Preliminary version
May 8, 2024

GRH AND FINITE FLAT GROUP SCHEMES OVER Z

LASSINA DEMBÉLÉ AND RENÉ SCHOOF

Abstract. Since simple commutative finite flat group schemes G over $\mathbf{Z}$ are killed by a prime number p, their order is a power of p. Tate asked whether a simple group scheme G is necessarily equal to $\mathbf{Z}/p\mathbf{Z}$ or μ_p. This has been proved for primes $p \leq 19$. Under assumption of the Generalized Riemann Hypothesis we extend this result to primes $p \leq 37$.

1. Introduction

A finite flat commutative group scheme G over $\mathbf{Z}$ is simple if and only if the set of its points $G(\overline{\mathbf{Q}})$ is an irreducible Galois module. Therefore G is annihilated by some prime number p and G is a p-group scheme in the sense that its order is a power of p. Group schemes of prime order p are simple. By a theorem of Oort and Tate [14], the only ones over $\mathbf{Z}$ are the constant group scheme $\mathbf{Z}/p\mathbf{Z}$ and its Cartier dual μ_p. Tate asked the following question [13].

Question 1.1. *Let p be a prime number. Are $\mathbf{Z}/p\mathbf{Z}$ and μ_p the only simple p-group schemes defined over $\mathbf{Z}$?*

Simple p-group schemes over $\mathbf{Z}$ cannot have order p^2. Indeed, suppose that such a group scheme G existed. Let G^D be the Cartier dual of G, and $G(\overline{\mathbf{Q}})$ and $G^D(\overline{\mathbf{Q}})$ their respective $\overline{\mathbf{Q}}$-points. Then, the determinant of the Galois action on $G(\overline{\mathbf{Q}})$ would be a power of the mod p cyclotomic character ω. Over the ring $\mathbf{Z}_p$ (and up to an unramified twist), the group scheme G would be either a (p,p)-group scheme in the sense of Raynaud [7], in which case the Galois action on the determinant is via ω, or an extension of group schemes isomorphic to $\mathbf{Z}/p\mathbf{Z}$ or μ_p. However, the Galois action on $G(\overline{\mathbf{Q}})$ and on $G^D(\overline{\mathbf{Q}})$ cannot be unramified at every prime. Therefore, over $\mathbf{Z}_p$ the group scheme G is an extension of $\mathbf{Z}/p\mathbf{Z}$ by μ_p, so that also in this case the action on the determinant would be via ω. Since ω is an odd character, Khare's proof of the level 1 Serre conjecture implies then that $G(\overline{\mathbf{Q}})$ must be reducible [4]. Therefore G cannot simple.

It is not known whether simple p-group schemes over $\mathbf{Z}$ can have order p^k for some $k \geq 3$. However, for small primes p this cannot happen. Abrashkin [1] and Fontaine [3] both showed that Question 1.1 has an affirmative answer for

The second author acknowledges GNSAGA and the MIUR Excellence Department Project awarded to the Department of Mathematics, University of Rome Tor Vergata, CUP E83C18000100006.

primes $p \leq 17$. In [2] this result is extended to $p = 19$. In this paper we prove the following theorem under the Generalized Riemann Hypothesis (GRH).

Theorem 1.2 (GRH)**.** *For every prime $p \leq 37$ the only simple finite flat commutative group schemes over $\mathbf{Z}$ of p-power order are $\mathbf{Z}/p\mathbf{Z}$ and μ_p.*

The main idea in the proof of Theorem 1.2 is also at the heart of the proof of the non-existence of abelian varieties with everywhere good reduction over $\mathbf{Q}$ by Abrashkin and Fontaine. It is the fact that for p a prime, and G a p-group scheme over $\mathbf{Z}$ killed by p, the field F generated by the points of G is a finite Galois extension of $\mathbf{Q}$ which has very little ramification. More precisely, F has the following two properties, the second of which follows from works of Abrashkin [1] and Fontaine [3].

(A) F is unramified outside p and ∞;
(B) $u_{F_\mathfrak{p}/\mathbf{Q}_p} \leq 1 + \frac{1}{p-1}$ for all primes $\mathfrak{p}$ of F lying over p.

Here, the invariant $u_{F_\mathfrak{p}/\mathbf{Q}_p}$, which only depends on the structure of the group scheme G over $\mathbf{Z}_p$, is defined as follows. Let $\mathfrak{p}$ be a prime of F lying over p, and let $F_\mathfrak{p}$ denote the completion of F at $\mathfrak{p}$. Let $\mathcal{O}_{F_\mathfrak{p}}$ be the ring of integers of $F_\mathfrak{p}$, and $\mathfrak{d}_\mathfrak{p}$ the different of $F_\mathfrak{p}$ over $\mathbf{Q}_p$. Then, by Kummer, we can write $\mathcal{O}_{F_\mathfrak{p}} = \mathbf{Z}_p[\alpha]$, for some $\alpha \in \mathcal{O}_{F_\mathfrak{p}}$. We define

$$u_{F_\mathfrak{p}/\mathbf{Q}_p} = i_\mathfrak{p} + v(\mathfrak{d}_\mathfrak{p}), \text{ where } i_\mathfrak{p} = \max\big\{v(\sigma(\alpha) - \alpha) : \sigma \in \mathrm{Gal}(F_\mathfrak{p}/\mathbf{Q}_p),\ \sigma \neq 1\big\}.$$

The valuation v is normalized by setting $v(p) = 1$. It follows that both $i_\mathfrak{p}$ and $v(\mathfrak{d}_\mathfrak{p})$ are in $\frac{1}{e_\mathfrak{p}}\mathbf{Z}$, where $e_\mathfrak{p}$ is the ramification index of $F_\mathfrak{p}$ over $\mathbf{Q}_p$. Note that the local root discriminant $\delta_{F_\mathfrak{p}}$ of F is equal to $p^{v(\mathfrak{d}_\mathfrak{p})}$ for each $\mathfrak{p}$. Therefore, by [3, sect. 3.3], the global root discriminant δ_F satisfies

$$\delta_F < p^{1+\frac{1}{p-1}}.$$

See [2] for a characterization of the invariant $u_{F_\mathfrak{p}/\mathbf{Q}_p}$ in terms of the upper numbering of the higher ramification groups.

The *Abrashkin-Fontaine field* is the maximal extension $\mathbf{Q} \subset F$ having the two properties (A) and (B) above. It contains the cyclotomic field $\mathbf{Q}(\zeta_p)$ as well as its Hilbert class field H. More generally, F does not admit any proper extensions that are unramified outside p and ∞ and are at most tamely ramified at p. In Section 3, we prove under the assumption of GRH that for $p \leq 37$ the Abrashkin-Fontaine field is actually equal to H. It follows that for $p \leq 37$, the points of a simple finite flat commutative p-power order group scheme G over $\mathbf{Z}$ are defined over the Hilbert class field H. A little bit of group theory then implies that the points of G are actually defined over the subfield $\mathbf{Q}(\zeta_p)$. The theorems of Oort and Tate [14] then imply Theorem 1.2. In other words, the group scheme G is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ or μ_p.

For $p \geq 41$, bounds on the root discriminant of F are too large for the GRH Odlyzko bounds to apply. Therefore we do not have any bound on the degree of the Abrashkin-Fontaine field F. However, for larger p, we expect that F is usually strictly larger than the Hilbert class field H. This already happens for small values of p. Indeed, for $p = 53$, the splitting field H' of $x^8 - x^7 + 3x^6 - 3x^5 + 2x^4 - 2x^3 + 5x^2 + 5x + 1$ is unramified outside 53 and ∞. Since it is only tamely ramified at 53, it is contained in the Abrashkin-Fontaine field for $p = 53$. However, the Galois group of H' over $\mathbf{Q}$ is the non-solvable group $\mathrm{PGL}_2(\mathbf{F}_7)$. This implies that H' cannot be a subfield of H.

Similarly, for $p = 59$ the splitting field H'' of $x^4 - x^3 - 7x^2 + 11x + 3$ is unramified outside 59 and ∞. Therefore it is contained in the Abrashkin-Fontaine field F for $p = 59$. The Galois group of H'' over $\mathbf{Q}$ is isomorphic to the symmetric group S_4.

Since the Galois group of the Hilbert class field H of $\mathbf{Q}(\zeta_{59})$ is metabelian, and S_4 is not, H'' is not contained in H.

The Abrashkin-Fontaine field F may not even be a finite extension of $\mathbf{Q}$. Indeed, the entire Hilbert class field tower of $\mathbf{Q}(\zeta_p)$ is contained in F. The smallest prime p for which we know this tower to be infinite is $p = 401$. Since the degree 8 subfield of $\mathbf{Q}(\zeta_{401})$ has class number 45, this follows from the following result. The proof is similar to the proof of [8, Theorem 5.1].

Proposition 1.3. *Let $p > 2$ be a prime. If there exists a divisor d of $p-1$ for which $(p-1)/d$ is odd and for which the class number of the degree $d/2$ subfield of $\mathbf{Q}(\zeta_p)$ exceeds $2d+5$, then the class field tower of $\mathbf{Q}(\zeta_p)$ is infinite.*

2. The Abrashkin-Fontaine field F

Let p be a prime and let H be the Hilbert class field of $\mathbf{Q}(\zeta_p)$. It is contained in the Abrashkin-Fontaine field F defined in the introduction. The root discriminants of F and its subfields are smaller than $p^{1+\frac{1}{p-1}}$. In particular, for $p = 2$ the root discriminant of F is < 4. Odlyzko's discriminant bounds easily imply that $F = \mathbf{Q}(i)$ in this case. For $p > 2$ we have the following results.

Proposition 2.1. *Let $p > 2$ be prime and let F be the Abrashkin-Fontaine field. Then*

(a) *the maximal abelian extension of $\mathbf{Q}$ inside F is $\mathbf{Q}(\zeta_p)$;*
(b) *the maximal abelian extension of $\mathbf{Q}(\zeta_p)$ inside F is the Hilbert class field H of $\mathbf{Q}(\zeta_p)$.*

Proof. (a) By the Kronecker-Weber theorem the maximal abelian extension of $\mathbf{Q}$ that is unramified outside p is contained in a cyclotomic field $\mathbf{Q}(\zeta_{p^v})$ for some $v \geq 0$. Since $u_{\mathbf{Q}_p(\zeta_{p^v})/\mathbf{Q}_p}$ is equal to v, we must have $v = 1$.

(b) By class field theory the maximal abelian extension of $\mathbf{Q}(\zeta_p)$ inside F is contained in a ray class field K of conductor π^a for some $a \geq 0$. Here π denotes the prime $\zeta_p - 1$ over p. It splits completely in the Hilbert class field H. Let $\mathfrak{p}$ be a prime over π in K and let $K_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$. We have $u_{\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p} = 1$ and $i_{\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p} = \frac{1}{p-1}$. It follows from [11, Lemma 2.1] that $u_{K_{\mathfrak{p}}/\mathbf{Q}_p} = 1 + \max(0, \frac{a}{p-1} - \frac{1}{p-1})$. Since $K \subset F$, this is at most $1 + \frac{1}{p-1}$. Therefore we have $a \leq 2$. The proposition now follows from the following lemma. □

Lemma 2.2. *Let p be an odd prime and let π denote the prime above p in $\mathbf{Q}(\zeta_p)$. Then the ray class fields of conductor π and π^2 are equal to the Hilbert class field H of $\mathbf{Q}(\zeta_p)$.*

Proof. Let $a \in \mathbf{Z}$ be coprime to p. Then the cyclotomic unit $\eta_a = (\zeta_p^a - 1)/(\zeta_p - 1)$ is congruent to a modulo π. Class field theory therefore implies that the ray class field of conductor π is equal to the Hilbert class field H. To prove that the ray class field of conductor π^2 is also equal to H, we compute η_a^{p-1} modulo π^2. We find

$$\eta_a^{p-1} = \left(\frac{\zeta_p^a - 1}{\zeta_p - 1}\right)^{p-1} = \left(\frac{(1+\pi)^a - 1}{\pi}\right)^{p-1} \equiv 1 - \frac{a-1}{2}\pi \mod \pi^2.$$

Since we can take $a = 2$, the lemma follows. □

In the rest of this section we collect some numerical data regarding the primes $p = 23$, 29, 31 and 37. The root discriminants of the corresponding Abrashkin-Fontaine fields are too large for the unconditional Odlyzko bounds to apply. However, under the Generalized Riemann Hypothesis (GRH), Odlyzko obtained bounds that still apply. See [5, Tables 1 and 3]. Table 1 contains data that are used in the proofs in the final section.

p	h	$\delta_{\mathbf{Q}(\zeta_p)}$	$p^{1+\frac{1}{p-1}}$	$[H^{\mathrm{unr}}:\mathbf{Q}]$	$[H^{\mathrm{unr}}:H]$	$[H^{\mathrm{tame}}:\mathbf{Q}]$	$[H^{\mathrm{tame}}:H]$	$[F:\mathbf{Q}]$	$[F:H]$
23	3	19.94	26.52	120	1	220	3	600	9
29	8	25.71	32.71	400	1	1000	4	4800	21
31	9	27.64	34.76	720	2	1900	7	10000	37
37	37	33.46	40.93	5300	3	42700	32	5684000	4267

TABLE 1. Odlyzko bounds

We use the following notations:

- p is a prime between 23 and 37.
- h is the class number of the cyclotomic field $\mathbf{Q}(\zeta_p)$.
- $\delta_{\mathbf{Q}(\zeta_p)}$ is the root discriminant of $\mathbf{Q}(\zeta_p)$.
- the root discriminant bound $p^{1+\frac{1}{p-1}}$ of the Abrashkin-Fontaine field F.
- H is the Hilbert class field of $\mathbf{Q}(\zeta_p)$.
- H^{unr} is the maximal unramified extension of H; and the column $[H^{\mathrm{unr}}:\mathbf{Q}]$ (resp. $[H^{\mathrm{unr}}:H]$) gives an upper bound on the degree of H^{unr} (resp. relative degree of H^{unr} over H).
- H^{tame} is the maximal tamely ramified extension of H; and the column $[H^{\mathrm{tame}}:\mathbf{Q}]$ (resp. $[H^{\mathrm{tame}}:H]$) gives an upper bound on the degree of H^{tame} (resp. relative degree of H^{tame} over H).
- The column $[F:\mathbf{Q}]$ (resp. $[F:H]$) is an upper bound on the degree of F (resp. $[F:H]$).

We note that H^{unr} has the same root discriminant as H, and that H^{tame} has root discriminant at most p. All the bounds assume GRH, and were computed using Odlyzko's bounds from [5, Table 1]. Only for $p = 37$, the degrees are outside the range of this table and we computed the Odlyzko bounds using [5, Table 3]. For instance, the bound 5684000 was obtained by choosing $b = 15.000$ and $E = 70185$.

3. **A representation-theoretic result**

In this section we fix a prime p and let k denote an algebraic closure of $\mathbf{F}_p$. Our proof of the main result of this paper depends on a representation theoretic result. For a finite abelian group G and a character $\chi : G \to k^*$, we let $k(\chi)$ denote the 1-dimensional k-vector space on which G acts through χ. The χ-*twist* of a $k[G]$-module M is the module $M \otimes_k k(\chi)$.

Proposition 3.1. *Let A be a finite abelian group and let Δ be a finite abelian group of order prime to p acting linearly on A. Let Q denote the semidirect product $A \rtimes \Delta$. Let V be a finite irreducible $k[Q]$-module. Then, as a Δ-module, V is isomorphic to a twist of $k[\Delta/H]$ for some subgroup $H \subset \Delta$.*

Proof. Let V be a finite irreducible $k[Q]$-module and let the action of Q on V be given by $\varrho : Q \longrightarrow \mathrm{Aut}(V)$. Then the p-Sylow subgroup P of A acts trivially on V. Since P is normal in Q, we may replace Q by Q/P and assume that p does not divide $\#Q$. Since A is abelian, $\varrho|_A$ is a sum of characters. Let $\psi : A \to k^*$ be one of those characters and let Δ_ψ be the stabilizer of ψ inside Δ and $H_\psi = A \rtimes \Delta_\psi$. Then, by Clifford theory there exists a representation $\theta : H_\psi \to k^*$, which extends ψ, such that

$$\varrho = \mathrm{Ind}_{H_\psi}^{Q} \theta.$$

Indeed, the proof in [12, §8.2, Proposition 25] not only works when the characteristic of the coefficient field is zero, but also when it is prime to the order of Q. Since Δ_ψ is the stabilizer of ψ, its action on V commutes with that of A. In fact, since Δ is

abelian, the action of Δ_ψ on V commutes with that of Q. So, by Schur's Lemma, Δ_ψ acts on V via a character $\chi_0 : \Delta_\psi \to k^*$. We extend χ_0 to a character of Δ. Then Δ_ψ acts trivially on the twisted module $V \otimes k(\chi_0^{-1})$. Since each character χ of Δ/Δ_ψ occurs at most once in V and since $\dim V = [\Delta : \Delta_\psi]$, it follows that each χ occurs *exactly* once, so that, as a Δ-module, $V \otimes k(\chi_0^{-1})$ is isomorphic to $k[\Delta/\Delta_\psi]$. This proves the proposition. □

Theorem 3.2. *Let p be a prime and let G be a simple finite flat commutative group scheme over $\mathbf{Z}$ of p-power order. If the field generated by the points of G is contained in the Hilbert class field of $\mathbf{Q}(\zeta_p)$, then $G \cong \mathbf{Z}/p\mathbf{Z}$ or $G \cong \mu_p$.*

Proof. Let G be a simple finite flat commutative group scheme over $\mathbf{Z}$ of p-power order, with the property that the field K generated by the points of G is contained in the Hilbert class field H of $\mathbf{Q}(\zeta_p)$. It suffices to show that K is contained in $\mathbf{Q}(\zeta_p)$. Indeed, in that case the group of points $G(\overline{\mathbf{Q}})$ is an irreducible module over $\mathbf{F}_p[\Delta]$, where $\Delta = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Since Δ is cyclic of order $p-1$, the group $G(\overline{\mathbf{Q}})$ has order p. It is then a consequence of the Oort-Tate classification of group schemes of order p that $G \cong \mathbf{Z}/p\mathbf{Z}$ or $G \cong \mu_p$.

This argument takes care of the primes p for which H is equal to $\mathbf{Q}(\zeta_p)$, in other words the primes $p \leq 19$. The following argument works for the primes $p > 19$. Let Q be the Galois group of the Hilbert class field H over $\mathbf{Q}$. Put $A = \mathrm{Gal}(H/\mathbf{Q}(\zeta_p))$ and $\Delta = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^*$. Since the unique prime over p in $\mathbf{Q}(\zeta_p)$ is principal, it splits completely in H. Therefore, the decomposition group at each prime of H lying over p is isomorphic to Δ. It follows that Q is a semidirect product $A \rtimes \Delta$.

Let V be an irreducible constituent of the $k[Q]$-module $G(\overline{\mathbf{Q}}) \otimes k$. Then Proposition 3.1 implies that, as a Δ-module, V is a sum of characters on Δ, each of which appears with multiplicity at most *one*. But, by the Oort-Tate classification, only the trivial character 1 and the cyclotomic character ω can occur in V. It follows that the dimension of V is at most 2.

If $\dim V$ were 2, Proposition 3.1 would imply that ω is trivial on the unique index 2 subgroup of Δ, so that ω is quadratic. This is a contradiction since $p > 3$. Therefore we have $\dim V = 1$. Since k^* is abelian, Proposition 2.1 implies that the subgroup A acts trivially on V. It follows that A also acts trivially on $G(\overline{\mathbf{Q}}) \otimes k$ and hence on $G(\overline{\mathbf{Q}})$, as required.

□

4. End of proof

In this section we prove the following result. Together with Theorem 3.2 it implies Theorem 1.2.

Theorem 4.1 (GRH)**.** *Let $p = 23$, 29, 31 or 37. Then the Abrashkin-Fontaine field F is equal to the Hilbert class field H of $\mathbf{Q}(\zeta_p)$.*

Proof. We have inclusions

$$\mathbf{Q} \subset \mathbf{Q}(\zeta_p) \subset H \subset F.$$

Let $\Gamma = \mathrm{Gal}(F/\mathbf{Q})$. By Proposition 2.1 its commutator subgroup Γ' is $\mathrm{Gal}(F/\mathbf{Q}(\zeta_p))$ and the commutator subgroup Γ'' of Γ' is $\mathrm{Gal}(F/H)$. Below we show that for $p = 23$, 29, 31 and 37 the group Γ'' is trivial, or equivalently that Γ' is abelian. This implies that $F = H$. Since the details are different for each prime, we proceed case by case.

Case $p = 23$. From Table 1, we see that $[F : H] = \#\Gamma'' \leq 9$. This implies that F is tamely ramified at 23, so that Table 1 implies that $\#\Gamma'' \leq 3$. It follows that $\mathrm{Aut}(\Gamma'')$ is abelian. This implies that Γ' is in the kernel of the map $\Gamma \to \mathrm{Aut}(\Gamma'')$

given by conjugation. It follows that Γ'' is in the center of Γ'. Since Γ'/Γ'' is cyclic, we find that $\Gamma' = \mathrm{Gal}(F/\mathbf{Q}(\zeta_p))$ is abelian, as required.

Case $p = 29$**.** We have the following inclusions

$$\mathbf{Q} \underset{4}{\subset} \underbrace{K \underset{\Delta}{\subset} \mathbf{Q}(\zeta_{29}) \underset{V}{\subset} H}_{\Gamma_2} \underset{\Gamma''}{\subset} F.$$

Here $V = \mathrm{Gal}(H/\mathbf{Q}(\zeta_{29}))$ is a 3-dimensional $\mathbf{F}_2$-vector space on which the order 7 group $\Delta = \mathrm{Gal}(\mathbf{Q}(\zeta_{29})/K)$ acts non-trivially. See [9].

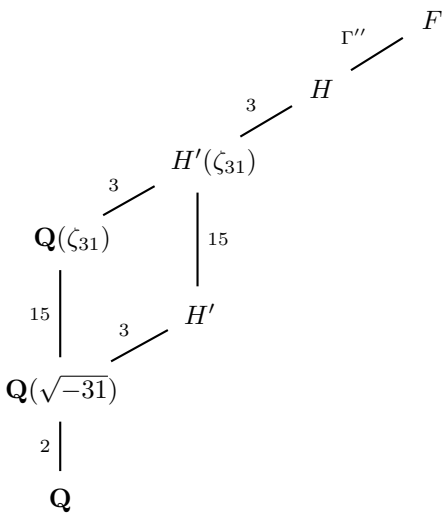
From Table 1, we see that $[F : H] = \#\Gamma'' \leq 21$. This implies that F is tamely ramified at 29, so that Table 1 implies that $\#\Gamma'' \leq 4$. So, Γ'' is either cyclic or isomorphic to Klein's four group. Since $[H : \mathbf{Q}] = 8 \cdot 28$ is not divisible by 3, it follows that the image of Γ in $\mathrm{Aut}(\Gamma'')$ has order at most 2. Therefore Γ' and hence its subgroup $\Gamma_2 = \mathrm{Gal}(H/K)$ act trivially on Γ''. We claim that the group extension

$$0 \longrightarrow \Gamma'' \longrightarrow \Gamma_1 \longrightarrow \Gamma_2 \longrightarrow 0$$

is split. It follows that K admits an extension E inside F with $\mathrm{Gal}(E/K) = \Gamma''$ of order at most 4. A short `pari`-computation [6] shows that the only such extension is K itself. This means that Γ'' is trivial and we are done.

It remains to show that the extension is split. Since $\#\Gamma_2 = 56$ is prime to 3, this is the case when $\#\Gamma'' = 3$. So, we may assume that Γ'' has order 1, 2 or 4. It suffices therefore to show that the cohomology group $H^2(\Gamma_2, \mathbf{Z}/2\mathbf{Z}) = 0$ vanishes. Since $H^2(\Gamma_2, \mathbf{Z}) = \mathrm{Hom}(\Gamma_2, \mathbf{Q}/\mathbf{Z})$ is trivial, our cohomology group is isomorphic to the 2-torsion of the Schur multiplier $H^3(\Gamma_2, \mathbf{Z})$. Since Δ and V have coprime order, the Hochschild-Serre spectral sequence degenerates and we find that $H^3(\Gamma_2, \mathbf{Z})$ is isomorphic to $H^3(V, \mathbf{Z})^\Delta$. The Schur multiplier of the abelian group V is $V \wedge V$ equipped with its natural Δ-action. In particular, the Δ-invariants are zero and we are done.

Case $p = 31$. From Table 1, we see that $[F : H] = \#\Gamma''$ is at most 37. If F is wildly ramified, the group Γ'' is cyclic of order 31 and its automorphism group is abelian. It follows that Γ' acts trivially on it. Since the class group of $\mathbf{Q}(\zeta_{31})$ is cyclic [9, Thm. III], this means that Γ' modulo its center is cyclic. It follows that Γ' is abelian and we are done.



If F is tamely ramified at 31, Table 1 implies that $[F : H] = \#\Gamma''$ is at most 7. It follows that $\mathrm{Aut}(\Gamma'')$ has order at most 6. If the image of $\Gamma \to \mathrm{Aut}(\Gamma'')$ is abelian, we find that Γ'' is contained in the center of Γ'. Since Γ'/Γ'' is cyclic, it follows that Γ' is abelian as required.

If the image of $\Gamma \to \mathrm{Aut}(\Gamma'')$ is not abelian, then Γ'' is isomorphic to V_4 or to S_3. Since S_3 is not the commutator subgroup of any group [10, Lemma 4.1], the group Γ'' must be isomorphic to Klein's group V_4. The group $\Gamma/\Gamma'' = \mathrm{Gal}(H/\mathbf{Q})$ has a unique quotient isomorphic to S_3. It is $\mathrm{Gal}(H'/\mathbf{Q})$, where H' is the Hilbert class field of $\mathbf{Q}(\sqrt{-31})$. It follows that the order 45 group $\mathrm{Gal}(H/H')$ acts trivially on Γ''.

This implies that H' admits an extension field E inside F for which $\mathrm{Gal}(E/H')$ is isomorphic to V_4. However, a short `pari` computation [6] shows that the ray class group of conductor $\sqrt{-31}$ of H' has odd order. Therefore this cannot occur.

Case $p = 37$. In Table 1, we find that $[F : H] \leq 4270$. Suppose that $F \neq H$. Then there a surjective homomorphism $\mathrm{Gal}(F/H) \to \Gamma_0$, where Γ_0 is a simple group. Let $H \subset L \subset F$ be the fixed field of its kernel, so that $\Gamma_0 = \mathrm{Gal}(L/H)$.

If the order of Γ_0 is divisible by 37, then Sylow theory implies that Γ_0 is either cyclic of order 37 or it is a non-commutative simple group of order $37(1 + 37k)$ for some $k \geq 1$. Since $\#\Gamma_0 \leq 4270$ this implies that $\#\Gamma_0 = 1406$, 2775 or 4144. We leave the exercise to show that groups of these orders cannot be simple to the reader. It follows that either Γ_0 is cyclic of order 37, or $\#\Gamma_0$ is prime to 37.

If Γ_0 is cyclic of order 37, we consider the maximal Galois extension $\mathbf{Q}(\zeta_{37}) \subset E$ inside F for which $P = \mathrm{Gal}(E/\mathbf{Q}(\zeta_{37}))$ is a 37-group. Then E contains the Hilbert class field H. The maximal Galois extension $H \subset E'$ inside F for which $\mathrm{Gal}(E'/H)$ is a 37-group, is Galois over $\mathbf{Q}(\zeta_{37})$. Therefore we have $E = E'$. It follows that E contains L. We have inclusions

$$\mathbf{Q} \subset \underbrace{\mathbf{Q}(\zeta_{37}) \subset H \subset L \subset E}_{P} \subset F.$$

By Proposition 2.1, the maximal *abelian* extension of $\mathbf{Q}(\zeta_{37})$ inside F is the Hilbert class field H. This means that $P/[P, P]$ is cyclic of order 37. By Burnside, P is also cyclic, and hence has order 37. It follows that $E = L = H$. Contradiction.

So $\#\Gamma_0 = [L : H]$ is prime to 37 and hence the extension $H \subset L$ is at most tamely ramified at the primes lying over 37. From Table 1, we see that $[L : H] \leq 32$. It follows that Γ_0 is cyclic of prime order $q \leq 31$.

Consider the maximal abelian exponent q-extension E'' of H inside F. Then we have

$$\mathbf{Q} \subset \mathbf{Q}(\zeta_{37}) \subset H \subset L \subset E'' \subset F.$$

and E'' is Galois over $\mathbf{Q}$. The degree $[E'' : H]$ is at most 32. The orders of the groups $\mathrm{GL}_d(\mathbf{F}_q)$ are not divisible by 37 when $q^d \leq 32$. It follows that conjugation by the cyclic order 37 group $\mathrm{Gal}(H/\mathbf{Q}(\zeta_{37}))$ is trivial on $\mathrm{Gal}(E''/H)$. This means that $\mathrm{Gal}(E''/H)$ is in the center of $\mathrm{Gal}(E''/\mathbf{Q}(\zeta_{37}))$. Since $\mathrm{Gal}(H/\mathbf{Q}(\zeta_{37}))$ is cyclic, the group $\mathrm{Gal}(E''/\mathbf{Q}(\zeta_{37}))$ is abelian. However, by Proposition 2.1 the field H is the maximal abelian extension of $\mathbf{Q}(\zeta_{37})$ inside F. Contradiction. So $F = H$ after all.

□

References

[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] Dembélé, L. and Schoof, R.: Finite flat group schemes over **Z** killed by 19, Journal of Number Theory, **260** (2024), 191–195.

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

[4] Khare, C.: Serre's modularity conjecture: The level one case, *Duke Mathematical Journal*, **134**, (2006) 557–589.
[5] Odlyzko, A.: Discriminant bounds, November 29, 1976. `http://www.dtc.umn.edu/∼odlyzko/unpublished/index.html`
[6] The PARI/GP computer algebra system, `https://pari.math.u-bordeaux.fr`
[7] Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$, Bull. Soc. Math. France, **102**, (1974) 241–280.
[8] Schoof, R.: Infinite class field towers of quadratic fields, *J. für die reine und angewandte Mathematik* **372**, (1986) 209–220.
[9] Schoof, R.: Minus class groups of cyclotomic fields of prime conductor, *Math. Comp.* **67**, (1998) 1225–1245.
[10] Schoof, R.: Semistable abelian varieties with good reduction outside 15, *Manuscripta Mathematica*, **139** (2012), 49–70.
[11] Schoof, R.: Abelian varieties over real quadratic fields with good reduction everywhere, in preparation.
[12] Serre, J.-P.: *Linear representations of finite groups*. Translated from the second French edition by Leonard L. Scott GTM, Vol. **42** Springer-Verlag, New York-Heidelberg, 1977. x+170 pp.
[13] Tate, J.T.: p-Divisible groups. Proc. of a Conference on Local Fields, Driebergen, Springer 1967.
[14] Tate, J.T. and Oort, F.: Group schemes of prime order, *Ann. Scient. École Norm. Sup.* **3** (1970), 1–21.
[15] Washington, L.C.: *Introduction to cyclotomic fields*, 2nd Ed, GTM **83**, Springer-Verlag 1997.

Department of Mathematics, King's College London, Strand, London WC2R 2LS, UK
E-mail address: `lassina.dembele@kcl.ac.uk`

Dipartimento di Matematica, 2^{A} Università di Roma, "Tor Vergata", I-00133 Roma ITALY
E-mail address: `schoof@mat.uniroma2.it`