Abelian varieties over real quadratic fields with good reduction everywhere

René Schoof

Dipartimento di Matematica
2^{a} Università di Roma "Tor Vergata"
I-00133 Roma ITALY
Email: schoof@mat.uniroma2.it

Abstract. We show that there do not exist any non-zero abelian varieties with good reduction everywhere over the real quadratic fields $\mathbf{Q}(\sqrt{\Delta})$ of discriminant Δ at most 21. On the other hand, for every discriminant $\Delta > 21$ there does exist a non-zero abelian variety over $\mathbf{Q}(\sqrt{\Delta})$ with good reduction everywhere.

1. Introduction.

In 1985 V.A. Abrashkin and J.-M. Fontaine each proved that there do not exist any non-zero abelian varieties over $\mathbf{Q}$ with good reduction modulo every prime [1, 3]. In their papers both authors extended this result to a few other number fields of small degree and discriminant. In this paper we consider abelian varieties over real quadratic fields with good reduction everywhere. Our main result is the following.

Theorem 1.1. *There do not exist any non-zero abelian varieties with good reduction everywhere over the real quadratic field* $\mathbf{Q}(\sqrt{\Delta})$ *if and only if the discriminant* Δ *is at most* 21.

One direction of the proof of Theorem 1.1 is easy. Abelian varieties over $\mathbf{Q}(\sqrt{\Delta})$ with good reduction everywhere can be constructed as follows. Let $Y(\Delta) \longrightarrow X_0(\Delta)$ denote the quadratic subcover of the cover of modular curves $X_1(\Delta) \longrightarrow X_0(\Delta)$ cut out by the unique quadratic Dirichlet character of conductor Δ. The curves $X_0(\Delta)$ and $Y(\Delta)$ and their Jacobians $J_0(\Delta)$ and $J(\Delta)$ are defined over $\mathbf{Q}$ and so is the abelian variety $A(\Delta) = J(\Delta)/J_0(\Delta)$. It follows from a result attributed to Langlands in [5, Prop. 2 on page 263], that $A(\Delta)$ acquires good reduction everywhere over the quadratic field $\mathbf{Q}(\sqrt{\Delta})$.

The dimension of $A(\Delta)$ is equal to the dimension of the space $S_2(\Gamma_0(\Delta), \chi_\Delta)$ of weight 2 'nebentypus' cusp forms and is given by

$$\begin{aligned}\dim\, A(\Delta) = &\frac{\Delta}{12}\prod_{p|\Delta}\left(1+\frac{1}{p}\right) - \frac{1}{2}\#\{d|\Delta : \gcd(d, \Delta/d) = 1\} \\ &- \frac{1}{4}\sum_{\substack{x\in\mathbf{Z}/\Delta\mathbf{Z}\\ x^2+1=0}} \chi_\Delta(x) - \frac{1}{3}\#\{x \in \mathbf{Z}/\Delta\mathbf{Z} : x^2+x+1=0\}.\end{aligned}$$

This follows from the Trace Formula. See [8, p.168]. It is an exercise in elementary number theory to check that the dimension of $A(\Delta)$ grows approximately linearly with Δ and that it is zero if and only if $\Delta = 5$, 8, 12, 13, 17 or 21.

This paper is devoted to proving the other direction of Theorem 1.1. To this aim we study —like Abrashkin, Fontaine and [11]— commutative finite flat group schemes over the rings of integers of $\mathbf{Q}(\sqrt{\Delta})$ for $\Delta \leq 21$. More precisely, we try to classify 2-power order group schemes, or 2-group schemes for short, over these rings. It turns out that unramified twists cause trouble. They give rise to many more non-isomorphic group schemes. Life is easier when the base ring does not admit any non-trivial unramified quadratic extensions. Therefore we replace each real quadratic base field by its narrow Hilbert class field F. This is the maximal abelian extension that is unramified at every finite prime. In the range of our computations, this means that $F = \mathbf{Q}(\sqrt{\Delta})$ for $\Delta = 5$, 8, 13 and 17, while $F = \mathbf{Q}(\sqrt{\Delta}, \sqrt{-3})$ for $\Delta = 12$ and 21. In each case the field F has narrow class number 1.

We first determine the *simple* 2-group schemes over the ring of integers O_F of F. This is a computation involving finite extensions of F with bounded ramification. Here class field theory and discriminant bounds play a role. Rather than following [11], we use directly the bounds on certain ramification indices proved by Abrashkin and Fontaine. The relevant properties of Herbrand functions are discussed in section 2. We employ Odlyzko's *unconditional* discriminant bounds [6]. They are unconditional, in the sense that they do not depend on the truth of the Generalized Riemann Hypothesis (GRH). In section 3 we determine the simple 2-group schemes over the rings of integers of the narrow Hilbert class fields F of the six fields $\mathbf{Q}(\sqrt{\Delta})$ with $\Delta \leq 21$. It so happens that in each case all simple 2-group schemes have order 2.

Next we determine the possible extensions of the simple 2-group schemes by one another. Extensions involving the group schemes μ_2 and $\mathbf{Z}/2\mathbf{Z}$ are discussed in section 4, The remaining extension groups are described in sections 7 and 8. It turns out that for each F, several extension groups over O_F vanish. In some of the cases where the extension group is non-trivial, we explicitly describe the Hopf algebras of the non-split extensions.

This enables us to obtain a rough classification of 2-group schemes over the ring O_F. The group schemes $A[2^n]$ of the 2^n-torsion points of g-dimensional abelian varieties A over F with good reduction everywhere, or rather of their Néron models over O_F, are examples of 2-group schemes over O_F. For each $\Delta \leq 21$ we apply a criterion established in section 5 and show that if A were non-zero, then the group schemes $A[2^n]$ would not fit the classification for $n \gg 0$. This implies Theorem 1.1.

The cases $\Delta = 5$, 8 and 12 had been dealt with earlier [1, 3, 11], but using 3-group schemes rather than 2-group schemes. The case $\Delta = 13$ already appeared in a preprint by Hendrik Verhoek [14]. We take care of all six cases in a uniform way in sections 6, 7 and 8.

The dimensions of the abelian varieties $A(\Delta)$ are always even. They are equal to 2 if and only if $\Delta = 24$, 28, 29, 33, 37 or 41. In these cases there exists an elliptic curve over $\mathbf{Q}(\sqrt{\Delta})$ with good reduction everywhere. The abelian variety $A(\Delta)$ is isogenous to the product of this elliptic curve by its Galois conjugate. For $\Delta = 24$ see [9]. We study the other cases in a separate paper [10].

2. Ramification.

In this section we fix a prime p and a finite extension K of the field $\mathbf{Q}_p$ of p-adic numbers. Let $K \subset L$ be a finite Galois extension of degree n. Put $G = \mathrm{Gal}(L/K)$. Let O_K and O_L denote the rings of integers of K and L respectively. Let $e_{L/K}$ denote the inertia index and let $\alpha \in O_L$ be such that $O_L = O_K[\alpha]$. Following Fontaine [3], we put $i_{L/K}(\sigma) = v_K(\sigma(\alpha) - \alpha)$ for every $\sigma \in G$. Here v_K is the valuation that is normalized by requiring that a uniformizer of K has valuation 1. So, $i_{L/K}(\sigma)$ is contained in $\frac{1}{e_{L/K}}\mathbf{Z}$ for $\sigma \neq \mathrm{id}$, while $i_{L/K}(\mathrm{id}) = +\infty$. We put $i_{L/K} = \max_{\sigma \neq \mathrm{id}} i_{L/K}(\sigma)$ and $u_{L/K} = i_{L/K} + v_K(\mathfrak{d}_{L/K})$. Here $\mathfrak{d}_{L/K}$ denotes the different of L over K. Its norm is equal to the discriminant $\Delta_{L/K}$. The valuation $v_K(\mathfrak{d}_{L/K})$ is equal to the valuation of the root discriminant $\delta_{L/K} = \Delta_{L/K}^{1/n}$.

The Herbrand function $\phi_{L/K}$ is the increasing, continuous and piecewise linear function defined by

$$\phi_{L/K}(x) = \sum_{\sigma \in G} \min(i_{L/K}(\sigma), x), \qquad (x \in \mathbf{R}_{\geq 0}).$$

We have $u_{L/K} = \phi_{L/K}(i_{L/K})$. See [3, Prop.1.3]. Alternatively, the invariant $u_{L/K}$ can be characterized as follows. The i-th ramification subgroup of $\mathrm{Gal}(L/K)$ in the upper numbering is trivial for $i > u_{L/K}$ and $u_{L/K}$ is minimal with respect to this property.

If L and L' are two finite Galois extensions of K, then $u_{LL'/K} = \max(u_{L/K}, u_{L'/K})$. This follows from [12, IV, Prop.14]. If $K \subset L$ is a finite abelian extension, then $u_{L/K}$ is equal to the valuation of the conductor of L over K. See [12, XV, section 2, Cor. 3 of Thm.1].

The following lemma is due to Abrashkin [2, section 3, Prop.1]. It is used to do the computations in section 3.

Lemma 2.1. *Let $K \subset L \subset M$ be a finite extension and suppose that both L and M are Galois over K. Then we have*

$$u_{M/K} \;=\; u_{L/K} + \max(0, \frac{u_{M/L}}{e_{L/K}} - i_{L/K}).$$

Equivalently, $u_{M/K}$ is equal to $u_{L/K}$ if $u_{M/L} \leq i_{L/K} e_{L/K}$, while it is $\frac{u_{M/L}}{e_{L/K}} + v_K(\mathfrak{d}_{L/K})$ otherwise.

Proof. Taking the derivative of the transitivity relation $\phi_{M/K}(x) = \phi_{L/K}(\frac{\phi_{M/L}(e_{L/K}x)}{e_{L/K}})$ for $x \in \mathbf{R}_{\geq 0}$, we find

$$\phi'_{M/K}(x) = \phi'_{L/K}\left(\frac{\phi_{M/L}(e_{L/K}x)}{e_{L/K}}\right)\phi'_{M/L}(e_{L/K}x), \qquad \text{for } x \in \mathbf{R}_{\geq 0}.$$

The formula differs from the one in [12, IV, Prop.15] because we use Fontaine's normalization rather than Serre's [3, 1.1]. Derivatives of Herbrand functions are decreasing, locally constant functions. If the function $\phi'_{M/K}$ is discontinuous at $x' \in \mathbf{R}_{\geq 0}$, then either $\phi'_{L/K}(\frac{\phi_{M/L}(e_{L/K}x)}{e_{L/K}})$ or $\phi'_{M/L}(e_{L/K}x)$ is discontinuous at x'. The rightmost discontinuities

of $\phi'_{M/K}$, $\phi'_{M/L}$ and $\phi'_{L/K}$ occur at $x = i_{M/K}$, $i_{M/L}$ and $i_{L/K}$ respectively. Therefore $i_{M/K}$ is equal to $\max(\frac{i_{M/L}}{e_{L/K}}, x_0)$ where $x_0 \in \mathbf{R}_{\geq 0}$ satisfies $\frac{\phi_{M/L}(e_{L/K}x_0)}{e_{L/K}} = i_{L/K}$.

Since the function $\phi_{M/L}(e_{L/K}x)$ is increasing, we have $x_0 \geq \frac{i_{M/L}}{e_{L/K}}$ if and only if

$$i_{L/K} = \frac{\phi_{M/L}(e_{L/K}x_0)}{e_{L/K}} \geq \frac{\phi_{M/L}(e_{L/K}\frac{i_{M/L}}{e_{L/K}})}{e_{L/K}} = \frac{u_{M/L}}{e_{L/K}}.$$

So, if $u_{M/L} \leq i_{L/K}e_{L/K}$ we have

$$u_{M/K} = \phi_{M/K}(x_0) = \phi_{L/K}(\frac{\phi_{M/L}(e_{L/K}x_0)}{e_{L/K}}) = \phi_{L/K}(i_{L/K}) = u_{L/K}.$$

On the other hand, if $u_{M/L} \geq i_{L/K}e_{L/K}$, then we have $i_{M/K} = \frac{i_{M/L}}{e_{L/K}}$ and hence

$$u_{M/K} = \phi_{M/K}\left(\frac{i_{M/L}}{e_{L/K}}\right) = \phi_{L/K}\left(\frac{\phi_{M/L}(e_{L/K}\frac{i_{M/L}}{e_{L/K}})}{e_{L/K}}\right) = \phi_{L/K}\left(\frac{u_{M/L}}{e_{L/K}}\right).$$

For $x \geq i_{L/K}$ the function $\phi_{L/K}$ is given by $\phi_{L/K}(x) = x + u_{L/K} - i_{L/K} = x + v_{L/K}(\mathfrak{d}_K)$. Therefore, the inequality $\frac{u_{M/L}}{e_{L/K}} \geq i_{L/K}$ leads to the formula

$$u_{M/K} = \frac{u_{M/L}}{e_{L/K}} + v_K(\mathfrak{d}_{L/K}) = u_{L/K} + \frac{u_{M/L}}{e_{L/K}} - i_{L/K},$$

as required.

A finite flat commutative group scheme over O_K is the direct product of a finite flat group scheme of order prime to p and a p-group scheme, i.e. a finite flat group scheme of p-power order. A finite flat group scheme of order prime to p is étale and the extension $K \subset L$ generated by its points is unramified. On the other hand, the points of a p-group scheme G generate an extension L of K that may be ramified. However, the ramification index $u_{L/K}$ can be bounded. Indeed, if G is killed by p^m we have

$$u_{L/K} \leq v_K(p)\left(m + \frac{1}{p-1}\right).$$

This was proved Fontaine [3]. The important case $v_K(p) = m = 1$ was proved independently by Abrashkin [1]. Since $v_K(i_{L/K}) > 0$, the bound implies the strict inequality

$$v(\mathfrak{d}_{L/K}) < v_K(p)\left(m + \frac{1}{p-1}\right).$$

An example is provided by the group scheme μ_p over $K = \mathbf{Q}_p$. In this case $L = \mathbf{Q}_p(\zeta_p)$ and $e_{L/K} = p-1$. When $p > 2$ we have $i_{L/K} = v_K(\zeta_p - 1) = \frac{1}{p-1}$ and $\mathfrak{d}_{L/K} = (\zeta_p - 1)^{p-2}$, so that $u_{L/K} = 1$.

3. Simple 2-group schemes.

Let F be a number field and let O_F denote its ring of integers. A finite flat commutative group scheme G over O_F is simple if and only if its Galois module of points is irreducible. This implies that it is killed by some prime number p. The number field E generated by the points of G is a finite Galois extension of F. The field E has the following two properties, the second of which follows from the work of Abrashkin [1] and Fontaine [3]:

- the extension $F \subset E$ is unramified outside p and infinity;
- $u_{E_\mathfrak{q}/F_\mathfrak{p}} \leq (1 + \frac{1}{p-1})v_\mathfrak{p}(p)$ for every prime $\mathfrak{p}$ of F lying over p.

Here $F_\mathfrak{p}$ denotes the local field at $\mathfrak{p}$ and $E_\mathfrak{q}$ is the local field at a prime $\mathfrak{q}$ of E lying over $\mathfrak{p}$. By $v_\mathfrak{p}$ we denote the valuation that takes the value 1 on a uniformizer of $F_\mathfrak{p}$. Since E is Galois over F, the index $u_{E_\mathfrak{q}/F_\mathfrak{p}}$ defined in the previous section, only depends on $\mathfrak{p}$ and not on the prime $\mathfrak{q}$ of E lying over it.

In the rest of this section we take $p = 2$ and let F be the narrow Hilbert class field of a real quadratic number field of discriminant $\Delta \leq 21$. So, F is one of the six fields $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{13})$, $\mathbf{Q}(\sqrt{17})$, $\mathbf{Q}(i, \sqrt{-3})$ and $\mathbf{Q}(\sqrt{-7}, \sqrt{-3})$.

Theorem 3.1. *Let F be the narrow Hilbert class field of a real quadratic number field $\mathbf{Q}(\sqrt{\Delta})$ of discriminant Δ. Let E be the maximal extension of F inside an algebraic closure that is unramified outside 2 and infinity and has the property that $u_{E_\mathfrak{q}/F_\mathfrak{p}} \leq 2v_\mathfrak{p}(2)$ for all primes $\mathfrak{q}$ of E lying over primes $\mathfrak{p}$ of F that lie over 2. If $\Delta \leq 21$, then the Galois group $\mathrm{Gal}(E/F)$ is a finite 2-group.*

Proof. Put $\Gamma = \mathrm{Gal}(E/F)$. We write Γ' for its commutator subgroup. The restrictions on the ramification imply that the maximal abelian extension $F \subset F'$ inside E is the ray class field of F of conductor $4 \cdot \infty$, where ∞ denotes the infinite primes of F. A short computation shows that in all cases the fields F' are of the form $F(\sqrt{O_F^*})$ and the Galois group Γ/Γ' of F' over F is isomorphic to Klein's four group V_4. The degrees $[F' : \mathbf{Q}]$ are equal to 8 except when $\Delta = 12$ or 21 is which case they are equal to 16. In addition, it turns out that for each prime $\mathfrak{p}'$ of F' over a prime $\mathfrak{p}$ of F lying over 2 the *equality* $u_{F'_{\mathfrak{p}'}/F_\mathfrak{p}} = 2v_\mathfrak{p}(2)$ holds.

Since the global different is a product of local differents, the last inequality of section 2 implies that the root discriminant δ_E of the field E satisfies

$$\delta_E \;<\; 4\delta_F \;=\; 4\sqrt{\Delta} \;\leq\; 4\sqrt{21} \;=\; 18.33\ldots$$

Odlyzko's discriminant bounds [6] imply $[E : \mathbf{Q}] < 200$ and hence $[E : F'] < 200/8 = 25$. Therefore Γ' and Γ are solvable groups. It follows that E is equal to F' if and only if the maximal abelian extension F'' of F' inside E is equal to F'. The Galois group of F'' over F' is Γ'/Γ''. We have

$$\mathbf{Q}(\sqrt{\Delta}) \quad \subset \quad F \quad \subset \quad F' \quad \subset \quad F'' \quad \subset \quad E.$$

Let $\mathfrak{p}''$ be a prime of F'' lying over $\mathfrak{p}'$ lying over a prime $\mathfrak{p}$ of F lying over 2. Since the u-invariant $u_{F'_{\mathfrak{p}'}/F_\mathfrak{p}}$ attains its maximal value $2v_\mathfrak{p}(2)$, Lemma 2.1 implies that $u_{F''_{\mathfrak{p}''}}$ cannot

exceed $i_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}} e_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}}$. It follows that F'' is equal to the ray class field of F' of conductor $\mathfrak{p}'^k$ with $k \leq i_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}} e_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}}$.

It is easy to compute $i_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}}$ and $e_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}}$. The values are listed in Table 3.2. The third column of the table contains the number of primes $\mathfrak{p}$ of F lying over 2. The fourth column contains $u_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}}$, where $\mathfrak{p}'$ is a prime of F' lying over $\mathfrak{p}$. The fifth contains $v_{\mathfrak{p}}(\mathfrak{d}_{F'})$ and the sixth $i_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}}$. The seventh column contains the ramification index of $\mathfrak{p}'$ over $\mathfrak{p}$. The exponent $k = i_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}} e_{F'_{\mathfrak{p}'}/F_{\mathfrak{p}}}$ is listed in the eighth column.

Table 3.2.

Δ	F	$\#\mathfrak{p}$	u	$v(\mathfrak{d})$	i	e	k
5	$\mathbf{Q}(\sqrt{5})$	1	2	3/2	1/2	4	2
8	$\mathbf{Q}(\sqrt{2})$	1	4	5/2	3/2	4	6
12	$\mathbf{Q}(i,\sqrt{3})$	1	4	3	1	4	4
13	$\mathbf{Q}(\sqrt{13})$	1	2	3/2	1/2	4	2
17	$\mathbf{Q}(\sqrt{17})$	2	2	1	1	2	2
21	$\mathbf{Q}(\sqrt{-3},\sqrt{-7})$	2	2	3/2	1/2	4	2

In each case we used PARI/GP [7] to compute $[F'' : F']$. In all cases except $\Delta = 17$ we find that this degree is 1. Since Γ' is a solvable group, it follows that $\Gamma' = \Gamma''$ and $F'' = F' = E$, so that $\mathrm{Gal}(E/F)$ is isomorphic to Klein's four group V_4. This proves the theorem for $\Delta \neq 17$.

In the exceptional case $\Delta = 17$ the field F'' is strictly larger than F'. More precisely, let $\mathfrak{p}'_1$ and $\mathfrak{p}'_2$ denote the two primes of F' lying over 2. Then Lemma 2.1 implies that F'' is the ray class field of F' of conductor ${\mathfrak{p}'_1}^2{\mathfrak{p}'_2}^2 = (2)$. A short PARI/GP computation shows that F'' is a quadratic extension of F'.

In order to have PARI/GP compute the maximal abelian extension F''' of F'' inside E we need explicit generators of the field F''. We claim that $F'' = K'$, where $K' = \mathbf{Q}(i, \sqrt[4]{\alpha})$ and $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{17} = (\frac{3}{2} - \frac{1}{2}\sqrt{17})^2\varepsilon$, where $\varepsilon = 4 + \sqrt{17}$. Indeed, K' contains F' and is a cyclic degree 4 extension of the subfield $K = \mathbf{Q}(i, \sqrt{17})$ of F'. We have

$$\mathbf{Q}(\sqrt{17}) \quad \subset \quad K \quad \subset \quad F' \quad \subset \quad K'.$$

Moreover, K' is the ray class field of conductor 2 of K. Since the discriminants of K' and F'' are equal, so are the fields themselves. Let F''' be the maximal abelian extension of F'' inside E. By Lemma 2.1 the field F''' is contained in the ray class field of F'' conductor $1 + i$. A PARI/GP computation shows that this ray class field is equal to F'' itself. This shows that $F''' = F'' = E$ and hence that $\mathrm{Gal}(E/F)$ is a 2-group. This proves the theorem.

Next we apply Theorem 3.1 and determine the simple 2-group schemes over the rings of integers of the narrow Hilbert class fields F of $\mathbf{Q}(\sqrt{\Delta})$ for $\Delta \leq 21$. Group schemes of order 2 are always simple. It is easy to describe them. For every factorization $2 = ab$ for certain $a, b \in O_F$, there exists a finite flat group scheme J_a of order 2 over the ring of integers O_F with algebra $O_F[X]/(X^2 - aX)$ and group law given by $x + x' - bxx'$. For

$a = 1$ and 2 we recover the group schemes $\mathbf{Z}/2\mathbf{Z}$ and μ_2 respectively. Two group schemes J_a and $J_{a'}$ are isomorphic if and only if $a/a' \in O_F^*$. The Cartier dual of J_a is J_b. See the first page of [13] for the computations. The following theorem says that in our case all simple group schemes have order 2.

Theorem 3.3. *Let F be the narrow Hilbert class field of a real quadratic field of discriminant Δ. If $\Delta \leq 21$, then every simple 2-group scheme over O_F has order 2. More precisely, they are $\mathbf{Z}/2\mathbf{Z}$, μ_2 and in addition*

- *the selfdual group scheme J_π where $\pi = \sqrt{2}$ for $\Delta = 8$ and $\pi = i - 1$ for $\Delta = 12$;*
- *the group scheme J_π and its Cartier dual $J_{\pi'}$ for $\Delta = 17$ or 21. Here $\pi\pi' = 2$ and $\pi = \frac{3}{2} + \frac{1}{2}\sqrt{17}$ for $\Delta = 17$, while $\pi = \frac{1}{2} + \frac{1}{2}\sqrt{-7}$ for $\Delta = 21$.*

Proof. Let G be a simple 2-group scheme over O_F. Then it is killed by 2. Let E' be the extension of F generated by the points of G. By the theorems of Abrashkin [1] and Fontaine [3], the field E' is contained in the maximal extension E of F that is unramified outside 2 and infinity and that has the property that $u_{E_\mathfrak{q}/F_\mathfrak{p}} \leq 2v_\mathfrak{p}(2)$ for all primes $\mathfrak{q}$ of E lying over primes $\mathfrak{p}$ of F that lie over 2.

It follows from Theorem 3.1 that $\mathrm{Gal}(E/F)$ and hence $\mathrm{Gal}(E'/F)$ are 2-groups. Since $G(\overline{F})$ is a Galois module of order a power of 2, the Galois group $\mathrm{Gal}(E'/F)$ must have non-zero fixed points. The assumption that G is simple then implies that it has order 2 and we are done.

4. Extensions involving $\mathbf{Z}/2\mathbf{Z}$ and μ_2.

In this section we study extensions of the group schemes $\mathbf{Z}/2\mathbf{Z}$ and μ_2 by one another over the ring of integers O_F of a number field F. We do so under the assumption that the narrow class number h_F of F is *odd*. By class field theory this means that F does not admit any quadratic extensions that are unramified at all finite primes.

Let H be a finit flat group scheme over O_F. We say that a finite flat commutative group scheme G over O_F is a *successive extension* of group schemes isomorphic to H, if it admits a filtration with closed flat subgroup schemes $0 = G_0 \subset G_1 \subset G_2 \subset \ldots \subset G_n = G$ all of whose subquotients G_{k+1}/G_k are isomorphic to H.

Proposition 4.1. *Let F be a number field with odd narrow class number h_F. Then any successive extension of group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$ is constant and any successive extension of group schemes isomorphic to μ_2 is diagonalizable.*

Proof. A successive extension of group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$ is étale. Therefore its points generate an unramified Galois extension of 2-power degree. Since h_F is odd, any such extension of F is necessarily equal to F itself. The result then follows from Galois theory. The statement concerning μ_2 follows by Cartier duality.

We denote the group of extensions of finite flat commutative group schemes G by H over a ring R by $\mathrm{Ext}^1_R(G, H)$. The previous proposition is equivalent to saying that the groups $\mathrm{Ext}^1_{O_F}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ and $\mathrm{Ext}^1_{O_F}(\mu_2, \mu_2)$ have order 2, generated by the extensions $0 \to \mathbf{Z}/2\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$ and $0 \to \mu_2 \to \mu_4 \to \mu_2 \to 0$ respectively.

Proposition 4.2. *Let F be a number field with odd narrow class number h_F. Then there is an exact sequence*

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

Moreover, the natural map $\mathrm{Ext}^1_{O_F}(\mathbf{Z}/2\mathbf{Z}, \mu_2) \longrightarrow \mathrm{Ext}^1_F(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ is injective. In particular, any extension G of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 over O_F that is killed by 2 and for which $\mathrm{Gal}(\overline{F}/F)$ acts trivially on $G(\overline{F})$, is split.

Proof. Since the flat cohomology group $H^1(\mathrm{Spec}(O_F), \mathbf{G}_m)$ is isomorphic to the narrow class group of O_F, it has odd order. Therefore the exactness of the sequence of flat cohomology groups associated to the exact Kummer sequence $0 \to \mu_2 \to \mathbf{G}_m \to \mathbf{G}_m \to 0$ over O_F implies that $H^1(\mathrm{Spec}(O_F), \mu_2)$ and hence $\mathrm{Ext}^1_{O_F}(\mathbf{Z}, \mu_2)$ is isomorphic to $O_F^*/{O_F^*}^2$. An application of the contravariant functor $\mathrm{Hom}(-, \mu_2)$ to the exact sequence $0 \to \mathbf{Z} \to \mathbf{Z} \to \mathbf{Z}/2\mathbf{Z} \to 0$ gives the required exact sequence. We have similar sequences over F and over $\overline{F}$ rather than over O_F. It follows that the group of points of the non-trivial extension coming from the subgroup $\{\pm 1\}$ of $\mathrm{Ext}^1_{O_F}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ is cyclic of order 4. The second statement follows from this and from the fact that the natural map $O_F^*/{O_F^*}^2 \to F^*/{F^*}^2$ is injective. This proves the proposition.

We make the homomorphisms in the exact sequence of Proposition 4.2 more precise. For $\epsilon \in O_F^*$ we consider the O_F-algebra

$$O_F[X, Y]/(Y^2 - Y, X^2 - 1 + Y(1 - \epsilon)).$$

Its $\overline{F}$-points are $(\pm 1, 0)$ and $(\pm\sqrt{\epsilon}, 1)$. There are two possible group laws, which we denote by H_ϵ^+ and H_ϵ^-, depending on the sign in the addition formula

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

The elements of $\mathrm{Ext}^1_{O_F}(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ are of the form H_ϵ^+ or H_ϵ^-. The group scheme H_ϵ^+ is killed by 2, while the points of H_ϵ^- form a cyclic group of order 4. The closed subgroup scheme given by $Y = 0$ is isomorphic to μ_2 and the corresponding quotient group scheme $\mathbf{Z}/2\mathbf{Z}$ is $\mathrm{Spec}(O_F[Y]/(Y^2 - Y))$. The class of the extension

$$0 \longrightarrow \mu_2 \longrightarrow H_\epsilon^\pm \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0$$

in $\mathrm{Ext}^1_{O_F}(\mathbf{Z}, \mu_2)$ is mapped to ϵ in $O_F^*/{O_F^*}^2$. The non-trivial extension in the kernel is the group scheme H_{-1}^-. This group scheme is defined over $\mathbf{Z}$. Its group of points is cyclic of order 4 and has trivial Galois action.

To prove the next result we consider base changes of 2-group schemes over O_F to the rings $O_F[\frac{1}{2}]$, $O_F \otimes \mathbf{Z}_2$ and $O_F \otimes \mathbf{Q}_2$. For a prime $\mathfrak{p}$ of O_F, we let $O_\mathfrak{p}$ denote the completed local ring at $\mathfrak{p}$. Writing $F_\mathfrak{p}$ for the fraction field of $O_\mathfrak{p}$, we have $O_F \otimes \mathbf{Z}_2 = \prod_{\mathfrak{p}|2} O_\mathfrak{p}$ and $O_F \otimes \mathbf{Q}_2 = \prod_{\mathfrak{p}|2} F_\mathfrak{p}$.

Proposition 4.3. *Let F be a number field with odd narrow class number h_F and let H be a 2-group scheme over O_F of order 2.*

(i) If H is étale, it is isomorphic to $\mathbf{Z}/2\mathbf{Z}$. Moreover, $\mathrm{Ext}^1_{O_F}(H, \mathbf{Z}/2\mathbf{Z})$ is a 1-dimensional $\mathbf{F}_2$-vector space. The non-zero element is the class of the non-split extension provided by $\mathbf{Z}/4\mathbf{Z}$.

(ii) If H is not étale, then the $\mathbf{F}_2$-dimension of $\mathrm{Ext}^1_{O_F}(H, \mathbf{Z}/2\mathbf{Z})$ is $t-1$, where t denotes the number of primes $\mathfrak{p}$ of O_F for which H over $O_\mathfrak{p}$ is a local 2-group scheme.

Proof. Part (i) follows from Proposition 4.1. For (ii), let T denote the set of primes of O_F for which H is not étale over the local ring $O_\mathfrak{p}$. For every $\mathfrak{p} \in T$ any extension $0 \to \mathbf{Z}/2\mathbf{Z} \to G \to H \to 0$ is split over $O_\mathfrak{p}$. Since $T \neq \emptyset$ this implies that G is killed by 2 over O_F. For $\mathfrak{p} \notin T$ the group scheme G is étale over $O_\mathfrak{p}$. It follows that the Galois action is unramified at *every* prime. Since h_F is odd, the action of $\mathrm{Gal}(\overline{F}/F)$ on $G(\overline{F})$ is trivial. In other words, the extension is split over $O_F[\frac{1}{2}]$. Since G is killed by 2 and the Galois action on its points is trivial, the extension is split over $O_\mathfrak{p}$ for every $\mathfrak{p}$.

Since $\mathrm{Hom}(H, \mathbf{Z}/2\mathbf{Z})$ is zero over $O_\mathfrak{p}$ for $\mathfrak{p} \in T$ and $T \neq \emptyset$, the same is true over O_F. Therefore the Mayer-Vietoris exact sequence [11, Cor.2.4] becomes

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

Let m denote the number of primes $\mathfrak{p}$ of O_F dividing 2. Then $\mathrm{Hom}_{F \otimes \mathbf{Q}_2}(H, \mathbf{Z}/2\mathbf{Z})$ is an m-dimensional vector space over $\mathbf{F}_2$, while $\mathrm{Hom}_{F \otimes \mathbf{Z}_2}(H, \mathbf{Z}/2\mathbf{Z})$ has dimension $m-t$. Since $\mathrm{Hom}_{O_F[\frac{1}{2}]}(H, \mathbf{Z}/2\mathbf{Z})$ has dimension 1, the result follows.

We describe the extensions in the group $\mathrm{Ext}^1_{O_F}(H, \mathbf{Z}/2\mathbf{Z})$ of Proposition 4.3 (ii) under the assumption that the primes in O_F lying over 2 are principal. Then for some non-unit divisor $a \in O_F$ of 2, the group scheme H is isomorphic to the group scheme J_a introduced in section 3. Its algebra is $O_F[X]/(X^2 - aX)$. The elements of the quotient group $\mathrm{Hom}_{F \otimes \mathbf{Q}_2}(H, \mathbf{Z}/2\mathbf{Z})/\mathrm{Hom}_{F \otimes \mathbf{Z}_2}(H, \mathbf{Z}/2\mathbf{Z})$ are naturally identified with *ordered* pairs of coprime principal ideals (a'), (a'') of O_F satisfying $(a) = (a'a'')$. The elements of the quotient by $\mathrm{Hom}_{O_F[\frac{1}{2}]}(H, \mathbf{Z}/2\mathbf{Z})$ are naturally identified with *unordered* pairs. For every factorization $(a) = (a'a'')$ of this type there is an extension of J_a by $\mathbf{Z}/2\mathbf{Z}$:

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow J_{a'} \times J_{a''} \longrightarrow J_a \longrightarrow 0,$$

The embedding $\mathbf{Z}/2\mathbf{Z} \hookrightarrow J_{a'} \times J_{a''}$ corresponds to the surjective algebra homomorphism

$$O_F[X, Y]/(X^2 - a'X, Y^2 - a''Y) \longrightarrow O_F[T]/(T^2 - T)$$

given by $X \mapsto a'T$, $Y \mapsto a''T$. The morphism $J_{a'} \times J_{a''} \longrightarrow J_a$ corresponds to the algebra homomorphism

$$O_F[S]/(S^2 - aS) \longrightarrow O_F[X, Y]/(X^2 - a'X, Y^2 - a''Y)$$

given by $S \mapsto a''X + a'Y - aXY$.

5. A criterion.

In sections 6 and 7 we prove that over certain number fields there do not exist any non-zero abelian varieties with good reduction everywhere. The strategy is to check the conditions of the following proposition.

Proposition 5.1. *Let F be a number field and let p be a prime. If there is a constant $c > 0$ so that for every finite flat p-group scheme G there is a filtration with finite closed flat subgroup schemes*

$$0 \quad \subset \quad G_1 \quad \subset \quad G_2 \quad \subset \quad G,$$

for which G_1 is diagonalizable, G/G_2 is constant and the exponent of G_2/G_1 is at most c, then there does not exist a non-zero abelian variety over F with good reduction everywhere.

Proof. Let A be an abelian variety over F with good reduction everywhere. For every $n \geq 1$ the subgroup scheme $A[p^n]$ is finite and flat over O_F. Therefore there is a filtration as in the hypothesis of the proposition

$$0 \quad \subset \quad G_1 \quad \subset \quad G_2 \quad \subset \quad A[p^n].$$

Put $g = \dim A$. We choose a prime ideal of the ring of integers O_F that does not divide p. Let $\mathbf{F}_q$ be its residue field. Over $\mathbf{F}_q$ the group scheme $A[p^n]/G_2$ is étale. Since it is a closed subgroup scheme of the abelian variety A/G_2, its order is at most $\#(A/G_2)(\mathbf{F}_q)$. Since A and A/G_2 are isogenous, they have the same number of points over $\mathbf{F}_q$. Therefore the order of $A[p^n]/G_2$ is at most $\#A(\mathbf{F}_q)$.

The dual abelian variety A^{dual} is isogeneous to A and also has good reduction everywhere. Taking Cartier duals of the filtration of $A[p^n]$ we obtain a filtration of $A^{\mathrm{dual}}[p^n]$ as in the hypothesis of the proposition. This time the étale group scheme $G_1^\vee$ is a closed subgroup scheme of the abelian variety A^{dual}/G', where G' is the kernel of the morphism $A^{\mathrm{dual}}[p^n] \to G_1^\vee$. Since the orders of G_1 and $G_1^\vee$ are equal, it follows that the order of G_1 is at most $\#(A^{\mathrm{dual}}/G')(\mathbf{F}_q) = \#A(\mathbf{F}_q)$.

Finally, we observe that the group $A[p^n](\overline{F})$ can be generated by $2g$ points. The same is true for every subquotient. Since the subquotient G_2/G_1 of $A[p^n]$ has exponent at most c, it has order at most c^{2g}. The fact that the order of the group scheme $A[p^n]$ is equal to the product of the orders of the group schemes A/G_2), G_2/G_1 and G_1, implies that it is at most $\#A(\mathbf{F}_q)^2 c^{2g}$. Since this bound is independent of n, while the order of $A[p^n]$ is equal to p^{2ng}, we must have $g = 0$ and hence $A = 0$.

This proves the proposition.

6. The cases $\Delta = 5$ and 13.

In this section we prove Theorem 1.1 for the discriminants $\Delta = 5$ and 13. The case $\Delta = 5$ was already taken care of by Abrashkin and Fontaine, using 3-group schemes rather than 2-group schemes. The case $\Delta = 13$ is in a preprint by Hendrik Verhoek [14]. Our approach involves only 2-group schemes.

In both cases the field $F = \mathbf{Q}(\sqrt{\Delta})$ is equal to its narrow Hilbert class field. Let O_F denote the ring of integers of F. By Theorem 3.3 the only simple 2-group schemes over O_F are $\mathbf{Z}/2\mathbf{Z}$ and μ_2.

Proposition 6.1. *Let $F = \mathbf{Q}(\sqrt{5})$ or $\mathbf{Q}(\sqrt{13})$. Over O_F we have the following.*

(i) Every successive extension of group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$ is constant and every successive extension of group schemes isomorphic to μ_2 is diagonalizable.

(ii) Every extension $0 \to \mathbf{Z}/2\mathbf{Z} \to G \to \mu_2 \to 0$ is split.

Part (i) follows from Proposition 4.1. Since in both cases there is only one prime in O_F lying over 2, Proposition 4.3 implies (ii).

We check the conditions of Proposition 5.1. Any 2-group scheme G over O_F admits a filtration by closed flat group schemes H_i and simple successive subquotients H_{i+1}/H_i, which by Theorem 3.3 are isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2. If in this filtration there is a simple subquotient H_{i+1}/H_i isomorphic to $\mathbf{Z}/2\mathbf{Z}$ with adjacent subquotient H_{i+2}/H_{i+1} isomorphic to μ_2, then the extension $0 \to H_{i+1}/H_i \to H_{i+2}/H_i \to H_{i+2}/H_{i+1} \to 0$ is split by Prop. 6.1 (ii). Therefore we can modify the filtration and obtain a filtration $\ldots \subset H_i \subset H'_{i+1} \subset H_{i+2} \subset \ldots$ so that H'_{i+1}/H_i isomorphic to μ_2 while the subquotient H_{i+2}/H'_{i+1} isomorphic to $\mathbf{Z}/2\mathbf{Z}$. Loosely speaking, we can switch two adjacent subquotients $\mathbf{Z}/2\mathbf{Z}$ and μ_2 when μ_2 is the right of $\mathbf{Z}/2\mathbf{Z}$. Repeating this we obtain, in the notation of Proposition 5.1, a filtration

$$0 \quad \subset \quad G_1 \quad \subset \quad G_2 \quad \subset \quad G,$$

where G_1 is a successive extension of group schemes isomorphic to μ_2 and G/G_2 is a successive extension of group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$. In addition we have $G_1 = G_2$. By Proposition 6.1 (i) the group scheme G_1 is diagonalizable while G/G_2 is constant. Proposition 5.1 therefore implies that there are no non-zero abelian varieties over F with good reduction everywhere.

7. The cases $\Delta = 8$ and 12.

In this section we deal with the discriminants $\Delta = 8$ and 12. For these discriminants Theorem 1.1 has already been proven using 3-group schemes rather than the 2-group schemes that we employ here. The case $\Delta = 8$ was taken care of by Abrashkin and Fontaine, while $\Delta = 12$ is covered by the main result of [11].

In the cases $\Delta = 8$ and 12 the relevant fields are $F = \mathbf{Q}(\sqrt{2})$ and $F = \mathbf{Q}(\sqrt{-3}, i)$ respectively. In both cases the prime 2 is ramified in F. Let $\pi \in O_F$ be a generator of the prime lying over 2. Let O_π denote the completed local ring at π and let F_π denote its field of fractions. By Theorem 3.3 there is next to $\mathbf{Z}/2\mathbf{Z}$ and μ_2 a third simple group scheme J_π over O_F. Here $\pi = \sqrt{2}$ for $\Delta = 8$ and $\pi = i - 1$ for $\Delta = 12$. In both cases the ideal (2) is the square of the ideal generated by π. The group scheme J_π is self-dual.

Proposition 7.1. *Over O_F we have the following.*

(i) Every successive extension of group schemes isomorphic to $\mathbf{Z}/2\mathbf{Z}$ is constant and every successive extension of group schemes isomorphic to μ_2 is diagonalizable.

(ii) The extension groups $\mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z})$, $\mathrm{Ext}^1_{O_F}(\mu_2, J_\pi)$ and $\mathrm{Ext}^1_{O_F}(J_\pi, \mathbf{Z}/p\mathbf{Z})$ vanish.

Proof. Part (i) follows from Proposition 4.1. Since in both cases there is only one prime in O_F lying over 2, Proposition 4.3 implies that $\mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Ext}^1_{O_F}(J_\pi, \mathbf{Z}/p\mathbf{Z}) = 0$. By Cartier duality $\mathrm{Ext}^1_{O_F}(\mu_2, J_\pi)$ is also zero.

Arguing as we did for the cases $\Delta = 5$ and 13 in the last paragraph of section 6, we find that every 2-group scheme G over O_F admits a filtration with finite closed flat subgroup schemes

$$0 \quad \subset \quad G_1 \quad \subset \quad G_2 \quad \subset \quad G,$$

for which G_1 is diagonalizable, G/G_2 is constant and G_2/G_1 is a successive extension of group schemes isomorphic to J_π. Below we show that for both $\Delta = 8$ and 12 the group scheme G_2/G_1 is annihilated by 2. Therefore Proposition 5.1 implies that there does not exist a non-zero abelian variety over F with good reduction everywhere.

Proposition 7.2. *Let $F = \mathbf{Q}(i, \sqrt{-3})$. Then every extension over O_F*

$$0 \longrightarrow J_\pi \longrightarrow H \longrightarrow J_\pi \longrightarrow 0$$

is split. Every successive extension of group schemes isomorphic to J_π is killed by 2.

Proof. Let H be an extension of J_π by J_π over O_F. Greither has computed these extensions over the local ring O_π. For $k \geq 1$ let U_k denote the subgroup $\{u \in O_\pi^* : u \equiv 1 \pmod{\pi^k}\}$ of O_π^*. By [4, Cor. 3.6] the group $\mathrm{Ext}^1_{O_\pi}(J_\pi, J_\pi)$ is isomorphic to U_3/U_2^2. Since $U_2^2 = U_5$, this extension group has order 4. The extension H_u corresponding to $u \in U_3$ is killed by 2. Its points generate the field $F_\pi(\sqrt{u})$. Since $U_3 \cap {O_F^*}^2 = U_2^2$, the extension H_u is split if and only if the Galois action on its points is trivial.

For every $u \equiv 1 \pmod{\pi^3}$, the discriminant of $F_\pi(\sqrt{u})$ is at most π^2. It follows that the conductor of the number field E generated by the points of H over F is at most 2. A short computation shows that the ray class field of F of conductor 2 is equal to F itself. It follows that the Galois action on $H(\overline{F})$ is trivial. Therefore H splits over O_π as well as over $O_F[\frac{1}{2}]$. It follows then from the exactness of the Mayer-Vietoris sequence [11, Cor.2.4] that H is split over O_F, as required. The second statement is clear.

Proposition 7.2 does not hold for $\Delta = 8$ and $F = \mathbf{Q}(\sqrt{2})$. We have the following instead.

Proposition 7.3. *Let $F = \mathbf{Q}(\sqrt{2})$. Then the group $\mathrm{Ext}^1_{O_F}(J_\pi, J_\pi)$ has order 2. In other words, there exists a unique non-split extension over O_F*

$$0 \longrightarrow J_\pi \longrightarrow \Upsilon \longrightarrow J_\pi \longrightarrow 0.$$

The group scheme Υ is self-dual and killed by 2. Every successive extension of group schemes isomorphic to J_π is killed by 2.

Proof. We can repeat most of the proof of the previous proposition. Near the end things become more complicated because the ray class field of conductor $2 \cdot \infty$ of F is not equal to F, but rather to the quadratic extension $F(i) = \mathbf{Q}(\zeta_8)$. It follows from from the exactness of the Mayer-Vietoris sequence [11, Cor.2.4] that $\mathrm{Ext}^1_{O_F}(J_\pi, J_\pi)$ has order 2, as required. Since it is unique, the non-split extension Υ is self-dual. By Greithers local results [4, Cor. 3.6], it is killed by 2.

We prove by induction that every successive extension of group schemes isomorphic to J_π is killed by 2. Indeed, let

$$0 \hookrightarrow H_1 \hookrightarrow H_2 \hookrightarrow \ldots \hookrightarrow H_n$$

be such an extension. The statement is obvious for $n = 1$. When $n = 2$ there are only two possibilities for H_n. It is either isomorphic to Υ or to $J_\pi \times J_\pi$. In either case it is killed by 2. For $n \geq 3$ consider H_2. If H_2 is isomorphic to Υ, then the extension $0 \to H_2 \to H_n \to H_n/H_2 \to 0$ splits. It follows by induction that H_n is killed by 2. The other possibility is that H_2 is isomorphic to $J_\pi \times J_\pi$. In this case H_2 admits two distinct closed flat subgroup schemes G_0 and G_0', both necessarily isomorphic to J_π. The natural morphism $H_n \to H_n/G_0 \times H_n/G_0'$ is injective. By induction both H_n/G_0 and H_n/G_0' are killed by 2. Therefore, so is H_n.

This proves the theorem.

Out of curiosity we determine the Hopf algebra of Υ. Its points generate the quadratic extension $F(i)$ of F. Since Υ admits is a closed subgroup scheme H isomorphic to J_π and since Υ/H is also isomorphic to J_π, it seems reasonable to guess that the Hopf algebra is of the form

$$O_F[X,Y]/(Y^2 - \sqrt{2}Y, X^2 - \sqrt{2}X + uY).$$

The equation $Y = 0$ cuts out the closed subgroup scheme H. The subalgebra $O_F[Y]/(Y^2 - \sqrt{2}Y)$ is the Hopf algebra of the quotient Υ/H. The element $u \in O_F$ must have the property that the discriminant $2 - 4u\sqrt{2}$ of the polynomial $X^2 - \sqrt{2}X + u\sqrt{2}$ is of the form $-v^2$ for some $v \in O_F$. With the choice $u = 1 + \sqrt{2}$ the discriminant is $-(2+\sqrt{2})^2$ and the points of Υ are $(0,0)$, $(\sqrt{2},0)$, $(\alpha, \sqrt{2})$ and $(\overline{\alpha}, \sqrt{2})$, where $\alpha = \frac{1+i(1+\sqrt{2})}{\sqrt{2}}$.

Choosing the point $(0,0)$ as the neutral element, the addition formula is of the form $(x,y) + (x',y') = (x + x' + g(x,x',y,y'), y + y' - \sqrt{2}yy')$, for a certain polynomial g. The coefficients of g are determined by solving a system of six linear equations in six unknowns obtained from the additive relations between the three non-zero points. The resulting addition formula is

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

The following proposition alloows us to apply proposition 5.1.

Proposition 7.4. *The extension groups* $\mathrm{Ext}^1_{O_F}(J_\pi, \Upsilon)$ *and* $\mathrm{Ext}^1_{O_F}(\Upsilon, J_\pi)$ *both vanish.*

Proof. By Cartier duality the two extension groups are isomorphic. It suffices therefore to show that any extension

$$0 \longrightarrow \Upsilon \longrightarrow V \longrightarrow J_\pi \longrightarrow 0$$

is split. Let J denote the unique order 2 subgroup scheme of Υ. Both J and Υ/J are isomorphic to J_π. Applying the functor $\mathrm{Hom}_{O_F}(J_\pi, -)$ to the short exact sequence $0 \to J \to \Upsilon \to \Upsilon/J \to 0$ we see that the natural map $\mathrm{Ext}^1_{O_F}(J_\pi, \Upsilon) \hookrightarrow \mathrm{Ext}^1_{O_F}(J_\pi, \Upsilon/J)$ is

injective. Suppose the extension V is not split. Then the image of V in $\mathrm{Ext}^1_{O_F}(J_\pi, \Upsilon/J)$ is also non-split. In other words, the extension

$$0 \longrightarrow \Upsilon/J \longrightarrow V/J \longrightarrow J_\pi \longrightarrow 0$$

is non-split. This can only happen when V/J is isomorphic to Υ. We choose generators $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ of $V(\overline{F})$ as follows. Let $\mathbf{e}_1 \in J(\overline{F})$, $\mathbf{e}_2 \in \Upsilon(\overline{F}) - J(\overline{F})$ and $\mathbf{e}_3 \in V(\overline{F}) - \Upsilon(\overline{F})$. Then the Galois action of $\sigma \in \mathrm{Gal}(\overline{F}/F)$ on $V(\overline{F})$ is given by the formulas

$$\begin{aligned}
\sigma(\mathbf{e}_1) &= \mathbf{e}_1, \\
\sigma(\mathbf{e}_2) &= \mathbf{e}_2 + \chi(\sigma)\mathbf{e}_1, \\
\sigma(\mathbf{e}_3) &= \mathbf{e}_3 + \chi(\sigma)\mathbf{e}_2 + \psi(\sigma)\mathbf{e}_1.
\end{aligned}$$

Here $\chi : \mathrm{Gal}(\overline{F}/F) \to \mathbf{F}_2$ is the character corresponding to the quadratic field extension $F \subset F(i)$ and ψ is an $\mathbf{F}_2$-valued map on $\mathrm{Gal}(\overline{F}/F)$. A short computation shows that for every $\sigma \in \mathrm{Gal}(\overline{F}/F)$ its square σ^2 fixes $\mathbf{e}_1$ and $\mathbf{e}_2$ while $\sigma^2(\mathbf{e}_3) = \mathbf{e}_3 + \chi(\sigma)\mathbf{e}_1$. It follows that the field E generated by the points of V is a cyclic extension of F of degree 4.

Since V is killed by 4, it follows from section 2 or [3, Théorème A] that the conductor of E is π^k where k is at most $v_\pi(2)(2+1) = 6$. Since $\pi^6 = \sqrt{2}^6 = 8$ and since $3 + 2\sqrt{2}$ is a generator of the totally positive units, the ray class group of F of conductor $\pi^6 \cdot \infty$ is isomorphic to $(\mathbf{Z}[\sqrt{2}]/8\mathbf{Z}[\sqrt{2}])^*/\langle 3 + 2\sqrt{2}\rangle$. A short computation shows that this group has exponent 2. Since E is contained in the ray class field $\pi^6 \cdot \infty$, this shows that E cannot exist. This means that the extension V is split. This proves the proposition.

It follows that $\mathrm{Ext}^1_{O_F}(G, \Upsilon)$ and $\mathrm{Ext}^1_{O_F}(\Upsilon, G)$ vanish for every group scheme G that is a successive extension of group schemes isomorphic to J_π. By the arguments at the end of section 6, Propositions 7.2, 7.3 and 7.4 imply that the conditions of Proposition 5.1 are satisfied for the field $F = \mathbf{Q}(\sqrt{2})$.

8. The cases $\Delta = 17$ and $\Delta = 21$.

In this section we prove Theorem 1.1 for the discriminants $\Delta = 17$ and $\Delta = 21$. Let F denote the narrow Hilbert class field of $\mathbf{Q}(\sqrt{\Delta})$. In both cases the narrow class number h_F of F is 1 and the unit group O_F^* is generated by -1 and a unit ε of infinite order. In both cases the prime 2 splits into a product of two distinct primes π and π' of O_F. To be specific, for $\Delta = 17$ we have $F = \mathbf{Q}(\sqrt{17})$ and $2 = -\pi\pi'$ where $\pi = \frac{3}{2} + \frac{1}{2}\sqrt{17}$ and $\pi' = \frac{3}{2} - \frac{1}{2}\sqrt{17}$. The unit ε is $4 + \sqrt{17}$. On the other hand, for $\Delta = 21$ the narrow Hilbert class field is $F = \mathbf{Q}(\sqrt{-3}, \sqrt{-7})$. We have $2 = \pi\pi'$ where $\pi = \frac{1}{2} + \frac{1}{2}\sqrt{-7}$ and $\pi' = \frac{1}{2} - \frac{1}{2}\sqrt{-7}$. In this case $\varepsilon = \frac{1}{2}(\sqrt{-3} + \sqrt{-7})$. Let O_π and $O_{\pi'}$ denote the corresponding completed local rings.

By Theorem 3.3 there are four simple 2-group schemes over O_F. They all have order 2. They are $\mathbf{Z}/2\mathbf{Z}$, μ_2 and the group schemes J_π and $J_{\pi'}$ introduced in section 3. They are Cartier dual to one another. We proceed by computing the possible extensions of these four simple group schemes by one another.

Theorem 8.1. *Over O_F we have the following.*

(i) *Any successive extension of group schemes isomorphic to* $\mathbf{Z}/2\mathbf{Z}$ *is constant; any successive extension of group schemes isomorphic to* μ_2 *is diagonalizable.*

(ii) *The group* $\mathrm{Ext}^1_{O_F}(\mu_2, \mathbf{Z}/2\mathbf{Z})$ *has order 2. The unique non-trivial extension is of the form*

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow J_\pi \times J_{\pi'} \longrightarrow \mu_2 \longrightarrow 0.$$

(iii) *The four extension groups* $\mathrm{Ext}^1_{O_F}(J_\pi, \mathbf{Z}/2\mathbf{Z})$, $\mathrm{Ext}^1_{O_F}(J_{\pi'}, \mathbf{Z}/2\mathbf{Z})$, $\mathrm{Ext}^1_{O_F}(\mu_2, J_\pi)$ *and* $\mathrm{Ext}^1_{O_F}(\mu_2, J_{\pi'})$ *all vanish.*

(iv) *The extension groups* $\mathrm{Ext}^1_{O_F}(J_\pi, J_{\pi'})$ *and* $\mathrm{Ext}^1_{O_F}(J_{\pi'}, J_\pi)$ *both vanish.*

Proof. Since $h_F = 1$, part (i) follows from Proposition 4.1. Parts (ii) and (iii) follow from Proposition 4.3 (ii) and Cartier duality. To prove (iv), it suffices to show that an exact sequence over O_F

$$0 \longrightarrow J_\pi \longrightarrow G \longrightarrow J_{\pi'} \longrightarrow 0$$

must split. Since J_π is étale over $O_{\pi'}$ and $J_{\pi'}$ is local over $O_{\pi'}$, the extension is split over $O_{\pi'}$. This implies that G is killed by 2. Over O_π the extension looks like

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

By the results of section 4, locally over O_π the points of G generate a field that is obtained by extracting a square root of a unit in O_π^*. Therefore the local conductor of the corresponding quadratic character, is at most π^2.

We proceed by proving that $\mathrm{Gal}(\overline{F}/F)$ acts trivially on $G(\overline{F})$. Since F is totally complex for $\Delta = 21$, while it is totally real for $\Delta = 17$, the proof diverges at this point. For $\Delta = 21$ the field F has no real infinite primes. A short computation shows that the ray class group of F of conductor π^2 is trivial. Therefore the Galois action on $G(\overline{F})$ is trivial.

For $\Delta = 17$, the field has two real infinite primes. The field extension $F \subset E$ generated by the points of G is a subfield of the ray class field of conductor $\pi^2 \cdot \infty$. Since G splits over $O_{\pi'}$, the Galois group $\mathrm{Gal}(E/F)$ is isomorphic to the 3-dimensional $\mathbf{F}_2$-vector space $V = (O/(\pi^2))^* \times \{\pm 1\} \times \{\pm 1\}$ modulo the subgroup generated by the images of the units -1 and $\varepsilon = 4 + \sqrt{17}$ and the Frobenius element π'. With respect to a suitable $\mathbf{F}_2$-basis of V, these images are the row vectors of the following matrix

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

Since the matrix is invertible, the extension field E is equal to F and once again the Galois action on $G(\overline{F})$ is trivial.

In both cases G is split over $O_F[\frac{1}{2}]$. Proposition 4.2 implies that G is also split over O_π. By the exactness of the Mayer-Vietoris sequence G is then split over O_F. See [11, Cor.2.4]. This proves the theorem.

Arguing as in the last paragraph of section 6, we find that every 2-group scheme G over O_F admits a filtration with finite closed flat subgroup schemes

$$0 \quad \subset \quad G_1 \quad \subset \quad G_2 \quad \subset \quad G,$$

for which G_1 is diagonalizable, G/G_2 is constant and G_2/G_1 is a product of two 2-group schemes, one being a successive extension of group schemes isomorphic to J_π and the other a successive extension of group schemes isomorphic to $J_{\pi'}$. Below we show that G_2/G_1 is killed by some absolute constant c. We can take $c = 2$ for $\Delta = 21$ and $c = 8$ for $\Delta = 17$. This is the content of Propositions 8.2 and 8.3. By Proposition 5.1 they imply that there does not exist a non-zero abelian variety over F with good reduction everywhere.

Proposition 8.2. *Over the ring of integers O_F of $F = \mathbf{Q}(\sqrt{-3}, \sqrt{-7})$ the extension groups $\mathrm{Ext}^1_{O_F}(J_\pi, J_\pi)$ and $\mathrm{Ext}^1_{O_F}(J_{\pi'}, J_{\pi'})$ vanish. Over O_F every successive extension of group schemes isomorphic to J_π is killed by 2. The same is true for successive extensions of group schemes isomorphic to $J_{\pi'}$.*

Proof. It suffices to show that every extension over O_F

$$0 \longrightarrow J_\pi \longrightarrow G \longrightarrow J_\pi \longrightarrow 0$$

splits. The group scheme G is étale over $O_{\pi'}$ and multiplicative over O_π. If G were *not* killed by 2, then $\mathrm{Gal}(\overline{F}/F)$ acts on $G(\overline{F})$ through a quadratic character χ that is unramified outside π' and for which $\omega\chi^{-1}$ is unramified over $O_{\pi'}$. Here ω denotes the cyclotomic character of conductor $4 = \pi^2\pi'^2$. Therefore χ has conductor π'^2. Since the ray class group of F of conductor π'^2 is trivial, this leads to a contradiction.

Therefore G is killed by 2. It follows that the Galois action is necessarily unramified at all primes. Therefore it is trivial. This implies that G is split over $O_F[\frac{1}{2}]$ and also over both O_π and $O_{\pi'}$. The exactness of the Mayer-Vietoris sequence implies therefore that G is split over O_F.

The last two statements are clear. This proves the proposition.

Proposition 8.2 is false for $F = \mathbf{Q}(\sqrt{17})$. There does exist a non-split extension of the group scheme J_π by itself. Since the ray class group of conductor $\pi^2 \cdot \infty$ is a quadratic extension of F, the equivalence of categories [11, Prop. 2.3 and Cor.2.4] implies that $\mathrm{Ext}^1_{O_F}(J_\pi, J_\pi)$ has order 2. Similarly, the group $\mathrm{Ext}^1_{O_F}(J_{\pi'}, J_{\pi'})$ has order 2. Here is an explicit description of the unique non-split extension G of J_π by itself. It is the order 4 group scheme whose algebra is

$$O_F[X, Y]/(X^2 - \pi X + Y, Y^2 - \pi Y)$$

and with group law given by

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

The points of G are defined over the quadratic extension $F(\sqrt{-\varepsilon})$ of F. The group $G(\overline{F})$ is cyclic of order 4. Multiplication by 2 is given by the formula

$$(x, y) \mapsto (y, 0).$$

So, the closed subgroup scheme given by $Y = 0$ is the kernel this morphism. The cokernel is the spectrum of the subalgebra $O_F[Y]/(Y^2 - \pi Y)$. The discriminant of G is π^8. The conjugate of G is also its Cartier dual.

Proposition 8.3. *Let $F = \mathbf{Q}(\sqrt{17})$. Every successive extension over O_F of group schemes isomorphic to J_π has exponent at most 8. The same is true for every successive extension of group schemes isomorphic to $J_{\pi'}$.*

Proof. Let $n \geq 1$ and let H be a 2-group scheme that has exponent 2^n and is a successive extension of group schemes isomorphic to J_π. Its Cartier dual $H^\vee$ also has exponent 2^n and is a successive extension of group schemes isomorphic to $J_{\pi'}$. Let F' be the field extension of F generated by the points of H and, similarly, let F'' be generated by the points of $H^\vee$. The field F' is unramified outside $\pi' \cdot \infty$ and F'' is unramified outside $\pi \cdot \infty$. Since the narrow class number of F is 1, it follows that we have $F' \cap F'' = F$.

Since O_π^* is isomorphic to $\mathbf{Z}_2^*$, class field theory implies that the Galois group of the maximal *abelian* extension of F inside F' is a quotient of the group $\mathbf{Z}_2^* \times \{\pm 1\} \times \{\pm 1\}$ modulo the images of the units -1 and ε. The latter group is isomorphic to Klein's four group V_4. Similarly, the Galois group of the maximal *abelian* extension of F inside F'' is a quotient of V_4. It follows that the Galois group of the maximal abelian extension E of F inside $F'F''$ has exponent 2. However, by Cartier duality E contains the 2^n-th roots of unity. Since $\mathrm{Gal}(F(\zeta_{2^n})/F)$ isomorphic to $(\mathbf{Z}/2^n\mathbf{Z})^*$, it follows that $n \leq 3$.

Bibliography

[1] Abrashkin, 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] Abrashkin, V.A.: A group-theoretical property of the ramification filtration, *Izvestiya RAN*, ser. matem. **62** (1998), 3–26; English transl., Izvestiya: Mathematics **62** (1998), 1073–1094.

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

[4] Greither, C.: Extensions of finite group schemes, and Hopf Galois theory over a complete discrete valuation ring, *Math Zeitschrift* **210** (1992), 37–68.

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

[6] Odlyzko, A.: Discriminant bounds, November 29, 1976. `http://www-users.cse.umn.edu/~odlyzko/unpublished/index.html`

[7] The PARI/GP computer algebra system, `https://pari.math.u-bordeaux.fr`

[8] Schoof, R. and Van der Vlugt, M.: Hecke operators and the weight distributions of certain codes, *Journal of Combinatorial Theory A* **57** (1991), 163–186.

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

[10] Schoof, R.: Abelian varieties over real quadratic fields with good reduction everywhere II, in preparation.

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

[12] Serre, J.-P.: *Corps Locaux*, Hermann, Paris, 1962.

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

[14] Verhoek, H.: Etale subquotients of prime torsion of abelian schemes, Universität Bielefeld (2012), preprint 12058; arXiv:1205.1409.