.

**Theorem 4.8.** *Under the above assumption on the prime  $p$ , the group  $\mathrm{Ext}_{\underline{C}}^1(\Psi, \Psi)$  is a vector space over the field  $\mathrm{End}(\Psi) \cong \mathbf{F}_4$  of dimension  $\leq 1$ .*

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

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

is injective. The result now follows from Corollary 4.7.

## 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  $\underline{C}$  are the group schemes  $\mathbf{Z}/2\mathbf{Z}$ ,  $\mu_2$ ,  $V$  and  $V^\vee$ . 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

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

**Lemma 5.1.** *Let  $p = 23$  and let  $G$  be a simple object of the category of 2-group schemes  $\underline{C}$  over  $\mathbf{Z}[\frac{1}{23}]$ . Then  $\text{Gal}(\mathbf{Q}/\mathbf{Q})$  acts on the group of points  $G(\mathbf{Q})$  through  $\Delta = \text{Gal}(H/\mathbf{Q})$ , where  $H$  denotes the Hilbert class field of  $\mathbf{Q}(\sqrt{-23})$ .*

**Proof.** Let  $G$  be a simple 2-power order group scheme in  $\underline{C}$ . We multiply  $G$  by  $V$  and by the Kummer extension of  $\mathbf{Z}/2\mathbf{Z}$  by  $\mu_2$  whose points generate the field  $\mathbf{Q}(i)$ . The result is an object of  $\underline{C}$  that is killed by 2. Let  $L$  be the field obtained by adjoining the points of  $G$  to  $\mathbf{Q}$ . Then  $L$  is a Galois extension containing  $H(i)$ . Put  $\pi = \text{Gal}(L/\mathbf{Q})$ . By the theorems of Fontaine [3] or Abrashkin [1], the root discriminant of  $L$  is strictly smaller than  $4\sqrt{23} = 19.18\dots$ . Odlyzko's discriminant bounds [8] imply the inequality  $[L : \mathbf{Q}] < 300$  and hence  $[L : H(i)] \leq 24$ . It follows that the group  $\pi = \text{Gal}(L/\mathbf{Q})$  is solvable.

Since the root discriminant of  $\mathbf{Q}(\zeta_8, \sqrt{-23})$  is equal to  $4\sqrt{23}$ , the field  $F = \mathbf{Q}(i, \sqrt{-23})$  is the maximal abelian extension of  $\mathbf{Q}$  inside  $L$ . Therefore  $\text{Gal}(L/F)$  is equal to the commutator subgroup  $\pi'$  of  $\pi$ .

**Claim.** The maximal abelian extension of  $F$  inside  $L$  is  $H(i)$ .

**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  $G$  is an object of  $\underline{C}$  that is killed by 2, the extension  $F \subset L$  is unramified outside 2. The root discriminant of  $H(i)$  is equal to  $2\sqrt{23} = 9.59\dots$ . By Odlyzko's bounds any unramified extension of  $H(i)$  has degree at most 20 over  $\mathbf{Q}$ . Since we have  $[H(i) : \mathbf{Q}] = 12$ , the field  $H(i)$  admits therefore no non-trivial unramified extensions at all. This implies that the maximal unramified abelian extension of  $F$  is  $H(i)$ . 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  $\langle i, \eta \rangle$ . Here  $\eta$  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  $\eta$  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  $\eta$  generate the group  $(O_F/(1 + i)^3 O_F)^*$ . Any quadratic extension of  $F$  of conductor divisible by  $(1 + i)^4 = (4)$  has root discriminant at least equal to  $4\sqrt{23}$ . It follows that such an extension 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  $\text{Gal}(L/H(i))$  is equal to  $\pi''$ . This proves the claim.

We proceed by determining the maximal abelian extension of  $H(i)$  inside  $L$ . The two primes in  $H(i)$  lying over 2 have residue fields isomorphic to  $\mathbf{F}_8$ . The image of the global units inside  $\mathbf{F}_8^* \times \mathbf{F}_8^*$  is a  $\text{Gal}(H(i)/\mathbf{Q})$ -submodule. Since the action of the Galois group on

$\mathbf{F}_8^* \times \mathbf{F}_8^*$  is irreducible and since the zeroes of  $T^3 - T + 1$  are units contained in  $H$  generate a non-trivial submodule, we conclude that the image of the units of  $O_{H(i)}$  generate  $\mathbf{F}_8^* \times \mathbf{F}_8^*$ . Since we already saw that  $H(i)$  admits no non-trivial unramified extension inside  $L$ , we see that  $\pi'' = \text{Gal}(L/H(i))$  has the property that  $\pi''/\pi'''$  is a 2-group of order  $\leq 16$ .

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

**Theorem 5.2.** *The only simple group schemes in the category  $\underline{C}$  are  $\mu_2$ ,  $\mathbf{Z}/2\mathbf{Z}$ ,  $V$  and its Cartier dual  $V^\vee$ .*

**Proof.** Let  $G$  be a simple object and recall that  $\Delta = \text{Gal}(H/\mathbf{Q})$  is isomorphic to  $S_3$ . By Lemma 2.1, the group  $G(\overline{\mathbf{Q}})$  is a simple  $\mathbf{F}_2[\Delta]$ -module. This implies that 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 is also irreducible. This follows from the fact that the primes over 2 are inert in the extension  $\mathbf{Q}(\sqrt{-23}) \subset H$ . Therefore  $G$  is either étale or local. In the first case, Galois theory implies that  $G \cong V$ . In the second case we twist the Galois action with the unramified 2-dimensional representation  $\rho : \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{Gal}(H/\mathbf{Q}) \cong \text{GL}_2(\mathbf{F}_2)$  in such a way that  $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$  acts trivially on the points of the twisted group scheme  $G(\rho)$ . Then we take the Zariski closure of one of the subgroups of order 2. An application of the Oort-Tate theorem to the ring  $\mathbf{Z}[\frac{1}{23}]$  shows that these order 2 subgroup schemes are isomorphic to  $\mu_2$ . 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  $\rho$ . So  $G$  is isomorphic to  $V$ .

This proves the corollary.

The next proposition shows that the prime  $p = 23$  satisfies the conditions of section 3.

**Lemma 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) *for each prime  $\mathfrak{p}$  over 2 in  $H$  the ray class field of conductor  $\mathfrak{p}^2$  is equal to  $H$*

**Proof.** Consider the cubic polynomial  $f(X) = X^3 + aX^2 - (a+3)X + 1$ . Its discriminant  $(a^2 + 3a + 9)^2$  is equal to 1 for  $a = (-3 + \sqrt{-23})/2$ . For this choice of  $a$  the zeroes of  $f$  are units that generate the Hilbert class field  $H$  of  $\mathbf{Q}(\sqrt{-23})$ . A standard computation employing Odlyzko's bounds shows that the only unramified extension of  $H$  is  $H$  itself. We leave this to the reader.

(a) The prime  $\sqrt{-23}$  of  $\mathbf{Q}(\sqrt{-23})$  splits in  $H$ . Therefore there are three primes lying over 23 in  $H$ . The zeroes of the polynomial  $f$  are units in  $O_H$ . We have

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

The zeroes 2, 12, 22 are a square, a square and a non-square respectively in  $\mathbf{F}_{23}$ . This means that the image in the 3-dimensional  $\mathbf{F}_2$ -vector space  $(O_H/(\sqrt{-23}))^*/(O_H/(\sqrt{-23}))^{*2}$  of the zeroes of  $f$  are the vector  $(0, 0, 1)$  and its cyclic permutations. It follows that the ray class group of conductor  $\sqrt{-23}$  is trivial.

(b) There are two primes over 2 in  $H$ . Both have residue field  $\mathbf{F}_8$ . Let  $\mathfrak{p}$  be the prime that divides  $a$ . Since  $(a) = \mathfrak{p}^3$ , we have

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

It follows that the image of the zeroes of  $f$  in the order 7 group  $(O_H/\mathfrak{p})^*$  is non-trivial. This means that the ray class group of conductor (2) is trivial. In order to compute the ray class group of conductor  $\mathfrak{p}^2$ , we use the fact the map  $y \mapsto 1 + 2y$  is an isomorphism of groups between the additive group  $O_H/\mathfrak{p}$  and the multiplicative group  $\{x \in O_H/\mathfrak{p}^2 : x \equiv 1 \pmod{\mathfrak{p}}\}$ . We have  $-1 \equiv 1 + 2 \cdot 1 \pmod{\mathfrak{p}^2}$  and for a zero  $u$  of  $f$  we have  $u^7 \equiv 1 + 2u^2 \pmod{\mathfrak{p}^2}$ . Since the additive subgroup of  $O_H/\mathfrak{p}$  is generated by 1 and by  $u, u^2$  and  $u^4$ , the ray class group of conductor  $\mathfrak{p}^2$  is trivial as required.

## 6. The modular curve.

In this section we take  $p = 23$  and we study the Jacobian  $J = J_0(23)$  of the modular curve  $X_0(23)$ . The following equation was obtained by J. González 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  $\mathcal{C}$ .

**Proposition 6.1.** *The group scheme  $J[2]$  is isomorphic to  $\Psi$ .*

**Proof.** Since  $J[2]$  is an object of  $\mathcal{C}$ , Theorem 5.2 implies that it admits a filtration with successive quotients isomorphic to  $\mathbf{Z}/2\mathbf{Z}$ ,  $\mu_2$ ,  $V$  or  $V^\vee$ . 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 is the Hilbert class field  $H$  of  $\mathbf{Q}(\sqrt{-23})$ .

Therefore one of the group schemes  $V$  and  $V^\vee$  must be a simple 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 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  $\text{End}(J[2])$ .

It follows that the ring  $\text{End}(G)$  is an  $\mathbf{F}_4$ -algebra. By Proposition 3.1 an application of the bifunctor  $\text{Hom}(-, -)$  to the exact sequence  $0 \rightarrow V^\vee \rightarrow G \rightarrow V \rightarrow 0$  shows that  $\#\text{End}(G) \leq 8$ . Then we must have that  $\#\text{End}(G) = 4$  and hence  $\text{End}(G) \cong \mathbf{F}_4$ .

However,  $\text{End}(G)$  cannot be a field. Indeed, the composition of the morphism  $G \rightarrow V$  with the unique non-zero morphism  $V \rightarrow V^\vee$  and the natural embedding  $V^\vee \hookrightarrow G$  is a non-zero endomorphism  $f : G \rightarrow G$  whose square is zero.

This proves the proposition.

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

**Proof.** By Proposition 4.8 the  $\mathbf{F}_4$ -dimension of  $\text{Ext}_{\underline{C}}^1(\Psi, \Psi)$  is at most 1. The group scheme  $J[4]$  is an object of the category  $\underline{C}$  that is a non-trivial extension of  $\Psi$  by  $\Psi$ . 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  $\underline{C}$ . It admits a filtration with simple subquotients, which by Theorem 5.2 are isomorphic to one of the simple group schemes  $\mathbf{Z}/2\mathbf{Z}$ ,  $\mu_2$ ,  $V$  and  $V^\vee$ .

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

$$0 \hookrightarrow G_1 \hookrightarrow G_2 \hookrightarrow A[2^n],$$

where  $G_1$  becomes diagonalizable and the group scheme  $A[2^n]/G_2$  become constant over the ring  $\mathbf{Z}[\frac{1+\sqrt{-23}}{2}, \frac{1}{23}]$ . Let  $\mathfrak{p}$  be a prime ideal of  $\mathbf{Z}[\frac{1+\sqrt{-23}}{2}, \frac{1}{23}]$  not over 2 and let  $\mathbf{F}_{\mathfrak{p}}$  denote its residue field. Let  $A'$  denote the abelian variety  $A/G_2$ . Since reduction modulo  $\mathfrak{p}$  maps the group of points of  $A[2^n]/G_2$  *injectively* into the finite group  $A'(k_{\mathfrak{p}})$ , we see that  $\#(A[2^n]/G_2) \leq \#A'(k_{\mathfrak{p}}) = \#A(k_{\mathfrak{p}})$ . This shows that  $\#(A[2^n]/G_2)$  is bounded as  $n$  grows. Similarly, using Cartier duality, one shows that  $\#G_1$  remains bounded as  $n$  grows.

By Theorem 3.7 the subquotient  $G_2/G_1$  of the filtration is a product  $E \times E'$ , where  $E'$  is an extension of group schemes isomorphic to  $\Phi$  and  $E$  admits a filtration with closed flat subgroup schemes with successive subquotients isomorphic to  $V$  or  $V^\vee$ . Since  $23 \equiv 7 \pmod{16}$ , Theorem 2.7 implies that  $E'$  is actually product of group schemes isomorphic to  $\Phi$ . Therefore  $E'$  is killed by 2 and hence  $\#E'$  is bounded as  $n$  grows. Theorem 4.4 implies that for each  $n \geq 1$ , the group scheme  $E$  admits a filtration of the form

$$0 \hookrightarrow H_1 \hookrightarrow H_2 \hookrightarrow E,$$

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

The same arguments as we used above, show then that  $\#(E/H_2)$  and  $\#H_1$  remain bounded as  $n \rightarrow \infty$  as  $n$  grows. By Corollary 6.2 the  $\text{End}(\Psi) \cong \mathbf{F}_4$ -vector space  $\text{Ext}_{\underline{C}}^1(\Psi, \Psi)$  has dimension 1 and 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  $H_2/H_1$  is isomorphic to a group scheme of the form

$$\bigoplus_{j=1}^t J[2^{m_j}],$$

for certain integers  $m_j > 0$  that depend on  $n$ .

Now we let  $n$  grow. The underlying group of  $A[2^n]$  is a product of  $2g'$  cyclic groups of order  $2^n$ . Here  $g' = \dim A$ . The fact that the orders of the group schemes  $G_1$ ,  $A[2^n]/G_2$ ,  $E'$ ,  $H_1$  and  $E/H_2$  remain bounded as  $n$  grows, implies that there are morphisms of group schemes

$$f_n : A[2^n] \longrightarrow J[2^n]^g, \quad n \geq 1,$$

where  $g$  satisfies  $2g = g'$ , with the property that  $\ker f_n$  and  $\operatorname{coker} f_n$  remain bounded as  $n$  grows. 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

$$0 \longrightarrow H \longrightarrow A_{\operatorname{div}} \longrightarrow J_{\operatorname{div}}^g \longrightarrow 0,$$

where  $H$  is a finite closed flat subgroup scheme of  $A$ . By Faltings' theorem [2] the abelian varieties  $A$  and  $J^g$  are therefore isogenous over  $\mathbf{Q}$ .

This proves Theorem 1.1.

## Bibliography

- [1] Abraškin, V.A.: Galois moduli of period  $p$  group schemes over a ring of Witt vectors, *Izv. Ak. Nauk CCCP*, Ser. Matem., **51** (1987). English translation in *Math. USSR Izvestiya*, **31** (1988) 1–46.
- [2] 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  $\mathbf{Z}$ , *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, 1976. <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  $\mathbf{Q}$  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*, to appear.
- [12] Tate, J.T. and Oort, F.: Group schemes of prime order, *Ann. Scient. École Norm. Sup.* **3** (1970) 1–21.