Algebra & Number Theory

Volume 12
2018
No. 5

Certain abelian varieties bad at only one prime

Armand Brumer and Kenneth Kramer

msp

ALGEBRA AND NUMBER THEORY 12:5 (2018)
dx.doi.org/10.2140/ant.2018.12.1027

Certain abelian varieties bad at only one prime

Armand Brumer and Kenneth Kramer

An abelian surface $A_{/\mathbb{Q}}$ of prime conductor N is *favorable* if its 2-division field F is an $\mathcal{S}_5$-extension over $\mathbb{Q}$ with ramification index 5 over $\mathbb{Q}_2$. Let A be favorable and let B be a semistable abelian variety of dimension $2d$ and conductor N^d with $B[2]$ filtered by copies of $A[2]$. We give a sufficient class field theoretic criterion on F to guarantee that B is isogenous to A^d.

As expected from our paramodular conjecture, we conclude that there is one isogeny class of abelian surfaces for each conductor in {277, 349, 461, 797, 971}. The general applicability of our criterion is discussed in the data section.

1. Introduction

Let $\mathfrak{I}_d(S)$ be the set of isogeny classes of simple abelian varieties over $\mathbb{Q}$ of dimension d with good reduction outside S, a finite set of primes. By [Faltings 1983], $\mathfrak{I}_d(S)$ is finite and it is empty when S is, by [Abrashkin 1987; Fontaine 1985]. All curves of genus 2 with good reduction outside 2 are found in [Merriman and Smart 1993; Smart 1997], yielding 165 isogeny classes of Jacobians. Factors of $J_0(2^{10})$ and Weil restrictions of elliptic curves over quadratic fields provide an additional 50 members of $\mathfrak{I}_2(\{2\})$, but the complete determination of $\mathfrak{I}_2(\{2\})$ is still open.

Research of the second author was partially supported by a PSC-CUNY Award, cycle 44, jointly funded by The Professional Staff Congress and The City University of New York.
MSC2010: primary 11G10; secondary 11R37, 11S31, 14K15.
Keywords: semistable abelian variety, group scheme, Honda system, conductor, paramodular conjecture.

For *semistable* abelian varieties, Fontaine's nonexistence result has been slightly extended [Brumer and Kramer 2001; 2004; 2014; Calegari 2004; Schoof 2005]. It is much more challenging to find all isogeny classes when some exist.

In a beautiful sequence of papers Schoof [2005; 2012b; 2012a] shows that for $S = \{N\}$ with prime $N \leq 23$ or $S = \{3, 5\}$ the classical modular variety $J_0(N)$ or $J_0(15)$, respectively, is the only simple semistable abelian variety of arbitrary dimension, up to isogeny. To apply Faltings' isogeny theorem on abelian varieties, Schoof introduces a general result on p-divisible groups whose constituents belong to a category $\underline{C}$ of finite flat group schemes. For the reader's convenience, the statement is included here as Theorem 3.3. For a suitable choice of category $\underline{D}$, depending on S, Schoof determines all simple objects and their extensions by one another. Because the Odlyzko bounds are used, the sets S to which these methods apply are severely limited.

In fact, given a finite set S of primes, it seems challenging to decide whether the dimension of the simple semistable abelian varieties good outside S is bounded.

This paper grew out of the desire to check the uniqueness of certain isogeny classes for larger conductors. Another motivation was to provide additional evidence for our conjecture. (See modification added in proof, page 1069.)

Paramodular conjecture [Brumer and Kramer 2014]. *Let $K(N)$ be the paramodular group of level N. There is a one-to-one correspondence*

isogeny classes of abelian surfaces $A_{/\mathbb{Q}}$ of conductor N with $\mathrm{End}_{\mathbb{Q}} A = \mathbb{Z}$	$\longleftrightarrow$	*weight 2 nonlifts f on $K(N)$, with rational eigenvalues, up to scalar multiplication*

in which the ℓ-adic representation of $\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell$ and that associated to f are isomorphic for any ℓ prime to N, so that the L-series of A and f agree.

The L-series of abelian surfaces of GL_2-type are understood via classical elliptic modular forms, while our conjecture treats all other abelian surfaces. It is verified in [Berger et al. 2015; Johnson-Leung and Roberts 2012] for the Weil restrictions of modular elliptic curves over quadratic fields, not isogenous to their conjugates. It is also compatible with twists [Johnson-Leung and Roberts 2017].

To ensure that we are not in the endoscopic case, we consider prime conductors. By [Brumer and Kramer 2014, Theorem 3.4.11], an abelian surface of prime conductor is isogenous to a Jacobian. For each N in $\{277, 349, 461, 797, 971\}$, the space of weight 2 nonlift paramodular forms on $K(N)$ is one-dimensional [Poor and Yuen 2015], so our conjecture predicts that there should be exactly one isogeny class of abelian surfaces of conductor N. In [Brumer and Kramer 2014], we proved that 277 is the smallest prime conductor. For each N listed above, there is a unique Galois module structure available for $A[2]$. For those N, $\mathbb{Q}(A[2])$ must be the Galois closure of a *favorable* quintic field as defined below.

Definition 1.1. Let N be an odd prime. A quintic extension $F_0/\mathbb{Q}$ of discriminant $\pm 16N$ is *favorable* if the prime over 2 has ramification index 5. A *favorable polynomial* is any minimal polynomial for a favorable quintic field. An abelian surface A of prime conductor N is *favorable* its 2-division field $\mathbb{Q}(A[2])$ is the Galois closure of a favorable quintic field.

We note some pleasant properties of favorable quintic fields.

Proposition 1.2. *Let F be the Galois closure of a favorable quintic field F_0 of discriminant $d_0 = 16N^*$ with $N^* = \pm N$. Then*:

(i) $\mathrm{Gal}(F/\mathbb{Q})$ *is isomorphic to the symmetric group $\mathcal{S}_5$. At each prime $\mathfrak{N} \mid N$, the inertia group $\mathcal{I}_{\mathfrak{N}} = \mathcal{I}_{\mathfrak{N}}(F/\mathbb{Q})$ is generated by a transposition.*

(ii) *The completion $F_{\mathfrak{P}}$ of F at each prime $\mathfrak{P} \mid 2$ is isomorphic to $\mathbb{Q}_2(\boldsymbol{\mu}_5, \sqrt[5]{2})$ and the decomposition group $\mathcal{D}_{\mathfrak{P}} = \mathcal{D}_{\mathfrak{P}}(F/\mathbb{Q})$ is the Frobenius group of order 20. The sign of N^* is determined by $N^* \equiv 5(8)$.*

(iii) *There is only one prime over 2 in the subfield K_{20} of F fixed by* $\mathrm{Sym}\{3, 4, 5\}$.

(iv) *If A is a favorable abelian surface, then the finite flat group scheme $A[2]_{|\mathbb{Z}_2}$ is absolutely irreducible and biconnected over $\mathbb{Z}_2$.*

Proof. (i) Since N exactly divides d_0, only one prime say $\mathfrak{N}_0$ over N ramifies in $F_0/\mathbb{Q}$ and the $\mathcal{O}_{F_0}$-ideal generated by N factors as $(N) = \mathfrak{N}_0^e \mathfrak{a}$, where $\mathfrak{a}$ is an ideal prime to $\mathfrak{N}_0$ and $e > 1$. If f is the residue degree of $\mathfrak{N}_0$ then $N^{(e-1)f}$ divides d_0, so $e = 2$, $f = 1$ and the other primes over N are unramified in $F_0/\mathbb{Q}$. Thus the completion $F_{\mathfrak{N}}$ is $\mathbb{Q}_N(\sqrt{d_0})$ and $\mathcal{I}_{\mathfrak{N}}$ has order 2. Since $\mathcal{I}_{\mathfrak{N}}$ acts nontrivially on $\sqrt{d_0}$, it is generated by a transposition. A transposition and a 5-cycle generate $\mathcal{S}_5$.

(ii) By assumption, $F_{\mathfrak{P}}/\mathbb{Q}_2$ has tame ramification of degree 5 and thus contains $\mathbb{Q}_2(\boldsymbol{\mu}_5, \sqrt[5]{2})$. Since $\mathcal{D}_{\mathfrak{P}}$ is solvable, $F_{\mathfrak{P}} = \mathbb{Q}_2(\boldsymbol{\mu}_5, \sqrt[5]{2})$. Any Frobenius automorphism at $\mathfrak{P}$ is a 4-cycle, so it acts nontrivially on $\sqrt{d_0}$ and therefore $N^* \equiv 5 \bmod 8$.

(iii) There are no transpositions in $\mathcal{D}_{\mathfrak{P}}$, so $D_{\mathfrak{P}} \cap \mathrm{Sym}\{3, 4, 5\}$ is trivial. Since $[K_{20} : \mathbb{Q}] = 20$, there is only one prime over 2 in K_{20}.

(iv) Since $\mathcal{D}_{\mathfrak{P}}$ acts on $A[2]$ via its unique 4-dimensional absolutely irreducible $\mathbb{F}_2$-representation, $A[2]_{|\mathbb{Z}_2}$ has no étale or multiplicative constituents. □

A *favorable* $\mathcal{S}_5$-field is the Galois closure of a favorable quintic field. The Jacobian of a genus 2 curve C is favorable only if C has a model $y^2 = f(x)$ with f favorable, but C might have bad reduction outside N.

In general, L is a *stem field* for M if M is the Galois closure of $L/\mathbb{Q}$. A *pair-resolvent* for an $\mathcal{S}_5$-field F is a subfield K fixed by the centralizer of a transposition in $\mathcal{S}_5$. Then K is well-defined up to isomorphism and is a stem field for F. If r_1 and r_2 are distinct roots of a quintic polynomial f with splitting field F, we can take $K = \mathbb{Q}(r_1 + r_2)$, the fixed field of $\mathrm{Sym}\{1, 2\} \times \mathrm{Sym}\{3, 4, 5\}$. There is only one prime $\mathfrak{p}$ over 2 in K by Proposition 1.2(iii). Let $\Omega_K^{(a)}$ be the maximal elementary 2-extension of K of modulus $\mathfrak{p}^a \cdot \infty$, i.e., the compositum of all quadratic extensions of K with that modulus. Write rk_a for the rank of $\mathrm{Gal}(\Omega_K^{(a)}/K)$.

The following is a restatement of Theorem 6.1.22.

Theorem 1.3. *Let A be a favorable abelian surface of conductor N and let K be a pair-resolvent field for $F = \mathbb{Q}(A[2])$. Suppose that B is a semistable abelian variety of dimension $2d$ and conductor N^d, with $B[2]$ filtered by copies of $A[2]$. If $\mathrm{rk}_2 = 0$ and $\mathrm{rk}_4 \le 1$, then B is isogenous to A^d. If B is a surface, it is isogenous to A.*

For the proof, we first construct suitable categories $\underline{E}$, chosen so that extensions of the simple objects $\mathcal{E}$ in $\underline{E}$ can be identified. Most of the paper is devoted to the study of such extension classes. A description of the extensions of $\mathcal{E}$ by $\mathcal{E}$ as group schemes over $\mathbb{Z}_p$ is obtained via Honda systems. For global applications, assume that $p = 2$ and $\mathbb{Q}(\mathcal{E})$ is a favorable $\mathcal{S}_5$-field. Monodromy at N restricts the extensions $\mathcal{W}$ of $\mathcal{E}$ by $\mathcal{E}$ as group schemes over $\mathbb{Z}\big[\frac{1}{2N}\big]$. A comparison with local data determines when $\mathcal{W}$ prolongs to a group scheme over $\mathbb{Z}\big[\frac{1}{N}\big]$ and leads to our class field theoretic criterion for the control of $\mathrm{Ext}^1_{\underline{E}}(\mathcal{E}, \mathcal{E})$ required by Schoof's theorem. Ray class field information, difficult to reach over F, becomes accessible over the degree 10 field K. Moreover, we found that Theorem 1.3 and Proposition 6.1.13 have no analog for other intermediate fields of $F/\mathbb{Q}$. A more detailed overview of our paper follows.

The category $\underline{E}$ of finite flat p-group schemes over $\mathbb{Z}\big[\frac{1}{N}\big]$ defined in §3 is motivated by necessary conditions for an abelian variety B to be isogenous to a product of given semistable abelian varieties A_i. It is essential to impose conductor bounds at N, without which Theorem 3.3 does not apply, as indicated in Example B.4. Thanks to Proposition A.2, we deduce in Theorem 3.7 that it suffices to study the subgroup $\mathrm{Ext}^1_{[p],\underline{E}}(\mathcal{E}, \mathcal{E})$ consisting of classes of extensions $\mathcal{W}$ of $\mathcal{E}$ by $\mathcal{E}$ such that $p\mathcal{W} = 0$.

We review group schemes and Honda systems over the ring of Witt vectors $\mathbb{W}$ of a finite field k of characteristic p in Section 2. In Section 4, finite Honda systems are used to classify absolutely simple biconnected finite flat group schemes $\mathcal{E}$ of rank p^4 over $\mathbb{W}$ and describe the classes $[\mathcal{W}]$ in $\mathrm{Ext}^1_{[p],\mathbb{Z}_p}(\mathcal{E}, \mathcal{E})$. We give the structure of the associated Galois modules E and W in Section 5 and obtain a conductor bound for the elementary abelian extension $K(W)/K(E)$ in Proposition 5.2.17. The latter improves on Fontaine's bound in our case, see Remark 5.2.19.

In Section 6, we restrict to $p = 2$ and give a class field theoretic condition equivalent to the vanishing of $\mathrm{Ext}^1_{[2],\underline{E}}(\mathcal{E}, \mathcal{E})$ in Proposition 6.1.21. Its proof exploits the following ingredients: (i) monodromy at N, to determine the matrix groups available for $\mathrm{Gal}(\mathbb{Q}(W)/\mathbb{Q})$ as W runs over the extensions of E by E as Galois modules, (ii) conductor bounds at $p = 2$, as described above and (iii) rigidification in Section 5.3 and (6.1.5) of the cocycles corresponding to local and global extensions of E by E, to check whether they are compatible, as needed for patching.

Appendix C contains several general facts required for the determination of abelian conductor exponents in our applications.

In Appendix D, we apply Theorem 1.3 to all the favorable quintic fields with N at most 25000 to obtain Table 1. In particular, there is a unique isogeny class of abelian surfaces for each conductor N in $\{277, 349, 461, 797, 971\}$. Curious about the wider applicability of our criterion, we studied the fields corresponding to 276109 favorable abelian surfaces of prime conductor at most 10^{10} found by an ad-hoc search. We were surprised to discover that the uniqueness, up to isogeny, in Theorem 1.3 holds uniformly for about 11.8% of those fields. The data is summarized in Table 3.

In our companion paper [Brumer and Kramer 2018], extensions $\mathcal{W}$ of exponent p^2 are studied and new "full image" results for certain subgroups of $\mathrm{GSp}_{2g}(\mathbb{Z}_2)$ generated by transvections are obtained. As a consequence, if A is a favorable abelian surface, then $\mathbb{Q}(A[4])$ is an elementary 2-extension of rank 11 over $\mathbb{Q}(A[2])$ with carefully controlled ramification. In Table 1, we also indicate the fields for which no favorable abelian surface can exist because there is no candidate for its 4-division field.

Write $\overline{K}$ for the algebraic closure of K and $G_K = \mathrm{Gal}(\overline{K}/K)$. For any local or global field K, let $\mathcal{O}_K$ be its ring of integers. If L/K is a Galois extension of number fields, let $\mathcal{D}_v(L/K)$ and $\mathcal{I}_v(L/K)$ be the decomposition and inertia subgroups of $\mathrm{Gal}(L/K)$ at a place v of L. We also use v for its restriction to each subfield of L. When the local extension L_v/K_v is abelian, $\mathfrak{f}_v(L/K)$ denotes the abelian conductor exponent of L_v/K_v. Write $\mathfrak{f}_v(V)$ for the Artin conductor exponent of a finite $\mathbb{Z}_p[\mathcal{D}_v]$-module V.

2. Some review of group schemes

Let R be a Dedekind domain with quotient field K. Calligraphic letters are used for finite flat group schemes $\mathcal{V}$ over R and the corresponding Roman letter for the Galois module $V = \mathcal{V}(\overline{K})$. The order of $\mathcal{V}$ is the rank over R of its affine algebra, or equivalently the order of the finite abelian group $V = \mathcal{V}(\overline{K})$.

By the following result of Raynaud [1974], group schemes occurring as subquotients of known group schemes can be treated via their associated Galois modules. Thus, the generic fiber functor induces an isomorphism between the lattice of finite flat closed R-subgroup schemes of $\mathcal{V}$ and that of finite flat closed K-subgroup schemes of $\mathcal{V}_{|K}$, where K is the field of fractions of R. The following results will be used without explicit reference.

Lemma 2.1. *Let R be a Dedekind domain with quotient field K and let $\mathcal{V}$ be a finite flat group scheme over R with generic fiber $V = \mathcal{V}_{|K}$. If $W = V_2/V_1$ is a subquotient of V, for closed immersions of finite flat K-group schemes $V_1 \hookrightarrow V_2 \hookrightarrow V$, there are unique closed immersions of finite flat R-group schemes $\mathcal{V}_1 \hookrightarrow \mathcal{V}_2 \hookrightarrow \mathcal{V}$, such that $V_i = \mathcal{V}_{i|K}$, and there is a unique isomorphism $\mathcal{V}_2/\mathcal{V}_1 \simeq \mathcal{W}$ compatible with $(\mathcal{V}_2/\mathcal{V}_1)_{|K} \simeq W$.*

Let p be a prime not dividing N, $R = \mathbb{Z}\big[\frac{1}{N}\big]$, $R' = \mathbb{Z}\big[\frac{1}{pN}\big]$ and let $\underline{\mathrm{Gr}}$ be the category of p-primary finite flat group schemes over R. Let $\underline{C}$ be the category of triples $(\mathcal{V}_1, \mathcal{V}_2, \theta)$ where $\mathcal{V}_1$ is a finite flat $\mathbb{Z}_p$-group scheme, $\mathcal{V}_2$ a finite flat R'-group scheme and $\theta : \mathcal{V}_1 \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \to \mathcal{V}_2 \otimes_{R'} \mathbb{Q}_p$ an isomorphism of $\mathbb{Q}_p$-group schemes. Then Proposition 2.3 of [Schoof 2003] asserts that the functor $\underline{\mathrm{Gr}} \to \underline{C}$ taking the R-group scheme $\mathcal{V}$ to $(\mathcal{V} \otimes_R \mathbb{Z}_p, \mathcal{V} \otimes_R R', \mathrm{id} \otimes_R \mathbb{Q}_p)$ is an equivalence of categories. We can identify $\mathcal{V} \otimes_R R'$ with the Galois module V, since $\mathcal{V}$ is étale over R'. For objects $\mathcal{V}_1$ and $\mathcal{V}_2$ of $\underline{\mathrm{Gr}}$, the Mayer–Vietoris sequence of [Schoof 2003, Corollary 2.4] specializes to:

$$
\begin{array}{l}
\mathrm{Hom}_{\mathbb{Q}_p}(V_1, V_2) \leftarrow \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{V}_1, \mathcal{V}_2) \times \mathrm{Hom}_{R'}(\mathcal{V}_1, \mathcal{V}_2) \leftarrow \mathrm{Hom}_R(\mathcal{V}_1, \mathcal{V}_2) \leftarrow 0 \\
\delta \downarrow \\
\mathrm{Ext}^1_R(\mathcal{V}_1, \mathcal{V}_2) \to \mathrm{Ext}^1_{\mathbb{Z}_p}(\mathcal{V}_1, \mathcal{V}_2) \times \mathrm{Ext}^1_{R'}(\mathcal{V}_1, \mathcal{V}_2) \to \mathrm{Ext}^1_{\mathbb{Q}_p}(V_1, V_2).
\end{array}
\tag{2.2}
$$

Corollary 2.3. *Let $\mathcal{V}_1$ and $\mathcal{V}_2$ be finite flat group schemes over $R = \mathbb{Z}[\frac{1}{N}]$ with $\mathcal{V}_1$ and $\mathcal{V}_2$ biconnected over $\mathbb{Z}_p$. The following natural maps are isomorphisms*:

$$\mathrm{Hom}_R(\mathcal{V}_1, \mathcal{V}_2) \to \mathrm{Hom}_{\mathrm{Gal}}(V_1, V_2) \quad \textit{and} \quad \mathrm{Ext}^1_R(\mathcal{V}_1, \mathcal{V}_2) \to \mathrm{Ext}^1_{\mathrm{Gal}}(V_1, V_2).$$

If $\mathcal{V}$ is a group scheme over R and $V_{|\mathbb{Q}_p}$ is absolutely irreducible, *then*

$$\mathrm{End}_{\mathbb{Q}_p}(\mathcal{V}) = \mathrm{End}_{R'}(\mathcal{V}) = \mathbb{F}_p, \quad \textit{and} \quad \mathrm{End}_R(\mathcal{V}) = \mathbb{F}_p.$$

In addition, $\delta = 0$ *in* (2.2) *with* $\mathcal{V}_1 = \mathcal{V}_2 = \mathcal{V}$.

Proof. The first claim follows from (2.2) and a theorem of Fontaine quoted in [Mazur 1977, Theorem 1.4]. For the second, use Schur's lemma and a diagram chase. □

We next review some basic material on Honda systems found in [Brinon and Conrad 2009; Conrad 1999; Fontaine 1977]. Let p be a prime, k a perfect field of characteristic $p > 0$, $\mathbb{W} = \mathbb{W}(k)$ the Witt vectors and K its field of fractions. Let $\sigma : \mathbb{W} \to \mathbb{W}$ be the Frobenius automorphism characterized by $\sigma(x) \equiv x^p \pmod{p}$ for x in $\mathbb{W}$. The Dieudonné ring $D_k = \mathbb{W}[\mathrm{F}, \mathrm{V}]$ is generated by the Frobenius operator F and Verschiebung operator V. We have $\mathrm{FV} = \mathrm{VF} = p$, $\mathrm{F}a = \sigma(a)\mathrm{F}$ and $\mathrm{V}a = \sigma^{-1}(a)\mathrm{V}$ for all a in $\mathbb{W}$.

A *Honda system* over $\mathbb{W}$ is a pair (M, L) consisting of a finitely generated free $\mathbb{W}$-module M, a $\mathbb{W}$-submodule L and a Frobenius semilinear injective endomorphism $\mathrm{F} : \mathrm{M} \to \mathrm{M}$ with $p\mathrm{M} \subseteq \mathrm{F}(\mathrm{M})$ and the induced map $\mathrm{L}/p\mathrm{L} \to \mathrm{M}/\mathrm{FM}$ an isomorphism. If F is topologically nilpotent, then (M, L) is *connected*. Since M is torsion free, M becomes a D_k-module with $\mathrm{V} = p\mathrm{F}^{-1}$.

A *finite Honda system* over $\mathbb{W}$ is a pair (M, L) consisting of a left D_k-module M of finite $\mathbb{W}$-length and a $\mathbb{W}$-submodule L with $\mathrm{V} : \mathrm{L} \to \mathrm{M}$ injective and the induced map $\mathrm{L}/p\mathrm{L} \to \mathrm{M}/\mathrm{FM}$ an isomorphism. If F is nilpotent on M, then (M, L) is *connected*. Morphisms are defined in the obvious manner. If (M, L) is a Honda system then $(\mathrm{M}/p^n\mathrm{M}, \mathrm{L}/p^n\mathrm{L})$ is a finite Honda system.

Honda systems owe their importance to the following fundamental result.

Theorem 2.4 [Fontaine 1975a;1975b]. *Let k be a perfect field of characteristic $p > 0$.*

(i) *If $p > 2$, there is a natural antiequivalence of categories $G \rightsquigarrow (\mathbf{D}(G_k), \mathbf{L}(G))$ from the category of p-divisible groups over $\mathbb{W}$ to that of Honda systems ($\mathbf{D}(G_k)$ is the Dieudonné module of G_k). The same holds for $p = 2$ if we restrict to connected objects on both sides.*

(ii) *If $p > 2$, there is a natural antiequivalence of categories from the category of finite flat p-primary group schemes over $\mathbb{W}$ to that of finite Honda systems and the same holds for $p = 2$ if we restrict to connected objects on both sides.*

(iii) *The cotangent space of G_k at the origin is $\mathbf{D}(G_k)/\mathrm{F}\mathbf{D}(G_k)$.*

(iv) *Both antiequivalences respect extensions of k. Moreover*, *if G is a p-divisible group over $\mathbb{W}$*, *then $(\mathbf{D}(G_k)/(p^n), \mathbf{L}(G)/(p^n))$ is naturally identified with the finite Honda system associated with $G[p^n]$ for all $n \geq 1$.*

Lemma 2.5. *Let* (M, L) *be a Honda system of exponent* p. *Then* $\mathrm{M} = \mathrm{L} + \mathrm{FM}$ *is a direct sum*, $\ker \mathrm{F} = \mathrm{VL} = \mathrm{VM}$, $\dim \ker \mathrm{F} = \dim \mathrm{L}$ *and* $\ker \mathrm{V} = \mathrm{FM}$.

Proof. Since $\mathrm{L}/p\mathrm{L} \to \mathrm{M}/\mathrm{FM}$ is an isomorphism, $\mathrm{M} = \mathrm{L} + \mathrm{FM}$ is a direct sum and

$$\dim \mathrm{M} = \dim \mathrm{FM} + \dim \mathrm{L} = \dim \mathrm{M} - \dim \ker \mathrm{F} + \dim \mathrm{L}.$$

Hence $\dim \ker \mathrm{F} = \dim \mathrm{L}$ and equality holds for each inclusion in $\mathrm{VL} \subseteq \mathrm{VM} \subseteq \ker \mathrm{F}$ because $\mathrm{V}_{|\mathrm{L}}$ is injective. In addition,

$$\dim \mathrm{L} = \dim \mathrm{VL} = \dim \mathrm{VM} = \dim \mathrm{M} - \dim \ker \mathrm{V},$$

so $\mathrm{M} = \mathrm{L} + \ker \mathrm{V}$ is a direct sum and the inclusion $\mathrm{FM} \subseteq \ker \mathrm{V}$ is an equality. □

Let $\widehat{\mathrm{CW}}_k$ denote the formal k-group scheme associated to the *Witt covector* group functor CW_k, see [Conrad 1999; Fontaine 1977]. When k' is a finite extension of k and K' is the field of fractions of $W(k')$, we have $\mathrm{CW}_k(k') \simeq K'/W(k')$. For any k-algebra R and $\mathbb{W} = W(k)$, let $D_k = \mathbb{W}[\mathrm{F}, \mathrm{V}]$ act on elements $\mathbf{a} = (\dots, a_{-n}, \dots, a_{-1}, a_0)$ of $\mathrm{CW}_k(R)$ by $\mathrm{F}\mathbf{a} = (\dots, a_{-n}^p, \dots, a_{-1}^p, a_0^p)$, $\mathrm{V}\mathbf{a} = (\dots, a_{-(n+1)}, \dots, a_{-2}, a_{-1})$ and $\dot{c}\mathbf{a} = (\dots, c^{p^{-n}} a_{-n}, \dots, c^{p^{-1}} a_{-1}, c a_0)$, where $\dot{c}$ in $\mathbb{W}$ is the Teichmüller lift of c. Note that such lifts generate $\mathbb{W}$ as a topological ring.

The Hasse–Witt exponential map is a homomorphism of additive groups,

$$\xi : \widehat{CW}_k(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}) \to \overline{K}/p\mathcal{O}_{\overline{K}} \quad \text{by} \quad (\dots, a_{-n}, \dots, a_{-1}, a_0) \mapsto \sum p^{-n} \tilde{a}_{-n}^{p^n},$$

independent of the choice of lifts $\tilde{a}_{-n}$ in $\mathcal{O}_{\overline{K}}$. If $\mathcal{U}$ is the group scheme of a Honda system (M, L), the points of the Galois module U correspond to D_k-homomorphisms $\varphi : \mathrm{M} \to \widehat{CW}_k(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})$ such that $\xi(\varphi(\mathrm{L})) = 0$ and we say that φ *belongs to* $\mathcal{U}$. The action of G_K on $U(\overline{K})$ is induced from its action on $\widehat{CW}_k(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})$.

We write $\dot{+}$ for the usual Witt covector addition [Conrad 1999, p. 242] and state some related elementary facts. For q a power of p and x, y in $\overline{K}$, the congruence $\Phi_q(x, y) \equiv ((\tilde{x} + \tilde{y})^q - \tilde{x}^q - \tilde{y}^q)/q \pmod{p\mathcal{O}_{\overline{K}}}$ defines a unique, possibly nonintegral element of $\overline{K}/p\mathcal{O}_{\overline{K}}$, independent of the choices of lifts $\tilde{x}$ and $\tilde{y}$ in $\mathcal{O}_{\overline{K}}$. The binomial theorem yields the following estimate.

Lemma 2.6. $$\mathrm{ord}_p((\tilde{x} + \tilde{y})^q - \tilde{x}^q - \tilde{y}^q) \geq 1 + q \min\{\mathrm{ord}_p(\tilde{x}), \mathrm{ord}_p(\tilde{y})\}.$$

It is convenient to write $(\vec{0}, x_{-n}, \dots, x_0)$ for the element $(\dots, 0, 0, x_{-n}, \dots, x_0)$ in $\widehat{CW}_k(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})$. A routine calculation using the formulas in [Abrashkin 1987; Conrad 1999] gives:

Lemma 2.7. *Addition in* $\widehat{CW}_k(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})$ *specializes to*

$$(\vec{0}, u_4, u_3, u_2, u_1, u_0) \dot{+} (\vec{0}, v_2, v_1, v_0) = (\vec{0}, u_4, u_3, u_2 + v_2, w_1, w_0),$$

where $w_1 = u_1 + v_1 - \Phi_p(u_2, v_2)$ *and*

$$w_0 = u_0 + v_0 + \tfrac{1}{p}(u_1^p + v_1^p) - \Phi_{p^2}(u_2, v_2) - \tfrac{1}{p}(u_1 + v_1 - \Phi_p(u_2, v_2))^p.$$

3. The new categories

After a review of local conductors, we introduce the categories in which extension classes will be studied.

Fix distinct primes N and p and let K be a finite extension of $\mathbb{Q}_N$. If L/K is a Galois extension, let $\mathcal{D}=\mathcal{D}(L/K)$ be its Galois group and $\mathcal{I}=\mathcal{I}(L/K)$ its inertia subgroup. When $\mathcal{I}$ acts tamely on the finite $\mathbb{Z}_p[\mathcal{D}]$-module V, its Artin conductor exponent is given by $\mathfrak{f}_N(V)=\text{length}_{\mathbb{Z}_p} V/V^{\mathcal{I}}$. If

$$0\to V_1\to V\to V_2\to 0$$

is an exact sequence of finite $\mathbb{Z}_p[\mathcal{D}]$-modules, then $\mathfrak{f}_N(V)\geq \mathfrak{f}_N(V_1)+\mathfrak{f}_N(V_2)$.

Let A be an abelian variety over $\mathbb{Q}_N$ with semistable bad reduction and let $\mathbb{T}_p(A)$ denote its p-adic Tate module. We freely use results of Grothendieck [Grothendieck and Raynaud 1972], reviewed in [Brumer and Kramer 2001]. The p^∞-division field $\mathbb{Q}_N(A[p^\infty])$ depends only on the isogeny class of A, so is shared by the dual variety $\hat{A}$. The inertia subgroup $\mathcal{I}$ of $\text{Gal}(\mathbb{Q}_N(A[p^\infty])/\mathbb{Q}_N)$ is pro-p cyclic and $(\sigma-1)^2(\mathbb{T}_p(A))=0$ for any topological generator σ of $\mathcal{I}$. The fixed space $M_f(A)=\mathbb{T}_p(A)^{\mathcal{I}}$ is a $\mathbb{Z}_p$-direct summand $\mathbb{T}_p(A)$ and the toric space $M_t(A)$ is the $\mathbb{Z}_p$-submodule of $\mathbb{T}_p(A)$ orthogonal to $M_f(\hat{A})$ under the natural pairing of $\mathbb{T}_p(A)$ with $\mathbb{T}_p(\hat{A})$. Moreover, $(\sigma-1)(\mathbb{T}_p(A))$ has finite index in $M_t(A)$. The conductor exponent of A at N, denoted $\mathfrak{f}_N(A)$, is the $\mathbb{Z}_p$-rank of $\mathbb{T}_p(A)/M_f(A)$. Equivalently, we have $\mathfrak{f}_N(A)=\text{rank}_{\mathbb{Z}_p} M_t(A)=\text{rank}_{\mathbb{Z}_p}(\sigma-1)(\mathbb{T}_p(A))$.

Lemma 3.1. *Suppose that $\mathfrak{f}_N(A[p])=\mathfrak{f}_N(A)$. Then we have $\mathfrak{f}_N(A[p^n])=n\mathfrak{f}_N(A[p])$ for all $n\geq 1$ and $(\sigma-1)(\mathbb{T}_p(A))=M_t(A)$.*

Proof. In the following diagram

$$(\sigma-1)(A[p^n]) \xleftarrow{\bar{\pi}} \frac{(\sigma-1)(\mathbb{T}_p(A))}{(\sigma-1)(\mathbb{T}_p(A))\cap p^n\mathbb{T}_p(A)} \xrightarrow{\bar{j}} M_t(A)/p^nM_t(A),$$

$\bar{\pi}$ is an isomorphism induced by the natural projection $\pi:\mathbb{T}_p(A)\to A[p^n]$ and $\bar{j}$ is an injection induced by the inclusion $j:(\sigma-1)(\mathbb{T}_p(A))\to M_t(A)$. Since $M_t(A)$ is a $\mathbb{Z}_p$-direct summand of $\mathbb{T}_p(A)$, we have $M_t(A)/p^nM_t(A)\simeq(\mathbb{Z}/p^n)^f$, where $f=\mathfrak{f}_N(A)$ and thus

$$nf=\text{length}_{\mathbb{Z}_p} M_t(A)/p^nM_t(A)\geq \mathfrak{f}_N(A[p^n])\geq n\mathfrak{f}_N(A[p]), \tag{3.2}$$

using super-additivity of conductors for the last inequality. By assumption, the left and right sides of (3.2) are equal, so $\mathfrak{f}_N(A[p^n])=n\mathfrak{f}_N(A[p])$. Then $\bar{j}\circ\bar{\pi}^{-1}$ is an isomorphism and $(\sigma-1)(\mathbb{T}_p)=M_t(A)$ upon passage to the limit. □

We recall the following elegant theorem of Schoof on p-divisible groups.

Theorem 3.3 [Schoof 2005, Theorem 8.3]. *Let $\underline{C}$ be a full subcategory of the category of p-primary group schemes over $O=\mathbb{Z}[\frac{1}{N}]$, closed under taking products, closed flat subgroup schemes and quotients by closed flat subgroup schemes. Let $G=\{G_n\}$ and $H=\{H_n\}$ be p-divisible groups over O, with G_n and H_n in $\underline{C}$. Suppose that*:

(i) *$R=\text{End}(G)$ is a discrete valuation ring with uniformizer π and residue field $k=R/\pi R$.*

(ii) *The map* $\mathrm{Hom}_O(G[\pi], G[\pi]) \xrightarrow{\delta} \mathrm{Ext}^1_{\underline{C}}(G[\pi], G[\pi])$, *induced by the cohomology sequence of* $0 \to G[\pi] \to G[\pi^2] \to G[\pi] \to 0$, *is an isomorphism of one-dimensional* k*-vector spaces.*

(iii) *Each* H_n *admits a filtration by flat closed subgroup schemes whose successive subquotients are isomorphic to* $G[\pi]$.

Then H *is isomorphic to* G^r *for some* r.

For Theorem 3.3 to be applicable, the critical condition required of the category $\underline{C}$ is that (ii) hold. Additional motivation for our choice of category is provided at the end of this section.

Definition 3.4. Let $\Sigma = \{\mathcal{E}_i \mid 1 \le i \le s\}$ be a collection of finite flat group schemes over $\mathbb{Z}[\frac{1}{N}]$ such that

(i) $\mathcal{E}_i$ is biconnected over $\mathbb{Z}_p$ for all i and

(ii) the Galois modules E_i are absolutely simple and pairwise nonisomorphic.

Given Σ, a category $\underline{E}$ of finite flat group schemes $\mathcal{V}$ over $\mathbb{Z}[\frac{1}{N}]$ is a Σ-*category* if the following properties are satisfied:

E1. Each composition factor of $\mathcal{V}$ is isomorphic to some $\mathcal{E}_i$ with $1 \le i \le s$.

E2. If σ_v generates inertia at $v \mid N$, then $(\sigma_v - 1)^2$ annihilates $V = \mathcal{V}(\overline{\mathbb{Q}})$.

E3. If n_i is the multiplicity of E_i in the semisimplification V^{ss} of V, then

$$\mathfrak{f}_N(V) = \mathfrak{f}_N(V^{ss}) = \sum n_i \mathfrak{f}_N(E_i).$$

A collection of semistable abelian varieties A_i, good outside N, is Σ-*favorable* if $\mathrm{End}\, A_i = \mathbb{Z}$, the $\mathcal{E}_i = A_i[p]$ satisfy (i) and (ii) and $\mathfrak{f}_N(A_i) = \mathfrak{f}_N(E_i)$ for $1 \le i \le s$.

In particular, a favorable abelian surface A is Σ-favorable with $\Sigma = \{A[2]\}$.

Lemma 3.5. *If* $0 \to \mathcal{W} \to \mathcal{V} \to \overline{\mathcal{V}} \to 0$ *is an exact sequence of finite flat group schemes and* $\mathcal{V}$ *is in* $\underline{E}$, *then* $\mathcal{W}$ *and* $\overline{\mathcal{V}}$ *also are in* $\underline{E}$.

Proof. By super-additivity of conductors and **E3** for V, we have

$$\mathfrak{f}_N(V^{ss}) = \mathfrak{f}_N(W^{ss}) + \mathfrak{f}_N(\overline{V}^{ss}) \le \mathfrak{f}_N(W) + \mathfrak{f}_N(\overline{V}) \le \mathfrak{f}_N(V) = \mathfrak{f}_N(V^{ss}).$$

Hence **E3** is valid for both W and $\overline{V}$. The rest is clear. □

Lemma 3.5 implies that $\underline{E}$ is a full subcategory of the category of p-primary group schemes over $\mathbb{Z}[\frac{1}{N}]$, closed under taking products, closed flat subgroup schemes and quotients by closed flat subgroup schemes. As in [Schoof 2005], this guarantees that $\mathrm{Ext}^1_{\underline{E}}$ is defined.

Notation 3.6. If $\mathcal{V}$ and $\mathcal{W}$ in $\underline{E}$ are annihilated by p, write $\mathrm{Ext}^1_{[p],\underline{E}}(\mathcal{V}, \mathcal{W})$ for the subgroup of $\mathrm{Ext}^1_{\underline{E}}(\mathcal{V}, \mathcal{W})$ whose classes are represented by extensions killed by p.

Theorem 3.7. *Let* $\{A_i \mid 1 \le i \le s\}$ *be a* Σ*-favorable collection of abelian varieties and let* $\underline{E}$ *be the* Σ*-category with* $\Sigma = \{\mathcal{E}_i = A_i[p] \mid 1 \le i \le s\}$.

(i) *If B is isogenous to $\prod_i A_i^{n_i}$, then subquotients of $B[p^r]$ are in $\underline{E}$.*

(ii) *Conversely, let B be semistable and write $B[p]^{ss} = \oplus n_i \mathcal{E}_i$. Suppose that $\mathfrak{f}_N(B) = \sum n_i \mathfrak{f}_N(E_i)$ and*

$$\mathbf{E4}: \mathrm{Ext}^1_{[p],\underline{E}}(\mathcal{E}_i, \mathcal{E}_j) = 0, \quad \textit{for all } 1 \le i \le j \le s.$$

Then B is isogenous to $\prod A_i^{n_i}$.

Proof. Lemmas 3.1 and 3.5 imply the first claim. For the converse, it suffices by Lemma 3.5 to show that $B[p^r]$ belongs to $\underline{E}$. Property **E1** is clear and **E2** follows from semistability. By super-additivity of conductors,

$$\sum n_i \mathfrak{f}_N(E_i) = \mathfrak{f}_N(B[p]^{ss}) \le \mathfrak{f}_N(B[p]) \le \mathfrak{f}_N(B) = \sum n_i \mathfrak{f}_N(E_i).$$

Thus each weak inequality above is an equality and so

$$\mathfrak{f}_N(B[p^r]) = r\mathfrak{f}_N(B[p]) = \sum r n_i \mathfrak{f}(E_i)$$

by Lemma 3.1. Hence **E3** holds and $B[p^r]$ is in $\underline{E}$.

Assuming **E4**, the lemma below enables us to define isotypic decompositions of the finite flat group schemes in $\underline{E}$. Thus the p-divisible group of B is the product of its isotypic p-divisible subgroups $H^{(i)}$. If $G^{(i)}$ is the p-divisible group of A_i, then $\mathrm{End}(G^{(i)}) = \mathbb{Z}_p$ by the theorem of Faltings proving Tate's conjecture. Vanishing of $\mathrm{Ext}^1_{[p],\underline{E}}(\mathcal{E}_i, \mathcal{E}_i)$ and Proposition A.2 imply that $\mathrm{Ext}^1_{\underline{E}}(\mathcal{E}_i, \mathcal{E}_i) = \mathbb{F}_p$ thanks to the existence of the extension $0 \to \mathcal{E}_i \to A_i[p^2] \to \mathcal{E}_i \to 0$. Theorem 3.3 now gives $H_i \simeq G_i^{n_i}$ and so the p-divisible group of B is isomorphic to that of $\prod A_i^{n_i}$. Conclude by Faltings' theorem [1983, §5] on isogenies. □

Lemma 3.8. *Let M be a finite length module over the ring R and $E_1, \dots, E_s$ its nonisomorphic simple constituents. Let M_i be the maximal R-submodule all of whose composition factors are isomorphic to E_i. If $\mathrm{Ext}^1_R(E_i, E_j) = 0$ for $i \ne j$, then $M = \bigoplus M_i$, i.e., M is the sum of its isotypic components.*

Proof. If all composition factors of the R-modules N and N' are isomorphic to E_i, the same is true of $N + N'$ as a quotient of $N \oplus N'$, so the definition of M_i makes sense. The sum of the M_i is direct, since no simple module occurs in the intersection of M_j with the sum of the other isotypics. By the long exact sequence of Ext and induction, $\mathrm{Ext}^1_R(E_i, P) = 0$ if P does not involve E_i. Let $M' = \bigoplus_{i=1}^s M_i \subsetneq M$ and let N be a minimal submodule of M containing M'. Then, after relabeling, we have $N/M' \simeq E_s$. The exact sequence $0 \to M'/M_s \to N/M_s \to E_s \to 0$ splits, so there is a submodule N' of N with $N'/M_s \simeq E_s$, contradicting maximality of M_s. □

We conclude with some comments on the definition of $\underline{E}$ and the assumptions in Theorem 3.7. Schoof uses categories $\underline{D}$ satisfying only **E1** and **E2**. However, as shown in Example B.4, $\mathrm{Ext}^1_{[2],\underline{D}}(\mathcal{E}, \mathcal{E}) \ne 0$ for the cases of interest to us, violating Theorem 3.3(ii). Motivated by Theorem 3.7(i), we were led to add **E3** as a necessary condition. For the reader who might wonder why **E3** was not imposed by Schoof, we offer the following explanation.

Remark 3.9. In [Schoof 2005, §7], $p=2$, $\dim E=2$ and $\Delta=\mathrm{Gal}(\mathbb{Q}(E)/\mathbb{Q})\simeq\mathcal{S}_3$, so $H^1(\Delta,\mathrm{Mat}_2(\mathbb{F}_2))=0$ and the obstruction to splitting of extensions that we encounter in Example B.4 does not arise for Schoof. Moreover, **E2** implies **E3** if $\dim E_i=2\mathfrak{f}_N(E_i)$ for all i. Indeed, $V/V^{\langle\sigma_v\rangle}\simeq(\sigma_v-1)V\subseteq V^{\langle\sigma_v\rangle}$ by **E2**. Let $V^{ss}=\oplus n_iE_i$ and write $\ell(V)=\mathrm{length}_{\mathbb{Z}_p}V$. Then

$$2\sum n_i\mathfrak{f}_N(E_i)=\sum n_i\dim_{\mathbb{F}_p}E_i=\ell(V)=\ell((\sigma_v-1)V)+\ell(V^{\langle\sigma_v\rangle})$$
$$\geq 2\ell((\sigma_v-1)V)=2\mathfrak{f}_N(V)\geq 2\sum n_i\mathfrak{f}_N(E_i).$$

Hence $\mathfrak{f}_N(V)=\sum n_i\mathfrak{f}_N(E_i)$.

The lower bound $\mathfrak{f}_N(V)\geq\sum n_i\mathfrak{f}_N(E_i)$ holds for the conductor of V, while **E3** imposes equality. Thus, in Theorem 3.7(ii), $\mathfrak{f}_N(B)$ is as small as possible given the structure of $B[p]^{ss}$. But minimality of conductor does not guarantee that B is semistable, as the following example shows.

Example 3.10. Setzer [1981] gives an elliptic curve over $K=\mathbb{Q}(\sqrt{37})$ with everywhere good reduction:

$$C: y^2-\epsilon y=x^3+\tfrac{1}{2}(3\epsilon+1)x^2+\tfrac{1}{2}(11\epsilon+1)x,\quad \epsilon=6+\sqrt{37}.$$

If B is its Weil restriction to $\mathbb{Q}$, then B has good reduction outside $N=37$ and $\mathfrak{f}_N(B)=2$ by Milne's conductor formula [1972, Proposition 1]. Let A be any of the elliptic curves over $\mathbb{Q}$ of conductor 37. These curves share the same group scheme $\mathcal{E}=A[2]$ and $\mathfrak{f}_N(E)=1$. Let $\underline{E}$ be the Σ-category with $\Sigma=\{\mathcal{E}\}$. Then $B[2]^{ss}=\mathcal{E}\oplus\mathcal{E}$ and so **E3** holds. But B has potential good reduction at N and inertia at $v\mid N$ acts on $\mathbb{T}_2(B)$ through the finite quotient $\mathrm{Gal}(\mathbb{Q}_N(\sqrt{37})/\mathbb{Q}_N)$, so **E2** fails. Note that B was considered earlier in [Shimura 1972].

Remark 3.11. In his work on deformations, Ploner [2015] considered conditions **E1, E2** and **E4** for two-dimensional group schemes.

4. Some Honda systems

Recall that $\mathbb{W}$ is the ring of Witt vectors over a finite field k of characteristic p and let K be the quotient field of $\mathbb{W}$. Suppose that $\mathcal{E}=A[p]$ is an absolutely simple finite flat group scheme of order p^4 where A is an abelian surface over K with biconnected good reduction. In this section, we classify the Honda systems of such $\mathcal{E}$'s and those of extensions of $\mathcal{E}$ by itself annihilated by p.

Proposition 4.1. *Let* (M,L) *be the Honda system for a group scheme* $\mathcal{E}$ *as above. Then there is a k-basis* x_1,x_2,x_3,x_4 *for* M *such that* $\mathrm{L}=\mathrm{span}\{x_1,x_2\}$,

$$\mathrm{V}=\begin{bmatrix}0&0&0&0\\1&0&0&0\\0&\lambda&0&0\\0&0&0&0\end{bmatrix}\quad\text{and}\quad\mathrm{F}=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&1\\1&0&0&0\end{bmatrix}\tag{4.2}$$

for some λ *in* $k^\times$. *Furthermore* $x_1',\dots,x_4'$ *is another such basis if and only if* $x_1'=r^{p^2}x_1$ *and* $\lambda'=r^{1-p^4}\lambda$ *with* r *in* $k^\times$.

Proof. Let $\mathfrak{E} = (\mathrm{M}, \mathrm{L})$ be the Honda system for $\mathcal{E}$. Refer to Lemma 2.5 as needed. Theorem 2.4, applied to the p-divisible group of A implies that $\dim L = 2$. By absolute simplicity, $\mathcal{E}$ becomes a Raynaud $\mathbb{F}_{p^4}$-module scheme over the Witt vectors $\mathbb{W}(\bar{k})$ [Raynaud 1974; Tate 1997, §4]. Berthelot [1977, Lemme 2.5] shows that $\mathrm{M}' = \mathrm{M} \otimes_k \bar{k}$ admits a basis $\{\xi_i \mid i \in \mathbb{Z}/4\mathbb{Z}\}$ such that $\mathrm{F}(\xi_i) = \xi_{i+1}$ or $\mathrm{V}(\xi_{i+1}) = \xi_i$, with L' spanned by a subset of that basis.

Suppose that L' does not contain two successive basis vectors. Then we may assume that $\mathrm{L}' = \mathrm{span}\{\xi_1, \xi_3\}$. By injectivity of V on L, we have $\mathrm{V}\xi_1 = \xi_0$ and $\mathrm{V}\xi_3 = \xi_2$. Since $\mathrm{F}(\mathrm{M}') = \mathrm{span}\{\mathrm{F}(\xi_1), \mathrm{F}(\xi_3)\}$ is 2-dimensional, $\mathrm{V}(\xi_2) \neq \xi_1$, so $\mathrm{F}(\xi_1) = \xi_2$ and similarly $\mathrm{F}(\xi_3) = \xi_0$. If $\eta = \xi_1 + \xi_3$, then $\mathrm{F}\eta = \mathrm{V}\eta = \xi_2 + \xi_0$. Thus there is a sub-Honda system $(\mathrm{M}'', \mathrm{L}'')$ of $\mathfrak{E}$ with $\mathrm{M}'' = \mathrm{span}\{\eta, \mathrm{F}\eta\}$ and $\mathrm{L}'' = \mathrm{span}\{\eta\}$, contradicting absolute simplicity of $\mathcal{E}$.

Therefore, we may assume that $\mathrm{L}' = \mathrm{span}\{\xi_1, \xi_2\}$. Since V is injective on L', we cannot have $\mathrm{F}(\xi_1) = \xi_2$, so $\xi_1 = \mathrm{V}\xi_2 \in \mathrm{L}' \cap \mathrm{VL}'$ and $\dim_k(\mathrm{L} \cap \mathrm{VL}) = 1$ over the original ground field k. Write $x_2 = \mathrm{V}x_1 \neq 0$ in $\mathrm{L} \cap \mathrm{VL}$ with x_1 in L and so $\mathrm{L} = \mathrm{span}\{x_1, x_2\}$. Set $x_4 = \mathrm{F}x_1$ and $x_3 = \mathrm{F}^2 x_1$. Since $\dim_k \ker \mathrm{F} = 2$ and F is nilpotent, $\mathrm{F}^3 = 0$. By iterating F on $\mathrm{M} = \mathrm{L} + \mathrm{FM}$ to find that $\mathrm{FM} = \mathrm{FL} + \mathrm{F}^2\mathrm{L} = \mathrm{span}\{x_3, x_4\}$. Thus x_1, x_2, x_3, x_4 is a basis for M. Injectivity of V on L implies that $\mathrm{V}x_2 \neq 0$. But $\mathrm{V}x_2$ is in $\ker \mathrm{F} = \mathrm{VL} = \mathrm{span}\{x_2, x_3\}$ and V is nilpotent. Hence $\mathrm{V}x_2 = \lambda x_3$ for some $\lambda \in k^\times$, resulting in matrix representations of the form (4.2).

For another such basis, x_2' generates $\mathrm{L} \cap \mathrm{VL}$, so $x_2' = r^p x_2$ with $r \in k^\times$. Then $x_1' = r^{p^2} x_1$ and $x_3' = \mathrm{F}^2 x_1' = r^{p^4} x_3$. Thus $\lambda' x_3' = \mathrm{V}x_2' = r\mathrm{V}x_2 = r\lambda x_3 = r^{1-p^4}\lambda x_3'$ and so $\lambda' = r^{1-p^4}\lambda$ in $k^\times$. □

Notation 4.3. For $\lambda \in k^\times$, let $\mathfrak{E}_\lambda = (\mathrm{M}_0, \mathrm{L}_0)$ be the Honda system in the proposition and call x_1, x_2, x_3, x_4 a *standard basis* for $\mathfrak{E}_\lambda$. Denote the corresponding group scheme, Galois module and representation by $\mathcal{E}_\lambda$, E_λ and ρ_{E_λ} respectively.

Let $\mathrm{Ext}^1(\mathfrak{E}_\lambda, \mathfrak{E}_\lambda)$ be the group of classes of extensions of Honda systems

$$0 \to \mathfrak{E}_\lambda \xrightarrow{\iota} (\mathrm{M}, \mathrm{L}) \xrightarrow{\pi} \mathfrak{E}_\lambda \to 0 \tag{4.4}$$

under Baer sum [Mac Lane 1963, Chapter III, Theorem 2.1] and let $\mathrm{Ext}^1_{[p]}(\mathfrak{E}_\lambda, \mathfrak{E}_\lambda)$ be the subgroup such that $p\mathrm{M} = 0$.

Proposition 4.5. *If* (M, L) *represents a class in* $\mathrm{Ext}^1_{[p]}(\mathfrak{E}_\lambda, \mathfrak{E}_\lambda)$, *there is a k-basis* $e_1, \dots, e_8$ *for* M *such that* $\iota(x_1) = e_1$, $\pi(e_5) = x_1$, $\mathrm{L} = \mathrm{span}\{e_1, e_2, e_5, e_6\}$,

$$\mathrm{V} = \left[\begin{array}{cccc|cccc} 0&0&0&0&0&\lambda s_2&0&0\\ 1&0&0&0&0&\lambda s_3&0&0\\ 0&\lambda&0&0&0&\lambda s_4&0&0\\ 0&0&0&0&s_1&\lambda s_5&0&0\\ \hline 0&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&\lambda&0&0\\ 0&0&0&0&0&0&0&0 \end{array}\right] \quad \textit{and} \quad \mathrm{F} = \left[\begin{array}{cccc|cccc} 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&1&0&-s_1^p&-s_5^p&0\\ 1&0&0&0&0&0&-s_2^p&0\\ \hline 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0 \end{array}\right]$$

with s_1, s_2, s_3, s_4, s_5 *in* k. *For* $\tilde{k} = k/(\sigma^4 - 1)(k)$, *the map* $(\mathrm{M}, \mathrm{L}) \rightsquigarrow (s_1, \ldots, s_5)$ *induces an isomorphism of additive groups* $\mathbf{s} : \mathrm{Ext}^1_{[p]}(\mathfrak{E}_\lambda, \mathfrak{E}_\lambda) \xrightarrow{\sim} k \oplus k \oplus k \oplus \tilde{k} \oplus k$.

Proof. Let $\{x_j \mid 1 \le j \le 4\}$ be a standard basis for $\mathfrak{E}_\lambda$ and define $e_j = \iota(x_j)$ in (4.4). Since $0 \to \mathrm{L}_0 \xrightarrow{\iota} \mathrm{L} \xrightarrow{\pi} \mathrm{L}_0 \to 0$ is exact, we can extend e_1, e_2 to a basis for L by adjoining elements $\tilde{e}_5, \tilde{e}_6$ of L such that $\pi(\tilde{e}_5) = x_1$ and $\pi(\tilde{e}_6) = x_2$.

From $\mathrm{V}(\pi(\tilde{e}_5)) = \pi(\tilde{e}_6)$, we have $\mathrm{V}\tilde{e}_5 = \tilde{e}_6 + r_1 e_1 + r_2 e_2 + r_3 e_3 + s_1 e_4$ with s_1 and all r_i in k. Replace $\tilde{e}_5$ by $e_5 = \tilde{e}_5 + \sigma^2(a_1)e_1 + \sigma(a_2)e_2$ and $\tilde{e}_6$ by $e_6 = \tilde{e}_6 + b_1 e_1 + b_2 e_2$ with a_i, b_i in k. Then

$$\begin{aligned} \mathrm{V}e_5 &= \mathrm{V}\tilde{e}_5 + \sigma(a_1)e_2 + \lambda a_2 e_3 \\ &= \tilde{e}_6 + r_1 e_1 + (r_2 + \sigma(a_1))e_2 + (r_3 + \lambda a_2)e_3 + s_1 e_4 \\ &= e_6 + (r_1 - b_1)e_1 + (r_2 + \sigma(a_1) - b_2)e_2 + (r_3 + \lambda a_2)e_3 + s_1 e_4. \end{aligned}$$

Now choose a_i, b_i so that $\mathrm{V}(e_5) - e_6 = s_1 e_4$. Finally, let $e_8 = \mathrm{F}e_5$ and $e_7 = \mathrm{F}e_8$. Since $\mathrm{V}(\pi(e_6)) = \lambda\pi(e_7)$, we may choose elements s_i of k such that

$$\mathrm{V}e_6 = \lambda(e_7 + s_2 e_1 + s_3 e_2 + s_4 e_3 + s_5 e_4). \tag{4.6}$$

This verifies the matrix representation of V. From $0 = \mathrm{FV}e_5 = \mathrm{F}e_6 + \sigma(s_1)e_3$, we get $\mathrm{F}e_6 = -\sigma(s_1)e_3$. Apply F to (4.6) to find $\mathrm{F}e_7$ and obtain the matrix of F.

The only ambiguity left is that e_5 might be replaced by $e_5 + \sigma^2(a_1)e_1$, in which case s_4 becomes $s_4 + a_1 - \sigma^4(a_1)$ while s_1, s_2, s_3, s_5 remain unchanged.

Another extension $(\mathrm{M}', \mathrm{L}')$ is equivalent to (M, L) if and only if there is an isomorphism h in the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{E}_\lambda & \xrightarrow{\iota'} & (\mathrm{M}', \mathrm{L}') & \xrightarrow{\pi'} & \mathfrak{E}_\lambda & \longrightarrow & 0 \\ & & \big\downarrow \text{ident} & & \big\downarrow h & & \big\downarrow \text{ident} & & \\ 0 & \longrightarrow & \mathfrak{E}_\lambda & \xrightarrow{\iota} & (\mathrm{M}, \mathrm{L}) & \xrightarrow{\pi} & \mathfrak{E}_\lambda & \longrightarrow & 0. \end{array} \tag{4.7}$$

Let $e'_1, \ldots e'_8$ be a basis for $(\mathrm{M}', \mathrm{L}')$ constructed as above. Since $h(e'_1), \ldots, h(e'_8)$ must be another such basis, the isomorphism h exists if and only if $h(e'_1) = e_1$ and $h(e'_5) = e_5 + \sigma^2(a_1)e_1$ with a_1 in k. It follows that $\mathbf{s}$ is a well-defined bijection.

To verify the additivity of $\mathbf{s}$, let (M, L) and $(\mathrm{M}', \mathrm{L}')$ represent two classes in $\mathrm{Ext}^1_{[p]}(\mathfrak{E}_\lambda, \mathfrak{E}_\lambda)$ and let $0 \to \mathfrak{E}_\lambda \xrightarrow{\iota''} (\mathrm{M}'', \mathrm{L}'') \xrightarrow{\pi''} \mathfrak{E}_\lambda \to 0$ represent their Baer sum. To obtain a k-basis for M'' let $\gamma_i = (e_i, 0)$ in $\mathrm{M} \times \mathrm{M}'$ for $1 \le i \le 4$ and $\gamma_i = (e_i, e'_i)$ for $5 \le i \le 8$, each of which satisfies the fiber product condition that $\pi''(\gamma_i) = \pi(e_i) = \pi'(e'_i)$. The relations are given by $\iota''(a) = (\iota(a), 0) = (0, \iota'(a))$ for all a in $\mathfrak{E}_\lambda$. We have

$$\begin{aligned} \mathrm{V}\gamma_5 &= (\mathrm{V}e_5, \mathrm{V}e'_5) = (e_6 + s_1 e_4, e'_6 + s'_1 e'_4) = \gamma_6 + (s_1 e_4, 0) + (0, s'_1 e'_4) \\ &= \gamma_6 + (s_1 e_4, 0) + (s'_1 e_4, 0) = \gamma_6 + (s_1 + s'_1)\gamma_4, \end{aligned}$$

$$\begin{aligned}
\mathrm{V}\gamma_6 &= (\mathrm{V}e_6, \mathrm{V}e_6') = \lambda(e_7, e_7') + \sum_{1\le i\le 4} \lambda(s_i e_i, s_i' e_i') = \lambda\gamma_7 + \sum_{1\le i\le 4} \lambda(s_i + s_i')\gamma_i,\\
\mathrm{F}\gamma_6 &= (\mathrm{F}e_6, \mathrm{F}e_6') = -(s_1^p e_3, (s_1')^p e_3') = -(s_1^p e_3, 0) - (0, (s_1')^p e_3')\\
&= -(s_1^p e_3, 0) - ((s_1')^p e_3, 0) = -(s_1 + s_1')^p \gamma_3,\\
\mathrm{F}\gamma_7 &= (\mathrm{F}e_7, \mathrm{F}e_7') = -(s_5^p e_3, (s_5')^p e_3') - (s_2^p e_4, (s_2')^p e_4')\\
&= -(s_5 + s_5')^p \gamma_3 - (s_2 + s_2')^p \gamma_4.
\end{aligned}$$

By completing the matrices for V and F, we find that $s_i'' = s_i + s_i'$ for $1 \le i \le 5$. □

5. The local theory

In this section, we study the fields of points of extensions of exponent p whose Honda systems were described above. In particular, we obtain good conductor bounds. We use freely the notation of Section 2. Let K be the quotient field of $\mathbb{W}$ and let $\dot{a}$ be the Teichmüller lift to $\mathbb{W}$ of a in k, with $\dot{0} = 0$. Assume that w is in $\mathcal{O}_{\overline{K}}$ and $\operatorname{ord}_p(w) > 0$. For a in $\overline{K}/w\mathcal{O}_{\overline{K}}$, let $\tilde{a}$ be an arbitrary lift to $\overline{K}$. Assertions requiring lifts are made only when the result is independent of the choices, as in the following examples. If a is not in $w\mathcal{O}_{\overline{K}}$, let $\operatorname{ord}_p(a) = \operatorname{ord}_p(\tilde{a})$. For w' in $\mathcal{O}_{\overline{K}}$ such that $0 < \operatorname{ord}_p(w') \le \operatorname{ord}_p(w)$, let $a \equiv b \pmod{w'}$ mean that $\tilde{a} - \tilde{b}$ is in $w'\mathcal{O}_{\overline{K}}$. If $f(X)$ is in $\overline{K}[X]$, we write $f(a) \equiv 0 \pmod{w''\mathcal{O}_{\overline{K}}}$ only if $f(\tilde{a})$ is in $w''\mathcal{O}_{\overline{K}}$, for all lifts $\tilde{a}$ of a. For this section, we write $x \sim y$ when $\operatorname{ord}_p(x/y - 1) > 0$ and $x = y + O(w)$ if $\operatorname{ord}_p(x - y) \ge \operatorname{ord}_p(w)$.

5.1. *The irreducible case.* Let $\mathcal{E}_\lambda$ be the group scheme and $x_1, \dots, x_4$ a standard basis for the corresponding Honda system $\mathfrak{E}_\lambda = (\mathrm{M}_0, \mathrm{L}_0)$ from Notation 4.3. The Galois module structure of E_λ is well-known, but a description of E_λ by Witt covectors is required for our analysis of extensions of $\mathcal{E}_\lambda$ by $\mathcal{E}_\lambda$. Let $F = K(E_\lambda)$, reserving Roman F and V for the Honda system Frobenius and Verschiebung operators in this section. Recall that points of the Galois module E_λ correspond to D_k-homomorphisms $\psi : \mathrm{M}_0 \to \widehat{CW}_k(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})$ such that $\xi(\psi(\mathrm{L}_0)) = 0$, see Section 2.

Proposition 5.1.1. *Let* $\mathfrak{R}_\lambda = \{a \in \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}} \mid \lambda^{p^2} a^{p^4} \equiv (-p)^{p+1} a \pmod{p^{p+2}\mathcal{O}_{\overline{K}}}\}$. *Given a in $\mathfrak{R}_\lambda$, define b and c in $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ by*

$$b \equiv -\tfrac{1}{p}\lambda^p a^{p^3} \pmod{p\mathcal{O}_{\overline{K}}} \quad \textit{and} \quad c \equiv \lambda a^{p^2} \pmod{p\mathcal{O}_{\overline{K}}}.$$

(i) *A D_k-map $\psi = \psi_a$ belongs to a point P_a of E_λ if and only if $\psi(x_1) = (\vec{0}, c, b, a)$ with a in $\mathfrak{R}_\lambda$. If so, $\psi(x_2) = (\vec{0}, c, b)$, $\psi(x_3) = (\vec{0}, \lambda^{-1}c)$ and $\psi(x_4) = (\vec{0}, a^p)$.*

(ii) *$F = K(E_\lambda)$ is the splitting field of $f_\lambda(x) = \dot{\lambda}^{p^2} x^{p^4-1} - (-p)^{p+1}$ over K. The maximal subfield of F unramified over K is $F_0 = K(\boldsymbol{\mu}_{p^4-1}, \eta)$, where η is any root of $x^{p+1} - \dot{\lambda}$. Moreover F/F_0 is tamely ramified of degree $t = (p^2+1)(p-1)$. For $a \ne 0$ we have*

$$\operatorname{ord}_p(a) = \frac{1}{t}, \quad \operatorname{ord}_p(b) = \frac{p^2 - p + 1}{t}, \quad \operatorname{ord}_p(c) = \frac{p^2}{t}. \tag{5.1.2}$$

(iii) $\mathfrak{R}_\lambda$ *is an* $\mathbb{F}_{p^4}$*-vector space under the usual operations in* $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ *and* $a \mapsto P_a$ *defines an* $\mathbb{F}_p[G_K]$*-isomorphism* $\mathfrak{R}_\lambda \xrightarrow{\sim} E_\lambda$.

Proof. (i) If ψ belongs to a point in E_λ, then $\psi(x_1) = (\vec{0}, c, b, a)$, since $V^3 = 0$. We obtain $\psi(x_2)$ and $\psi(x_3)$ by applying V, while $\psi(x_4) = \psi(\mathrm{F}x_1) = (\vec{0}, c^p, b^p, a^p)$. Use $0 = \mathrm{VF}(x_1) = \mathrm{V}x_4$ to find that $c^p = b^p = 0$, so $\mathrm{ord}_p(b), \mathrm{ord}_p(c) \geq 1/p$. In addition, $\mathrm{F}(x_4) = x_3$ implies that $c = \lambda a^{p^2}$. Let $\tilde{a}, \tilde{b}, \tilde{c}$ denote lifts to $\mathcal{O}_{\overline{K}}$. Vanishing of $\xi(\psi(L))$ provides the additional congruences modulo $p\mathcal{O}_{\overline{K}}$:

$$\tilde{a} + \tfrac{1}{p}\tilde{b}^p + \tfrac{1}{p^2}\tilde{c}^{p^2} \equiv 0 \quad \text{and} \quad \tilde{b} + \tfrac{1}{p}\tilde{c}^p \equiv 0. \tag{5.1.3}$$

Thus $p\,\mathrm{ord}_p(\tilde{c}) = \mathrm{ord}_p(p\tilde{b}) \geq 1 + \frac{1}{p}$ and so $\frac{1}{p^2}\tilde{c}^{p^2} \equiv 0$. With this simplification, the required congruences follow from (5.1.3). Furthermore, these congruences are sufficient to imply that ψ belongs to $\mathcal{E}_\lambda$ when $\psi(x_1) = (\vec{0}, c, b, a)$.

(ii) If $f_\lambda(\theta) = 0$ and ζ generates $\boldsymbol{\mu}_{p^4-1}$, then the roots of f_λ have the form $\theta_j = \zeta^j\theta$ while their reductions modulo p give all nonzero elements of $\mathfrak{R}_\lambda$. For the converse, let $\tilde{a}$ be a lift of $a \in \mathfrak{R}_\lambda$ and $g(x) = x^{p^4} - x$. Then $g(\tilde{a}/\theta) \equiv 0 \pmod{\frac{p}{\theta}\mathcal{O}_{\overline{K}}}$ and so $\tilde{a} \equiv 0$ or $\tilde{a} \equiv \theta_j \pmod{p\mathcal{O}_{\overline{K}}}$ for some j by Hensel's lemma. Hence $F = K(\boldsymbol{\mu}_{p^4-1}, \theta)$ is the splitting field of f_λ. Let F_0 be the maximal subfield of F unramified over K. Since $\dot{\lambda}^{p^2}$ and therefore also $\dot{\lambda}$ is a $(p+1)$ power in $K(\theta)$, each root η of $x^{p+1} - \dot{\lambda}$ is in F_0. Furthermore, θ satisfies an Eisenstein polynomial of the form $\eta^{p^2}x^t + \omega p = 0$ over F_0 for some ω in $\boldsymbol{\mu}_{p+1}$. Hence K/F_0 is tamely ramified of degree t and we obtain the desired ordinals of a, b, c.

(iii) The embedding $\mathbb{F}_{p^4} = \mathbb{W}(\mathbb{F}_{p^4})/p\mathbb{W}(\mathbb{F}_{p^4}) \hookrightarrow \mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ defines the scalar multiplication by $\mathbb{F}_{p^4}$. Closure of $\mathfrak{R}_\lambda$ under this operation and under the usual addition in $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$ is clear. The asserted Galois isomorphism follows from the correspondence between D_k-homomorphisms belonging to $\mathcal{E}_\lambda$ and points of E_λ once we check that $a \mapsto P_a$ is additive. If a_1 and a_2 are in $\mathfrak{R}_\lambda$, then there is some a in $\mathfrak{R}_\lambda$ such that $\psi_{a_1}(x_1) \dot{+} \psi_{a_2}(x_1) = \psi_a(x_1)$. Denote this equation of Witt covectors by $(\vec{0}, c_1, b_1, a_1) \dot{+} (\vec{0}, c_2, b_2, a_2) = (\vec{0}, c, b, a)$. Then $c = c_1 + c_2$, so $a^{p^2} = a_1^{p^2} + a_2^{p^2}$ in $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$. By using lifts of a, a_1 and a_2 of the form $\omega_0\theta$, $\omega_1\theta$ and $\omega_2\theta$, with each ω_j in $\boldsymbol{\mu}_{p^4-1} \cup \{0\}$, we find that

$$\omega_0^{p^2} \equiv \omega_1^{p^2} + \omega_2^{p^2} \equiv (\omega_1 + \omega_2)^{p^2} \left(\mathrm{mod}\ \frac{p}{\theta^{p^2}}\mathcal{O}_{\overline{K}}\right).$$

Since the ω's lie in the absolutely unramified field $\mathbb{Q}_p(\boldsymbol{\mu}_{p^4-1})$ and $\mathrm{ord}_p(p/\theta^{p^2}) > 0$, we obtain $\omega_0 \equiv \omega_1 + \omega_2 \pmod{p}$ and thus $a = a_1 + a_2$ in $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$. Alternatively, $\mathrm{ord}_p(a - a_1 - a_2) \geq 1$ by the covector addition formulas in Lemma 2.7. □

Remark 5.1.4. (i) By (ii) above, the lifts of all $a \neq 0$ in $\mathfrak{R}_\lambda$ to $\mathcal{O}_{\overline{K}}$ comprise the cosets $\zeta^j\theta + p\mathcal{O}_{\overline{K}}$. Thus $\mathfrak{R}_\lambda$ descends to an $\mathbb{F}_{p^4}$-vector subspace of $\mathcal{O}_F/p\mathcal{O}_F$ and we write

$$\mathfrak{R}_\lambda(F) = \{a \in \mathcal{O}_F/p\mathcal{O}_F \mid \dot{\lambda}^{p^2}a^{p^4} \equiv (-p)^{p+1}a \pmod{p^{p+2}\mathcal{O}_F}\}.$$

For α in $\mathbb{F}_{p^4}$ and a in $\mathfrak{R}_\lambda$, we write $\alpha P_a = P_{\alpha a}$, in agreement with multiplication on Witt covectors. In fact, $\alpha\psi_a = \psi_{\alpha a}$, since evaluating on x_1 gives

$$[\alpha](\vec{0}, c_a, b_a, a) = (0, \alpha^{1/p^2} c_a, \alpha^{1/p} b_a, \alpha a) = (\vec{0}, c_{\alpha a}, b_{\alpha a}, \alpha a).$$

(ii) If h is in the ramification subgroup of $\mathrm{Gal}(F/K)$, then h acts on $\mathfrak{R}_\lambda(F)$ by $h(a) = \alpha a$, where $\alpha \in \boldsymbol{\mu}_t$ depends on h. The structure of $\mathcal{E}_\lambda$ as a Raynaud $\mathbb{F}_{p^4}$-module scheme is reflected by $h(P_a) = P_{h(a)} = P_{\alpha a} = \alpha P_a$. However, Frobenius in $\mathrm{Gal}(F/K)$ acts on the scalars.

(iii) By Proposition 5.1.1, we have $b^p \equiv -pa (\mathrm{mod}\ p^2)$, $c^p \equiv \lambda^p a^{p^3} \equiv -pb (\mathrm{mod}\ p^2)$ and $c^{p^2} \equiv (-p)^{p+1} a (\mathrm{mod}\ p^{p+2})$. These congruences are independent of the choices of lifts to $\mathcal{O}_{\overline{K}}$.

Using the local structure above, we next obtain a group scheme $\mathcal{E}$ over $\mathbb{Z}\big[\frac{1}{N}\big]$ fulfilling the hypotheses of Definition 3.4 for a Σ-category $\underline{E}$ with $\Sigma = \{\mathcal{E}\}$. We also determine the image of the Galois representation provided by E.

Corollary 5.1.5. *Let E be a four-dimensional symplectic module over $\mathbb{F}_p$ and let $\rho : G_{\mathbb{Q}} \to \mathrm{GSp}(E)$ be unramified outside $\{p, N, \infty\}$ and tamely ramified at the prime $N \neq p$. Suppose that*:

(i) *ρ restricted to a decomposition group at p is isomorphic to a local representation of the form ρ_{E_λ} as in* Notation 4.3.

(ii) *Inertia at $v \mid N$ acts on E via a cyclic quotient $\langle\sigma_v\rangle$ with $(\sigma_v - 1)^2 = 0$ and $\mathrm{rank}(\sigma_v - 1) = 1$ as a matrix.*

(iii) *The fixed field of $\rho^{-1}(\mathrm{Sp}(E))$ is $\mathbb{Q}(\mu_p)$ when p is odd.*

Then there is a unique finite flat group scheme $\mathcal{E}$ over $\mathbb{Z}\big[\frac{1}{N}\big]$ whose associated Galois representation is ρ. Moreover, the Galois image $G = \rho(G_{\mathbb{Q}})$ is $\mathrm{GSp}_4(\mathbb{F}_p)$ for $p \geq 2$ or possibly $\mathrm{O}_4^-(\mathbb{F}_2) \simeq \mathcal{S}_5$ when $p = 2$.

Proof. By (i), the local representation is irreducible and so is E. We patch as described before (2.2) to get the uniqueness.

Since σ_v is a transvection by (ii), the normal subgroup P generated by transvections is nontrivial. Follow the proof of [Brumer and Kramer 2012, Proposition 2.8], using $\dim E = 4$ and the fact that N is square-free, to conclude that E is irreducible for the group P generated by transvections. If $p = 2$, we find that G is isomorphic to $\mathrm{Sp}_4(\mathbb{F}_2) \simeq \mathcal{S}_6$ or $\mathrm{O}_4^-(\mathbb{F}_2) \simeq \mathcal{S}_5$. Since 5 must divide $|G|$, we rule out $\mathcal{S}_3 \wr \mathcal{S}_2$. When p is odd, G contains $\mathrm{Sp}_4(\mathbb{F}_p)$ by [Kemper and Malle 1997] and thus is isomorphic to $\mathrm{GSp}_4(\mathbb{F}_p)$ by (iii). □

When $p = 2$ and A is a favorable abelian surface, $\mathcal{E} = A[2]$ provides a representation ρ as in the corollary.

5.2. *Extensions of exponent p.* Let $0 \to \mathcal{E}_\lambda \xrightarrow{\iota} \mathcal{W} \xrightarrow{\pi} \mathcal{E}_\lambda \to 0$ be an extension of $\mathcal{E}_\lambda$ by $\mathcal{E}_\lambda$ killed by p with parameters $\mathbf{s}(\mathcal{W}) = [s_1 \cdots s_5]$ from Proposition 4.5. Let P_a denote the point of E_λ corresponding to a in $\mathfrak{R}_\lambda(F)$, see Proposition 5.1.1(iii) and Remark 5.1.4. Then the fiber over P_a has the form $Q + \iota(E_\lambda)$ for any fixed Q in W such that $\pi(Q) = P_a$. We write $F_a = F(Q)$ for the *fiber field* generated over F by the coordinates of Q.

Notation 5.2.1. Write $R_u = \overline{K}/\frac{p}{u}\mathcal{O}_{\overline{K}}$, provided that u is in $\mathcal{O}_{\overline{K}}$ and $\mathrm{ord}_p(u) < 1$.

Proposition 5.2.2. *For φ to correspond to a point of W in the fiber over $P_a \neq 0$, it is necessary and sufficient that $\varphi(e_1) = (\vec{0}, c, b, a)$ as in* Proposition 5.1.1 *and*

$$\varphi(e_5) = (\vec{0}, (\lambda s_2)^1/p^2 c, (\lambda s_2)^1/pb + (\lambda s_3)^1/pc, cz, by, ax)$$

where x, y, z in $\overline{K}$ satisfy all the following congruences:

$$\begin{aligned} &\text{i)} && x - y^p + p^{p-1} z^{p^2} = 0 \quad \text{in } R_a. \\ &\text{ii)} && y - z^p + p\lambda^{-p}\epsilon_p a^{p-p^3} = 0 \quad \text{in } R_b. \\ &\text{iii)} && x^{p^2} - z + wa^{-p^2} = 0 \quad \text{in } R_c. \end{aligned} \tag{5.2.3}$$

with $w = s_2 a + s_3 b + s_4 \lambda^{-1} c + s_5 a^p$, $\epsilon_p = s_1$ if $p \geq 3$ and $\epsilon_2 = s_1 - (\lambda s_2)^2$ if $p = 2$. Equivalently, z in $\overline{K}$ satisfies $f_a(z) = 0$ in R_c, where

$$f_a(Z) = [(Z^p - p\lambda^{-p}\epsilon_p a^{p-p^3})^p - p^{p-1} Z^{p^2}]^{p^2} - Z + wa^{-p^2} \tag{5.2.4}$$

and the classes of x in R_a and y in R_b are determined by (5.2.3)(i) *and* (ii). *When $\epsilon_p = 0$, we may instead use $f_a(Z) = Z^{p^4} - Z + wa^{-p^2}$.*

Proof. Let φ in $\mathrm{Hom}_{D_k}(\mathrm{M}, \widehat{CW}_k(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}))$ be an element of $\mathcal{W}$. Since M is generated by e_1 and e_5 as a D_k-module, φ is determined by $\varphi(e_1)$ and $\varphi(e_5)$. The injection of $\mathfrak{E}_\lambda$ to M yields $\varphi(e_j) = \psi(x_j)$ for $1 \leq j \leq 4$, as in Proposition 5.1.1(i). Set $\varphi(e_5) = (\vec{0}, d_4, d_3, d_2, d_1, d_0)$, with only the five rightmost coordinates significant, since $\mathrm{V}^5 = 0$. Applying $\mathrm{FV} = 0$ to e_5 gives $d_4^p = d_3^p = d_2^p = d_1^p = 0$.

From the matrix representation of V, we have

$$\varphi(e_6) = \mathrm{V}(\varphi(e_5)) \dot{+} [-s_1]\varphi(e_4) = (\vec{0}, d_4, d_3, d_2, d_1 - s_1 a^p)$$

and so $\varphi(\lambda^{-1}\mathrm{V}e_6) = [\lambda^{-1}](\vec{0}, d_4, d_3, d_2)$. We also have

$$\begin{aligned} \varphi(\lambda^{-1}\mathrm{V}e_6) &= \varphi(e_7) \dot{+} \varphi(s_2 e_1) \dot{+} \varphi(s_3 e_2) \dot{+} \varphi(s_4 e_3) \dot{+} \varphi(s_5 e_4) \\ &= \mathrm{F}^2\varphi(e_5) \dot{+} (\vec{0}, \sigma^{-2}(s_2)c, \sigma^{-1}(s_2)b, s_2 a) \dot{+} (\vec{0}, \sigma^{-1}(s_3)c, s_3 b + s_4\lambda^{-1}c + s_5 a^p) \\ &= (\vec{0}, d_0^{p^2}) \dot{+} (\vec{0}, s_2^{1/p^2}c, s_2^{1/p}b + s_3^{1/p}c, s_2 a + s_3 b + s_4\lambda^{-1}c + s_5 a^p - \Phi_p(s_2^{1/p}b, s_3^{1/p}c)) \\ &= (\vec{0}, s_2^{1/p^2}c, s_2^{1/p}b + s_3^{1/p}c, s_2 a + s_3 b + s_4\lambda^{-1}c + s_5 a^p + d_0^{p^2}). \end{aligned}$$

since $\Phi_p(s_2^{1/p}b, s_3^{1/p}c) = 0$ by (5.1.2) and Lemma 2.6. Modulo $p\mathcal{O}_{\overline{K}}$, this gives:

$$d_4 \equiv (\lambda s_2)^{1/p^2}c, \quad d_3 \equiv (\lambda s_2)^{1/p}b + (\lambda s_3)^{1/p}c, \quad d_2 \equiv \lambda(d_0^{p^2} + w). \tag{5.2.5}$$

Vanishing of the Hasse–Witt map on $\varphi(\mathrm{L})$ gives the following additional relations:

$$\begin{aligned} \xi(\varphi(e_5)) &= \frac{d_4^{p^4}}{p^4} + \frac{d_3^{p^3}}{p^3} + \frac{d_2^{p^2}}{p^2} + \frac{d_1^p}{p} + d_0 \equiv 0 \pmod{p\mathcal{O}_{\overline{K}}}, \\ \xi(\varphi(e_6)) &= \frac{d_4^{p^3}}{p^3} + \frac{d_3^{p^2}}{p^2} + \frac{d_2^p}{p} + d_1 - s_1 a^p \equiv 0 \pmod{p\mathcal{O}_{\overline{K}}}. \end{aligned} \tag{5.2.6}$$

Since $p^2 \operatorname{ord}_p(d_4) \geq p^2 \operatorname{ord}_p(c) > p+1$, we have $p^{-3}d_4^{p^3} \equiv 0$ and $p^{-4}d_4^{p^4} \equiv 0 \pmod{p}$. Thus the d_4-terms drop out of (5.2.6). By (5.2.5), we have

$$\begin{aligned} d_3^p &\equiv \lambda s_2 b^p + \lambda s_3 c^p \pmod{p^2}, \\ d_3^{p^2} &\equiv (\lambda s_2)^p b^{p^2} + (\lambda s_3)^p c^{p^2} \pmod{p^3}, \\ d_3^{p^3} &\equiv (\lambda s_2)^{p^2} b^{p^3} + (\lambda s_3)^{p^2} c^{p^3} \pmod{p^4}. \end{aligned}$$

In addition,

$$\operatorname{ord}_p\left(\frac{c^{p^j}}{p^j}\right) > \operatorname{ord}_p\left(\frac{b^{p^j}}{p^j}\right) = \frac{p^j(p^2-p+1)}{(p-1)(p^2+1)} - j = p^{j-1}\left(1 + \frac{1}{(p-1)(p^2+1)}\right) - j$$

is greater than 1 if (i) $j = 3$ and all p or (ii) $j = 2$ and $p \geq 3$. If $j = 2$ and $p = 2$, we also have $\operatorname{ord}_2(c^4/4) > 1$ and so (5.2.6) simplifies to

$$p^{-2}d_2^{p^2} + p^{-1}d_1^p + d_0 \equiv 0 \quad \text{and} \quad p^{-1}d_2^p + d_1 - \epsilon_p a^p \equiv 0. \tag{5.2.7}$$

Let $x = d_0/a$ in R_a, $y = d_1/b$ in R_b and $z = d_2/c$ in R_c. Then (5.2.5) and (5.2.7) give (5.2.3), using the equations for a, b, c in Remark 5.1.4(iii). It follows that $f_a(z) = 0$ in R_c for f_a given by (5.2.4). When $\epsilon_p = 0$, we have

$$\operatorname{ord}_p(z) = \frac{1}{p^4}\operatorname{ord}_p(wa^{-p^2}) \geq -\frac{(p^2-1)}{p^4}\operatorname{ord}_p(a) = -\frac{p+1}{p^4(p^2+1)}$$

and thus

$$\operatorname{ord}_p\left(\binom{p^2}{j} p^{(p-1)j} z^{p^4}\right) = (p-1)j + 2 - \operatorname{ord}_p(j) + p^4 \operatorname{ord}_p(z) \geq 1,$$

i.e., the middle terms of the binomial expansion for $f_a(z)$ drop out.

Conversely, if $f_a(z) = 0$ in R_c and x and y are defined by (5.2.3)(i) and (ii), then (5.2.3)(iii) holds and we obtain a D_k-homomorphism belonging to a point of W in the fiber over P. □

Notation 5.2.8. If λ in $k^\times$ is fixed, then a in

$$\mathfrak{R}_\lambda(F) = \{a \in \mathcal{O}_F/p\mathcal{O}_F \mid \dot{\lambda}^{p^2} a^{p^4} \equiv (-p)^{p+1} a \pmod{p^{p+2}\mathcal{O}_F}\}$$

determines b and c in $\mathcal{O}_F/p\mathcal{O}_F$ by the congruences in Proposition 5.1.1. If z in R_c satisfies the resulting congruence $f_a(z) = 0$ in R_c, then z determines x in R_a and y in R_b by (5.2.3). Using the congruences in (5.2.5), set $\mathbf{d}_a(z) = (\vec{0}, d_4, d_3, cz, by, ax)$. Let φ_z be the D_k-homomorphism such that $\varphi_z(e_1) = (\vec{0}, c, b, a)$ and $\varphi_z(e_5) = \mathbf{d}_a(z)$ and let Q_z be the corresponding point in W. The *fiber field* generated by the point of W lying over the point P_a of E is $F_a = F(Q_z)$.

We next examine the effect of various choices of lifts on constructing a generator for the extension F_a/F. Under the assumptions of Notation 5.2.8, choose lifts to $\mathcal{O}_K$ of λ and the entries in $\mathbf{s}$. By Remark 5.1.4(i), a has a lift $\tilde{a}$ in $\mathcal{O}_F$. Using the congruences in Proposition 5.1.1 as equations, $\tilde{a}$ determines lifts $\tilde{b}$ and $\tilde{c}$ in $\mathcal{O}_F$ of b and c. Let $\tilde{f}$ be the polynomial with coefficients in F obtained by using the respective lifts to replace the corresponding coefficients of $f_a(Z)$.

Corollary 5.2.9. *Construct $\tilde{f}(Z)$ in $F[Z]$ by choosing the lifts described above. If θ is any root of $\tilde{f}$ in $\overline{K}$, then $F_a = F(\theta)$. If $\epsilon_p = 0$ then $h(X) = X^p - X + \tilde{w}\tilde{a}^{-p^2}$ splits completely in F_a.*

Proof. Let M be the splitting field of $\tilde{f}$ over F. Since the p^4 solutions to the congruence $f_a(Z) = 0$ in R_c correspond to the distinct points of W in the fiber over P_a, the roots of $\tilde{f}$ in $\overline{K}$ remain distinct when reduced to R_c. If θ is any root of $\tilde{f}$, its reduction z in R_c determines the point Q_z. Thus F_a is contained in M. If γ is in $\mathrm{Gal}(M/F_a)$, then $Q_z = \gamma(Q_z) = Q_{\gamma(z)}$, so $\gamma(z) = z$ in R_c. But then $\gamma(\theta) = \theta$, since the roots of $\tilde{f}$ are distinct modulo $\frac{p}{c}\mathcal{O}_{\overline{K}}$. Hence $F_a = F(\theta) = M$ is independent of the various choices of lifts.

When $\epsilon_p = 0$, we have $p^4 \operatorname{ord}_p(\theta) = \operatorname{ord}_p(w/a^{p^2}) \geq (1-p^2) \operatorname{ord}_p(a)$. We find that $\alpha = \theta^{p^3} + \theta^{p^2} + \theta^p + \theta$ satisfies

$$\alpha^p - \alpha \equiv \theta^{p^4} - \theta \equiv -wa^{-p^2} \left(\bmod \frac{p}{a^{p^2}}\mathcal{O}_L\right),$$

since the worst case middle term in the binomial expansion of α^p leads to

$$\operatorname{ord}_p(p\theta^{p^3(p-1)}\theta^{p^2}) = 1 + (p^4 - p^3 + p^2) \operatorname{ord}_p(\theta) \geq 1 - p^2 \operatorname{ord}_p(a).$$

Hence $h(\alpha) \equiv 0 \pmod{pa^{-p^2}\mathcal{O}_L}$. Upon clearing denominators, Hensel's lemma [Lang 1994, II, §2] implies that h has a root in F_a and the other roots come by refining $\alpha + j$ with $1 \leq j \leq p-1$. □

A polynomial g_a of degree p^4, analogous to f_a, but such that y in R_b satisfies $g_a(y) = 0$ in R_b, can also be derived from Proposition 5.2.2 as in the Corollary below. Then y determines x in R_a and z in R_b and thus Q_z. Choosing appropriate lifts leads to $\tilde{g}(Y)$ in $F[Y]$, such that a root of $\tilde{g}$ also generates the extension F_a/F. Similar considerations apply to x.

Corollary 5.2.10. *Let $\mathbf{s} = [s_1 0000]$ and choose lifts $\tilde{\lambda}$, $\tilde{s}_1$ in $\mathcal{O}_K$ and $\tilde{a}$ in $\mathcal{O}_F$. Then $F_a = F(\vartheta)$ for any root ϑ in $\overline{K}$ of $\tilde{g}(Y) = Y^{p^4} - Y - p\tilde{\lambda}^{-p}\tilde{s}_1\tilde{a}^{p-p^3}$. In addition, $h(X) = X^p - X - p\tilde{\lambda}^{-p}\tilde{s}_1\tilde{a}^{p-p^3}$ splits completely in F_a.*

Proof. By assumption, $w = 0$ and $\epsilon_p = s_1$. It suffices to treat $s_1 \neq 0$. In the proof of Proposition 5.2.2, we showed that $d_1^p = 0$ in $\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}}$. Hence

$$\operatorname{ord}_p(y) = \operatorname{ord}_p\left(\tfrac{d_1}{b}\right) \geq \tfrac{1}{p} - (p^2 - p + 1) \operatorname{ord}_p(a) = -\tfrac{1}{p} \operatorname{ord}_p(a).$$

Then $\operatorname{ord}_p(y) > \operatorname{ord}_p(pa^{p-p^3})$ and so $\operatorname{ord}_p(z^p) = \operatorname{ord}_p(pa^{p-p^3}) = (1-p)/(p^2+1)$ by (5.2.3)(ii). It follows that

$$\operatorname{ord}_p(p^{p-1}z^{p^2}) = p - 2 + \frac{p+1}{p^2+1}. \tag{5.2.11}$$

Since (5.2.11) is positive, (5.2.3)(i) and (5.2.3)(iii) imply that

$$\operatorname{ord}_p(y) = \frac{1}{p} \operatorname{ord}_p(x) = \frac{1}{p^3} \operatorname{ord}_p(z) = -\frac{1}{p^4}\left(\frac{p-1}{p^2+1}\right). \tag{5.2.12}$$

By (5.2.11), if $p \geq 3$, the term $p^{p-1}z^{p^2}$ drops out of (5.2.3)(i) and then we deduce from (5.2.3) that $g_a(y) = y^{p^4} - y + p\lambda^{-p}s_1a^{p-p^3}$ is 0 in R_b. If $p = 2$, apply Lemma 2.6 to (5.2.3)(ii) to obtain $x^4 = y^8$ in R_c. Thus $z = y^{16}$ in R_c and it again follows that $g_a(y) = 0$ in R_b. Conversely, from y satisfying $g_a(y) = 0$

in R_b, we can find x and z such that (5.2.3) holds. The concluding arguments are analogous to those in the proof of Corollary 5.2.9. □

We have focused on x, y, z in Proposition 5.2.2 because, as we show next, distinct solutions to $f_a(Z) = 0$ in R_c differ by elements of $\boldsymbol{\mu}_{p^4-1}$.

Lemma 5.2.13. *Let Q_z lie in the fiber over $P_a \neq 0$. Then every other point in the same fiber has the form $Q_{z'}$ with $z' = z + \omega$ in R_c as ω ranges over $\boldsymbol{\mu}_{p^4-1}$. If so,*

$$y' = y + \omega^p \text{ in } R_b, \quad x' = x + \omega^{p^2} \text{ in } R_a \tag{5.2.14}$$

and $Q_{z'} = Q_z + \iota(P_{a'})$ with $a' = \omega^{p^2} a$ in $\mathfrak{R}_\lambda$.

Proof. We have $f_a(z) = 0$ in R_c and we use (5.2.3)(i) and (ii) to find y and x. Putting $z' = z + \omega$ and using (5.2.14) to define y' and x' gives another solution to the congruences (5.2.3), thereby accounting for the additional $p^4 - 1$ points $Q_{z'}$ in the fiber over P_a.

Let $Q_{z'} = Q_z + \iota(P_{a'})$ and evaluate the corresponding D_k-homomorphisms at e_5 to find the equation of Witt covectors $\mathbf{d}_a(z') = \mathbf{d}_a(z) \dotplus (\vec{0}, c', b', a')$. This sum reduces to ordinary addition on coordinates in k. Indeed, apply Verschiebung twice and use Lemma 2.7 to get $cz' = cz + c'$ and so $c' = \omega c$ in k. By Remark 5.1.4(iii), c' determines b' and a'. In particular, the various lifts satisfy

$$(-p)^{p+1} a' \equiv (c')^{p^2} \equiv \omega^{p^2} c^{p^2} \equiv (-p)^{p+1} \omega^{p^2} a \pmod{p^{p+2} \mathcal{O}_{\overline{K}}}.$$

Hence $a' = \omega^{p^2} a$ in k and similarly $b' = \omega^p b$ in k. □

The next lemmas treat special cases used in the following subsection to describe Kummer generators when $p = 2$.

Lemma 5.2.15. *If $P_a \neq 0$, then the field F_a of points of the fiber over P_a equals the full field of points $K(W)$ for the Honda parameters in* (5.2.16).

Proof. If $\mathbf{s} = [s_1 s_2 000]$, use the first form of $f_a(Z)$ in Proposition 5.2.2 with $w = s_2 a$. In the remaining cases below, $\epsilon_p = 0$ and the simpler equation for $f_a(Z)$ holds. Note that $f_{\eta a}(\eta^e Z) = \eta^e f_a(Z)$ for all η in $\boldsymbol{\mu}_{p^4-1}$, with e given by

$\mathbf{s}$	$[s_1 s_2 000]$	$[00 s_3 00]$	$[0000 s_5]$	$[000 s_4 0]$
e	$1-p^2$	p^3-p^2	$p-p^2$	0

. (5.2.16)

The correspondence between the roots of $f_a(Z)$ and those of $f_{\eta a}(Z)$ induced by $z \leftrightarrow \eta^e z$ shows that $F_{\eta a} = F_a$ and so each of these fields equals $K(W)$. □

Proposition 5.2.17. *If $\mathcal{W}$ is an extension of $\mathcal{E}_\lambda$ by $\mathcal{E}_\lambda$ killed by p and $L = K(W)$, then its abelian conductor exponent satisfies $\mathfrak{f}(L/F) \leq p^2$. Moreover, $\mathfrak{f}(F'/F) \leq p^2$ for every intermediate field F' of L/F.*

Proof. Let $\mathbf{s}(\mathcal{W}) = [s_1s_2s_3s_4s_5]$ and write $s_1 = \epsilon_p + \delta_p$, with $\delta_p = 0$ for odd primes p and $\delta_2 = (\lambda s_2)^2$. Then $\mathcal{W} = \mathcal{W}_1 + \cdots + \mathcal{W}_5$ is a Baer sum of group schemes corresponding to the sum of Honda parameters

$$[\epsilon_p 0000] + [\delta_p s_2 000] + [00s_3 00] + [000s_4 0] + [0000s_5], \tag{5.2.18}$$

some of which may be trivial. For the fiber fields $F_a^{(j)}$ of each of these W_j, we show that $\mathfrak{f}(F_a^{(j)}/F) \le p^2$ in the next lemmas. Since F_a is contained in the compositum of all $F_a^{(j)}$, we then have $\mathfrak{f}(F_a/F) \le p^2$ by Lemma C.9. Furthermore, L is the compositum of all F_a as P_a varies over E_λ, so $\mathfrak{f}(L/F) \le p^2$. Finally $\mathfrak{f}(F'/F) \le p^2$ because the upper ramification numbering behaves well for quotients. ☐

Remark 5.2.19. In contrast to the proposition, Fontaine's higher ramification bound leads to $\mathfrak{f}(L/F) \le p^2 + 2$ by Proposition C.12, since Proposition 5.1.1(ii) gives $e_{F/K} = e_F = (p^2+1)(p-1)$. In particular, when $p = 2$, the sharper bound is essential for our applications.

We next verify the lemmas needed for the proof of the Proposition. For $P_a \ne 0$ and f_a as in Proposition 5.2.2, recall that $F_a = F(Q_z)$, where $f_a(z) = 0$ in R_c. Let π_a be a uniformizer of F_a.

Lemma 5.2.20. *If* $\mathbf{s} = [000s_40]$, *then* F_a/F *is unramified of degree* 1 *or* p.

Proof. The claim follows from separability of $f_a(Z) = Z^{p^4} - Z + s_4$ over k. ☐

Lemma 5.2.21. *For the parameters* $\mathbf{s}$ *below*, F_a/F *is totally ramified of degree* p^4.

(i) *If* $\mathbf{s} = [s_10000]$ *with* $s_1 \ne 0$, *then* $\mathfrak{f}(F_a/F) = p^2 - 2p + 2$.

(ii) *Let* $\mathbf{s} = [s_1s_2s_3s_4s_5]$, *with* $s_2 \ne 0$. *Set* $s_1 = 0$ *for odd* p *and* $s_1 = (\lambda s_2)^2$ *for* $p = 2$. *Then* $\epsilon_p = 0$ *for all* p *and* $\mathfrak{f}(F_a/F) = p^2$.

(iii) *If* $\mathbf{s} = [00s_3s_40]$ *and* $s_3 \ne 0$, *then* $\mathfrak{f}(F_a/F) = p$.

(iv) *If* $\mathbf{s} = [000s_4s_5]$ *and* $s_5 \ne 0$, *then* $\mathfrak{f}(F_a/F) = p$.

Proof. To find the conductors, we determine t in F_a to which Proposition C.5 applies. In all cases below, $g(t) - t$ is in $\boldsymbol{\mu}_{p^4-1}$ for all $g \ne 1$ in $\mathrm{Gal}(F_a/F)$ by Lemma 5.2.13 and $F_a = F(t)$.

In case (i), let $F_a = F(\vartheta)$ as in Corollary 5.2.10 and let y be the image of ϑ in R_b. Observe that by (5.2.12), F_a/F is totally ramified of degree p^4 and we have $\mathrm{ord}_{\pi_a}(y) = \mathrm{ord}_p(y)\,\mathrm{ord}_{\pi_a}(p) = -(p-1)^2$. Using $t = y$ gives $\mathfrak{f}(F_a/F) = p^2 - 2p + 2$.

In the remaining cases, $\epsilon_p = 0$ and $F_a = F(\theta)$ as in Corollary 5.2.9, with θ a root of $\tilde{f}(Z) = 0$ in $\mathcal{O}_{\overline{K}}$ and $\tilde{f}$ a lift of the simpler version of f_a in Proposition 5.2.2. If z is the image of θ in R_c, then $p^4 \,\mathrm{ord}_p(z) = \mathrm{ord}_p(w) - p^2\,\mathrm{ord}_p(a)$ and so we have

case	(ii)	(iii)	(iv)
$\mathrm{ord}_p(z)$	$-\frac{p+1}{p^4(p^2+1)}$	$-\frac{1}{p^4(p^2+1)}$	$-\frac{1}{p^3(p^2+1)}$

In cases (ii) and (iii), observe that F_a is totally ramified of degree p^4 over F, with $\mathrm{ord}_{\pi_a}(z) = 1 - p^2$ and $1 - p$ respectively. We use $t = z$ to determine $\mathfrak{f}(F_a/F)$.

In case (iv), $w = s_5 a^p + s_4 a^{p^2}$. Choose $\beta \in \mathbb{W}^\times$ such that $\beta^p \equiv s_5 \pmod{p\mathbb{W}}$ and let $t = \theta^{p^3} + \beta a^{1-p}$. By Lemma 2.6, with O-notation from the start of Section 5,

$$t^p = \theta^{p^4} + s_5 a^{p-p^2} + O(\pi_a) = \theta - s_4 + O(\pi_a),$$

so $\mathrm{ord}_p(t) = 1/p\,\mathrm{ord}_p(\theta) = 1/(p^4(p^2+1))$. Hence the ramification index of $F(t)/F$ is at least p^4. Since $F(t) \subseteq F_a$ and $[F_a : F] \le p^4$, we have $F_a = F(t)$, totally ramified over F. If $g(z) = z + \omega$ as in Lemma 5.2.13, then

$$g(t) - t = g(\theta)^{p^3} - \theta^{p^3} \in (\theta + \omega + \pi_a \mathcal{O}_{\overline{K}})^{p^3} - \theta^{p^3} \subseteq \omega^{p^3} + \pi_a \mathcal{O}_{\overline{K}}.$$

Proposition C.5 therefore applies with $\mathrm{ord}_{\pi_a}(t) = 1 - p$ to give $\mathfrak{f}(F_a/F) = p$. □

5.3. *Local corners.* For this subsection, $p = 2$ and $K = \mathbb{Q}_2$. Let $\mathcal{E}$ be the simple group scheme $\mathcal{E}_\lambda$ of Notation 4.3, with $\lambda = 1$ necessarily. Let E be the Galois module of $\mathcal{E}$, $F = \mathbb{Q}_2(E)$ and $\Delta = \mathrm{Gal}(F/\mathbb{Q}_2)$. By Proposition 5.1.1, $F = \mathbb{Q}_2(\boldsymbol{\mu}_{15}, \varpi)$, with uniformizer ϖ satisfying $\varpi^5 = 2$. Fix a generator σ of the inertia subgroup of Δ and a Frobenius τ generating $\mathrm{Gal}(F/\mathbb{Q}(\varpi))$ with $\tau\sigma\tau^{-1} = \sigma^2$. Then $\Delta = \langle \sigma, \tau \rangle$ is isomorphic to the Frobenius group of order 20 and E is the unique nontrivial irreducible module over $\mathrm{R} = \mathbb{F}_2[\Delta]$.

Let W represent a class in $\mathrm{Ext}^1_{[2],\mathbb{Q}_2}(E, E)$, $L = \mathbb{Q}_2(W)$ and $\mathfrak{h} = \mathrm{Hom}_{\mathbb{F}_2}(E, E)$. Then $[W]$ corresponds to a cohomology class $[\psi]$ in $H^1(\mathrm{Gal}(L/\mathbb{Q}_2), \mathfrak{h})$ such that

$$\rho_W(g) = \begin{bmatrix} \rho_E(g) & \psi(g)\rho_E(g) \\ 0 & \rho_E(g) \end{bmatrix} \quad \text{for all } g \in \mathrm{Gal}(L/\mathbb{Q}_2), \tag{5.3.1}$$

as in (B.1). We introduce *corners* to rigidify ψ and facilitate comparison with the cocycles arising from global extensions.

Suppose that V is any finitely generated R-module and let $T_\sigma = \sigma^4 + \sigma^3 + \sigma^2 + \sigma + 1$ in R be the trace with respect to σ. Since σ has odd order, $V = V_0 \oplus V'$, where V_0 is the submodule on which σ acts trivially and $V' = \ker T_\sigma = (\sigma - 1)(V)$. The *corner subgroup* of V, which depends on the choice of τ, is defined as

$$\mathrm{Cor}(V) = \{v \in V \mid \tau(v) = v \text{ and } T_\sigma(v) = 0\}.$$

If $v_1, \dots, v_n$ is an $\mathbb{F}_2$-basis for $\mathrm{Cor}(V)$, then $\mathrm{R}v_i \simeq E$ and $V' = \bigoplus_{i=1}^n \mathrm{R}v_i$.

We consistently write P for the unique nonzero element of $\mathrm{Cor}(E)$, so $P = P_\varpi$ as in Proposition 5.1.1(iii) and $P, \sigma(P), \sigma^2(P), \sigma^3(P)$ is an $\mathbb{F}_2$-basis for E affording the matrix representations

$$s = \rho_E(\sigma) = \begin{bmatrix} 0&0&0&1 \\ 1&0&0&1 \\ 0&1&0&1 \\ 0&0&1&1 \end{bmatrix} \quad \text{and} \quad t = \rho_E(\tau) = \begin{bmatrix} 1&0&1&0 \\ 0&0&1&1 \\ 0&1&1&0 \\ 0&0&1&0 \end{bmatrix}. \tag{5.3.2}$$

We will also use the twisted action of $\mathbb{F}_{16}$ on E described in Remark 5.1.4. If a primitive fifth root of unity ζ in $\mathcal{O}_F$ is defined by $\sigma(\varpi) = \zeta\varpi$, then $\sigma(\alpha P) = \alpha\zeta P$ and $\tau(\alpha P) = \tau(\alpha) P$ for all α in $\mathbb{F}_{16}$.

The endomorphisms s and t belong to $\mathfrak{h}$, with respective minimal polynomials $s^4 + s^3 + s^2 + s + 1 = 0$ and $t^4 - 1 = 0$. We next describe $\mathfrak{h}$ as an R-module.

Lemma 5.3.3. *An $\mathbb{F}_2$-basis for $\mathfrak{h}_0 = \ker((\sigma - 1) \mid \mathfrak{h})$ is $1, s, s^2, s^3$, with τ acting on $\mathfrak{h}_0$ as one Jordan block. An $\mathbb{F}_2$-basis for* $\mathrm{Cor}(\mathfrak{h})$ *is t, t^2, t^3. We have $\mathfrak{h} \simeq \mathfrak{h}_0 \oplus_{j=1}^{3} \mathrm{R}t^j$, with each $\mathrm{R}t^j \simeq E$. The cohomology group $H^1(\Delta, \mathfrak{h})$ vanishes.*

Proof. The elements of $\mathfrak{h}_0$ are precisely the $\mathbb{F}_2[s]$-endomorphisms of E. Since E is a cyclic $\mathbb{F}_2[s]$-module, $\mathrm{End}_{\mathbb{F}_2[s]}(E) = \mathbb{F}_2[s] \simeq \mathbb{F}_{16}$. The action of τ on $\mathfrak{h}_0$ is the action of Frobenius on $\mathbb{F}_{16}$ and thus has one Jordan block. Similarly, the elements of $\mathrm{Cor}(\mathfrak{h})$ are $\mathbb{F}_2[t]$-endomorphisms of E, so contained in $\mathbb{F}_2[t]$. But only the linear combinations of t, t^2, t^3 are annihilated by the action of T_σ on $\mathfrak{h}$.

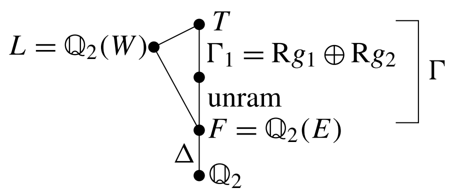
We have $H^1(\langle\tau\rangle, \mathfrak{h}_0) = H^1(\langle\tau\rangle, \mathbb{F}_{16}) = 0$ by the additive Hilbert Theorem 90 and $H^1(\langle\sigma\rangle, \mathfrak{h}) = 0$ because σ has odd order. Applying inflation-restriction with respect to the exact sequence $1 \to \langle\sigma\rangle \to \Delta \to \langle\tau\rangle \to 1$ shows that $H^1(\Delta, \mathfrak{h}) = 0$. □

Notation 5.3.4. For t as in (5.3.2), the following elements comprise $\mathrm{Cor}(\mathfrak{h})$. Their labels are consistent with Notation 6.1.2.

$$\begin{aligned} &\gamma_0 = 0, && \gamma_4 = t + t^2 + t^3, && \gamma_5 = t + t^3, && \gamma_9 = t^2, \\ &\gamma_{11} = t + t^2, && \gamma'_{11} = t^2 + t^3, && \gamma_{15} = t^3, && \gamma'_{15} = t. \end{aligned} \tag{5.3.5}$$

All occur as values of extension cocycles for E by E when we range over Honda parameters, see Proposition 5.3.12 below.

Motivated by the conductor bound in Proposition 5.2.17, we assume from now on that $\mathfrak{f}_\mathfrak{p}(L/F) \le 4$. If T is the maximal elementary 2-extension of F with ray class conductor exponent 4, then T is Galois over $\mathbb{Q}_2$ and we denote the action of δ in Δ on elements h of $\Gamma = \mathrm{Gal}(T/F)$ by ${}^{\delta}h = \tilde{\delta} h \tilde{\delta}^{-1}$ independent of the choice of lift $\tilde{\delta}$ of δ to $\mathrm{Gal}(T/\mathbb{Q}_2)$. We also write σ for an element of order 5 in $\mathrm{Gal}(T/\mathbb{Q}_2)$ projecting to σ in Δ. We have the following diagram of fields and Galois groups,



where Γ_1 is the wild ramification subgroup (see Appendix C) of Γ. We next describe the complete lower ramification filtration on Γ and its structure as a module for $\mathrm{R} = \mathbb{F}_2[\Delta]$.

Proposition 5.3.6. *Let $g_0 = \mathrm{Artin}(\varpi, T/F)$, $g_1 = \mathrm{Artin}(1+\varpi+\varpi^3, T/F)$ and $g_2 = \mathrm{Artin}(1+\varpi^3, T/F)$. Then $\Gamma = \mathrm{R}g_0 \oplus \mathrm{R}g_1 \oplus \mathrm{R}g_2 \simeq \mathbb{F}_2 \oplus E \oplus E$ and*

$$\Gamma_1 \rhd \Gamma_2 = \Gamma_3 \rhd \Gamma_4 = \{1\},$$

with $\Gamma_1 = \mathrm{R}g_1 \oplus \mathrm{R}g_2$ and $\Gamma_3 = \mathrm{R}g_2$. There is a Frobenius Φ of order 8 in $\mathrm{Gal}(T/\mathbb{Q}_2)$ projecting to τ in Δ and satisfying $\Phi\sigma\Phi^{-1} = \sigma^2$. In addition, $\mathrm{Gal}(T/\mathbb{Q}_2) = \Gamma_1 \rtimes H$ with $H = \langle\sigma, \Phi\rangle$.

Proof. We use the standard filtration $U_F^{(n)}$ on local units, see (C.1). The R-module structure of Γ follows from the class field theory isomorphism

$$\mathrm{Artin}(-, T/F) : F^\times/U_F^{(4)} F^{\times 2} \xrightarrow{\sim} \Gamma.$$

In particular, R acts trivially on the Frobenius g_0 of Γ, while $\mathrm{R}g_1$ and $\mathrm{R}g_2$ are isomorphic to E as R-modules. Since $\Gamma_1 = \mathrm{Artin}(U_F, T/F)$, we have $\Gamma_1 = \mathrm{R}g_1 \oplus \mathrm{R}g_2$ and similarly for Γ_2, using $U_F^{(2)} \subset U_F^{(3)} F^{\times 2}$. Note that

$$\Gamma_1 = \ker(T_\sigma \mid \Gamma) = \mathrm{Image}((\sigma - 1) \mid \Gamma).$$

There is a residue extension of degree 2 for T/F, so Frobenius Φ projecting to τ has order 8. Set $\Phi\sigma^3\Phi^{-1} = h\sigma$ for some h in Γ_1. By direct computation, $T_\sigma(h) = (h\sigma)^5 = (\Phi\sigma^3\Phi^{-1})^5 = 1$. Hence $h = {}^\sigma x/x$ for some x in Γ_1 and so $(x\Phi)\sigma^3(x\Phi)^{-1} = \sigma$. Replace Φ by $x\Phi$ to guarantee that $\Phi\sigma\Phi^{-1} = \sigma^2$. Then Δ acts trivially on Φ^4, so $\Phi^4 = g_0$. Since $H = \langle\sigma, \Phi\rangle$ is isomorphic to the Galois group of the maximal tame extension of F in T, we find that $\mathrm{Gal}(T/\mathbb{Q}_2)$ is a semidirect product of H by the normal subgroup Γ_1. □

Let $r_{T/L} : \mathrm{Gal}(T/\mathbb{Q}_2) \twoheadrightarrow \mathrm{Gal}(L/\mathbb{Q}_2)$ be the natural projection. Note that the inertia group $\mathrm{Gal}(L/F)_1$ of $\mathrm{Gal}(L/F)$ is the wild ramification subgroup $\mathrm{Gal}(L/\mathbb{Q}_2)_1$ of $\mathrm{Gal}(L/\mathbb{Q}_2)$.

Corollary 5.3.7. *The subgroup* $\overline{H} = r_{T/L}(\langle\sigma, \Phi\rangle)$ *of* $\mathrm{Gal}(L/\mathbb{Q}_2)$ *projects onto* Δ *in* $\mathrm{Gal}(F/\mathbb{Q}_2)$. *As* R*-modules*, $\mathrm{Gal}(L/F)_1 \simeq E^b$, *with* $0 \le b \le 2$.

(i) *If L/F is totally ramified, then* $\mathrm{Gal}(L/F) = \mathrm{Gal}(L/F)_1$ *and* $|\overline{H}| = 20$.

(ii) *Otherwise*, *L/F has residue degree* 2, $\mathrm{Gal}(L/F) \simeq \mathrm{Gal}(L/F)_1 \oplus \mathbb{F}_2$ *and $\overline{H}$ has order and exponent* 40.

Proof. That $\overline{H}$ projects onto Δ and that $\mathrm{Gal}(L/F)_1 = r_{T/L}(\Gamma_1)$ is the direct sum of at most 2 copies of E is immediate. Moreover, L/F is totally ramified if and only if $g_0 = \Phi^4$ is in $\ker r_{T/L}$. Thus $|\overline{H}| = 20$ in case (i) and 40 in case (ii). □

Since T contains $L = \mathbb{Q}_2(W)$, the cocycle ψ in (5.3.1) inflates to $\mathrm{Gal}(T/\mathbb{Q}_2)$. We may arrange for $\psi(\sigma) = 0$, since σ has odd order. Lemma 5.3.3 and (B.3) give injectivity of the restriction map:

$$0 \to H^1(\mathrm{Gal}(T/\mathbb{Q}_2), \mathfrak{h}) \xrightarrow{\mathrm{res}} H^1(\Gamma, \mathfrak{h})^\Delta = \mathrm{Hom}_{\mathrm{R}}(\Gamma, \mathfrak{h}) \tag{5.3.8}$$

and we say that $\chi = \mathrm{res}([\psi])$ in $\mathrm{Hom}_{\mathrm{R}}(\Gamma, \mathfrak{h})$ *belongs to* W. Note that χ is determined by its values on g_0, g_1, g_2, as defined in Proposition 5.3.6.

Lemma 5.3.9. *The field* $L = \mathbb{Q}_2(W)$ *is the fixed field of* $\ker\chi$. *Moreover*:

(i) $\chi(g_i)$ *is in* $\mathrm{Cor}(\mathfrak{h})$ *for* $i = 1, 2$ *and* $\chi(g_0)$ *is in* $\{0, I_4\}$.

(ii) *L/F is unramified if and only if* $\chi(g_1) = \chi(g_2) = 0$.

(iii) $\mathfrak{f}(L/F) = 4$ *if and only if* $\chi(g_2) \neq 0$. *If* $\chi(g_2) = 0$, *then* $\mathfrak{f}(L/F) = 0$ *or* 2.

(iv) *The residue degree of L/F is* 1 *or* 2, *according to whether* $\chi(g_0) = 0$ *or* I_4.

Proof. The matrix representation (5.3.1) shows that g in $\mathrm{Gal}(T/\mathbb{Q}_2)$ acts trivially on W if and only if g is in $\Gamma = \mathrm{Gal}(T/F)$ and $\chi(g) = 0$. Then items (i)–(iv) immediately follow from Proposition 5.3.6. In particular, (i) holds by considering the action of Δ on g_0, g_1 and g_2. □

Write $\mathcal{W}_{\mathbf{s}}$ for the extension of $\mathcal{E}$ by $\mathcal{E}$ of exponent 2 with Honda parameter $\mathbf{s}$ and $W_{\mathbf{s}}$ for its Galois module. Belonging to $W_{\mathbf{s}}$ are the cohomology class $[\psi_{\mathbf{s}}]$ in $H^1(\mathrm{Gal}(T/\mathbb{Q}_2), \mathfrak{h})$ and its restriction $\chi_{\mathbf{s}}$ in $\mathrm{Hom}_{\mathbb{F}_2[\Delta]}(\Gamma, \mathfrak{h})$, as described above. The rest of this section is devoted to evaluating $\chi_{\mathbf{s}}$ as $\mathbf{s}$ varies.

If h is in $\Gamma = \mathrm{Gal}(T/F)$ and Q_{z_j} is any point in the fiber over $\sigma^j(P)$, see Notation 5.2.8, any basis of the form

$$P, \sigma(P), \sigma^2(P), \sigma^3(P), Q_{z_0}, Q_{z_1}, Q_{z_2}, Q_{z_3} \tag{5.3.10}$$

yields the same matrix $\rho_{W_{\mathbf{s}}}(h)$ in (5.3.1). Moreover, $h(Q_{z_j}) = Q_{z_j} + \chi_{\mathbf{s}}(h)\sigma^j(P)$.

Let M/F be a finite elementary 2-extension. Define its *Kummer group* by

$$\boldsymbol{\kappa}(M/F) = F^\times \cap M^{\times 2} \quad \text{and let} \quad \bar{\boldsymbol{\kappa}}(M/F) = \boldsymbol{\kappa}(M/F)/F^{\times 2}.$$

By definition, $F^{\times 2} \subseteq \boldsymbol{\kappa}(M/F)$ and we have $M = F(\{\sqrt{\theta} \mid \theta \in \boldsymbol{\kappa}(M/F)\})$. Kummer theory gives a perfect pairing

$$\mathrm{Gal}(M/F) \times \bar{\boldsymbol{\kappa}}(M/F) \to \boldsymbol{\mu}_2 \quad \text{by } (g, \theta) \mapsto g(\sqrt{\theta})/\theta.$$

Lemma 5.3.11. *Let $P = P_\varpi$ and let F_ϖ be the subfield of L generated by the points of $W_{\mathbf{s}}$ in the fiber over P. If $\mathbf{s} = [10000]$, then $\boldsymbol{\kappa}(F_\varpi/F)$ contains $1 + 2\varpi^4$. If $s_1 = s_2$, then $\boldsymbol{\kappa}(F_\varpi/F)$ contains $1 + 2s_2\varpi^2 + 2(s_3 + s_5)\varpi^4$.*

Proof. Refer to Proposition 5.2.2. Since $p = 2$ and $\lambda = 1$, we have $\epsilon_2 = 0$ when $s_1 = s_2$. Then take the square class of the discriminant of the polynomial $h(X)$ in Corollary 5.2.9. Similarly, use Corollary 5.2.10 when $s = [10000]$. □

We first determine $\chi_{\mathbf{s}}$ when L/F is a nontrivial totally ramified extension. For compatibility with the notation for decomposition groups in Section 6, where we consider global Galois module extensions of E by E, set $\mathcal{D}_{\mathfrak{p}}(L/F) = \mathrm{Gal}(L/F)$.

Proposition 5.3.12. *If L/F is totally ramified, then $\chi_{\mathbf{s}}(g_0) = 0$. Depending on the conductor exponent $\mathfrak{f}(L/F)$, we have:*

(i) $\underline{\mathfrak{f}(L/F) = 2}$. *Then $|\mathcal{D}_{\mathfrak{p}}(L/F)| = 16$, $\chi_s(g_2) = 0$ and*

$\mathbf{s}$	[00001]	[00100]	[10000]	[10101]	[00101]	[10001]	[10100]
$\chi_{\mathbf{s}}(g_1)$	γ_{15}	γ'_{15}	γ_9	γ_4	γ_5	γ'_{11}	γ_{11}

(ii) $\underline{\mathfrak{f}(L/F) = 4 \text{ and } |\mathcal{D}_{\mathfrak{p}}(L/F)| = 16}$. *Then $\chi_{\mathbf{s}}(g_2) = \gamma_9$ and $\chi_{\mathbf{s}}(g_1) = 0$ or γ_9 according to whether $\mathbf{s} = [11000]$ or $[01000]$.*

(iii) $\mathfrak{f}(L/F) = 4$ *and* $|\mathcal{D}_\mathfrak{p}(L/F)| = 256$. *Then* $\chi_s(g_2) = \gamma_9$ *and*

$\mathbf{s}$	[11001]	[11100]	[01101]	[11101]	[01001]	[01100]
$\chi_\mathbf{s}(g_1)$	γ_{15}	γ'_{15}	γ_4	γ_5	γ'_{11}	γ_{11}

Proof. We begin with some basic Honda parameters, from which the others can be generated by Baer sum. Recall that F_a denotes the extension of F obtained by adjoining the coordinates of the points in the fiber of $W_\mathbf{s}$ above one point P_a of order 2 in E.

Basic cases: (1) $\mathbf{s} = [00001]$, [00100] or [10000]. By Lemma 5.2.21, F_a/F is totally ramified of degree 16 and $\mathfrak{f}(F_a/F) = 2$. Thus $\chi_\mathbf{s}(g_0) = \chi_\mathbf{s}(g_2) = 0$ by Lemma 5.3.9 and so $L = F_a$ is the subfield of T fixed by $\mathrm{R}g_0 \oplus \mathrm{R}g_2$ independent of a.

(2) $\mathbf{s} = [11000]$. Lemma 5.2.15 indicates that $L = F_a$ does not depend on a. Now L/F is totally ramified of degree 16 and $\mathfrak{f}(L/F) = 4$ by Lemma 5.2.21, so $\chi_\mathbf{s}(g_0) = 0$ but $\chi_\mathbf{s}(g_2) \neq 0$. By Lemma 5.3.11, the Kummer group $\bar{\boldsymbol{\kappa}}(L/F)$ contains the coset $\kappa = (1+2\varpi^2)F^{\times 2}$ and therefore equals $\mathrm{R}\kappa$. By evaluating the pairing of Kummer theory and class field theory given by Hilbert symbols, we find that g_1 acts trivially on the square roots of elements of $\bar{\boldsymbol{\kappa}}(L/F)$, so $\chi_\mathbf{s}(g_1) = 0$.

Set $h = g_1$ in the basic case (1) and $h = g_2$ in (2). Recall that the primitive fifth root of unity ζ is defined by $\sigma(\varpi) = \zeta\varpi$. To find the matrix $\chi_\mathbf{s}(h)$, we use a basis for $W_\mathbf{s}$ of the form

$$P, \sigma(P), \sigma^2(P), \sigma^3(P), Q_{z_0}, Q_{z_1}, Q_{z_2}, Q_{z_3},$$

where z_j is a root of the Honda polynomial $f_{\zeta^j\varpi}$, see Notation 5.2.8. The action of $\Delta = \mathrm{Gal}(F/\mathbb{Q}_2)$ puts h in the corner group of $\mathcal{D}_\mathfrak{p}(L/F)$, so $\chi_\mathbf{s}(h)$ is in $\mathrm{Cor}(\mathfrak{h})$ and therefore equals one of the matrices in (5.3.5). In particular, $\chi_\mathbf{s}(h)(P) = \alpha_0 P$, with $\alpha_0 = 0$ or 1. Write $h(Q_{z_j}) = Q_{z_j} + \alpha_j P$, where $\alpha_0 = 0$ or 1 and

$$\alpha_j = c_{0j} + c_{1j}\zeta + c_{2j}\zeta^2 + c_{3j}\zeta^3 \text{ in } \mathbb{Z}[\zeta], \quad \text{for } 1 \le j \le 3.$$

Then the $(j+1)$-column of the matrix $\chi_\mathbf{s}(h)$ is $[c_{0j}, c_{1j}, c_{2j}, c_{3j}]^T \bmod 2$ by (5.3.10).

From $h(Q_{z_0}) = Q_{z_0} + \alpha_0 P$, we get $h(z_0) = z_0 + \alpha_0$ by Lemma 5.2.13. In the proof of Lemma 5.2.15, we showed that there is a correspondence between roots of f_ϖ and $f_{\zeta^j\varpi}$, allowing us to choose $z_j = \zeta^{je} z_0$, with e given by (5.2.16) and $j = 1, 2, 3$. Then $h(z_j) = z_j + \alpha_0\zeta^{je}$ in R_c. Since h is not trivial on L, we have $\alpha_0 = 1$. Further use of Lemma 5.2.13 gives

$$h(Q_{z_j}) = Q_{z_j} + \zeta^{4je} P_{\zeta^j\varpi} = Q_{z_j} + \zeta^{(1-e)j} P.$$

This determines $\chi_\mathbf{s}(h)$ for all $\mathbf{s}$ in the basic cases.

Remaining cases. Write $\mathbf{s} = \mathbf{t} + \mathbf{u}$, choosing Honda parameters $\mathbf{t}$ and $\mathbf{u}$ already treated above. Then $W_\mathbf{s}$ is the Baer sum of $W_\mathbf{t}$ and $W_\mathbf{u}$ and $\chi_\mathbf{s} = \chi_\mathbf{t} + \chi_\mathbf{u}$.

In (ii), use $[01000] = [11000] + [10000]$. In (i), the last three entries follow by varying $\mathbf{t}$ and $\mathbf{u}$ among first three entries. Use $[10101] = [10000] + [00101]$ to complete (i). For (iii), let $\mathbf{t} = [11000]$ and let $\mathbf{u}$

run over the Honda parameters in (i), omitting [10000]. Since g_1 and g_2 are independent and nontrivial on L, we have $\mathrm{Gal}(L/F) = Rg_1 \oplus Rg_2$ of order 256. □

We briefly treat the remaining 16 nontrivial Honda parameters, even though Lemma 6.1.14 shows that they are not needed for our global applications.

Proposition 5.3.13. *If L/F is not totally ramified, then $\mathbf{s} = \mathbf{t} + \mathbf{u}$, where $\mathbf{t}$ ranges over* [00000] *and the* 15 *Honda parameters in* Proposition 5.3.12, *while* $\mathbf{u} =$ [00010]. *Then $\chi_{\mathbf{s}}(g_0) = I_4$, $\chi_{\mathbf{s}}(g_j) = \chi_{\mathbf{t}}(g_j)$ for $j = 1, 2$ and $\mathbb{Q}_2(W_{\mathbf{s}})$ is the compositum of $\mathbb{Q}_2(W_{\mathbf{t}})$ and the unramified quadratic extension of F.*

Proof. By Lemma 5.2.20, $F(W_{\mathbf{u}})$ is the splitting field of $Z^{16} - Z - 1$, namely the unramified quadratic extension of F. Thus $\chi_{\mathbf{u}}(g_0) = I_4$ and $\chi_{\mathbf{u}}(g_1) = \chi_{\mathbf{u}}(g_2) = 0$ by Lemma 5.3.9. The rest follows from $\chi_{\mathbf{s}} = \chi_{\mathbf{t}} + \chi_{\mathbf{u}}$. □

6. Global conclusions

6.1. *Favorable abelian surfaces.* There are two irreducible $\mathcal{S}_5$-representations of dimension 4 over $\mathbb{F}_2$. Denote the one taking transpositions to transvections by $\iota : \mathcal{S}_5 \to \mathrm{SL}_4(\mathbb{F}_2)$ and fix it by sending $(12) \mapsto r$ and $(12345) \mapsto s$, where

$$r = \begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{bmatrix} \quad \text{and} \quad s = \begin{bmatrix} 0&0&0&1 \\ 1&0&0&1 \\ 0&1&0&1 \\ 0&0&1&1 \end{bmatrix}. \quad \text{Let } t = \begin{bmatrix} 1&0&1&0 \\ 0&0&1&1 \\ 0&1&1&0 \\ 0&0&1&0 \end{bmatrix}. \tag{6.1.1}$$

The image of ι is isomorphic to the odd orthogonal group $\mathrm{O}_4^-(\mathbb{F}_2) \subset \mathrm{Sp}_4(\mathbb{F}_2)$. In addition, $\iota((2354)) = t$ and $\Delta = \langle s, t \rangle$ is the Frobenius group of order 20.

Fix a favorable quintic field F_0 with discriminant $d_{F_0/\mathbb{Q}} = \pm 16N$ and Galois closure F. Proposition 1.2(i) implies that the inertia group $\mathcal{I}_v(F/\mathbb{Q})$ at each place $v \mid N$ is generated by a transposition σ_v when we identify $\mathrm{Gal}(F/\mathbb{Q})$ with $\mathcal{S}_5$. In this section, E is the Galois module giving $\rho_E : \mathrm{Gal}(F/\mathbb{Q}) = \mathcal{S}_5 \xrightarrow{\iota} \mathrm{SL}_4(\mathbb{F}_2)$. Using the matrices r, s, t in (6.1.1), σ_v is conjugate to $\rho_E^{-1}(r)$, inertia at a some $\mathfrak{p} \mid 2$ is generated by $\sigma = \rho_E^{-1}(s)$ and $\tau = \rho_E^{-1}(t)$ is a Frobenius in the decomposition group $\mathcal{D}_{\mathfrak{p}}(F/\mathbb{Q}) = \langle \sigma, \tau \rangle$. Hence the restriction of ρ_E to $\mathcal{D}_{\mathfrak{p}}(F/\mathbb{Q})$ agrees with the representation ρ_{E_λ} of Definition 4.1, as normalized in (5.3.2). By Corollary 5.1.5, E extends to a group scheme $\mathcal{E}$ over $\mathbb{Z}[\frac{1}{N}]$. Let $\underline{E}$ be the Σ-category introduced in Definition 3.4 with $\Sigma = \{\mathcal{E}\}$. This subsection is devoted to criteria for the validity of axiom **E4** in Theorem 3.7, needed to prove Theorem 6.1.22.

To treat extensions W of E by E of exponent 2, let $\mathcal{P} = \mathcal{P}_{E,E}$ be the parabolic group as in (B.2). We describe subgroups of $\mathcal{P}$ in which the relevant representations ρ_W take their values.

Notation 6.1.2. Let $c : \mathrm{Mat}_4(\mathbb{F}_2) \to \mathcal{P}$ by $c(m) = \left[\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right]$ and $d : \mathcal{S}_5 \to \mathcal{P}$ by $d(g) = \left[\begin{smallmatrix} \iota(g) & 0 \\ 0 & \iota(g) \end{smallmatrix}\right]$. Let G_0 be the image of d. With γ_a as in 5.3.4 and $\mathrm{S} = \mathbb{F}_2[\mathcal{S}_5]$, we define S-submodules of $\mathrm{Mat}_4(\mathbb{F}_2) = \mathrm{End}(E)$ with adjoint action of $\mathcal{S}_5$

$$\Gamma_4 = \mathrm{S}\gamma_4, \quad \Gamma_5 = \mathrm{S}\gamma_5, \quad \Gamma_9 = \mathrm{S}\gamma_9, \quad \Gamma_{11} = \mathrm{S}\gamma_{11}, \quad \Gamma_{15} = \mathrm{S}\gamma_{15}. \tag{6.1.3}$$

Let $G_a =< G_0, c(\gamma_a) >= c(\Gamma_a) \rtimes G_0$.

The radical of G_a equals $c(\Gamma_a)$ and has size 2^a. The abelianization of G_a is cyclic of order 2 and so defines the character $\epsilon_0 : G_a \to \mathbb{F}_2$, generalizing the additive signature on $\mathcal{S}_5$. If $a = 0$ or 4, all automorphisms of G_a are inner. The center of the other G_a's is generated by $c(1)$ and there is an automorphism

$$\epsilon : G_a \to G_a \quad \text{by} \quad \epsilon(g) = gc(1)^{\epsilon_0(g)}. \tag{6.1.4}$$

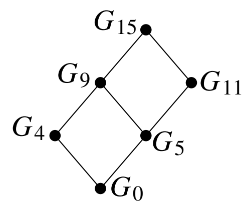
When $a = 5$ or 9, $\mathrm{Aut}(G_a)$ is generated by ϵ, modulo automorphisms induced from conjugation by elements of the normalizer of G_a in $\mathcal{P}$.

The corner group of an $\mathbb{F}_2[\Delta]$-module consists of the elements fixed by t and annihilated by the trace T_s. Using Magma, we find the nonzero corners of Γ_a.

a	4	5	9	11	15
$\mathrm{Cor}(\Gamma_a) - \{\gamma_0\}$	$\{\gamma_4\}$	$\{\gamma_5\}$	$\{\gamma_4, \gamma_5, \gamma_9\}$	$\{\gamma_5, \gamma_{11}, \gamma'_{11}\}$	$\{\text{all } \gamma_i\}$

(6.1.5)

Inclusions among the groups G_a follow from this table and are indicated in the Hasse diagram by ascending lines.



(6.1.6)

Moreover, G_9 is isomorphic to the fiber product of G_4 and G_5 over G_0 and similarly for the other parallelograms. When an inclusion $G_b \subset G_a$ exists, Magma extends the identity on G_0 to a surjection $f_{a,b} : G_a \twoheadrightarrow G_b$ sending γ_a to γ_b.

Definition 6.1.7. An involution g in a group H is *good* if its conjugates generate H. If g is good in $H \subseteq \mathcal{P}$ and $\mathrm{rank}(g - 1) = 2$, then g is *very good.*

Remark 6.1.8. A Magma verification shows that each G_a has a unique conjugacy class of very good involutions, represented by $d(r)$ with r as in (6.1.1).

Proposition 6.1.9. *Let L be an elementary 2-extension of $F = \mathbb{Q}(E)$, Galois over $\mathbb{Q}$, with L/F unramified outside $\{2, \infty\}$ and $\mathfrak{f}_\mathfrak{p}(L/F) \le 4$ for all $\mathfrak{p} \mid 2$. Then*:

(i) *The maximal subfield of L abelian over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{N^*})$, with $N^* = \pm N \equiv 5(8)$.*

(ii) *For $v \mid N$, inertia $\mathcal{I}_v(L/\mathbb{Q})$ is generated by a good involution in* $\mathrm{Gal}(L/\mathbb{Q})$.

Proof. By Proposition 1.2, F contains $\sqrt{N^*}$. For $v \mid N$, the inertia group $\mathcal{I}_v(F/\mathbb{Q})$ has order 2. Since L/F is unramified, $\mathcal{I}_v(L/\mathbb{Q})$ is generated by an involution σ_v. Intermediate fields $L \supseteq F' \supseteq F$ satisfy $\mathfrak{f}_\mathfrak{p}(F'/F) \le \mathfrak{f}_\mathfrak{p}(L/F) \le 4$. But Lemma C.6 implies that $\mathfrak{f}_\mathfrak{p}(F(i)/F) = 6$ and $\mathfrak{f}_\mathfrak{p}(F(\sqrt{\pm 2})/F) = 11$, so $L \cap F(i, \sqrt{2}) = F$. Since $L/\mathbb{Q}$ is unramified outside $\{2, N, \infty\}$, item (i) follows from Kronecker–Weber. The subfield of L fixed by the normal closure of σ_v is unramified outside $\{2, \infty\}$ and is contained in $\mathbb{Q}(i)$ by [Brumer and Kramer 2001], so equals $\mathbb{Q}$. Thus (ii) holds. ☐

Corollary 6.1.10. *For* $[W]$ *in* $\mathrm{Ext}^1_{[2],\mathbb{Q}}(E,E)$, *assume that* $L=\mathbb{Q}(W)$ *satisfies the hypotheses in the proposition and* $\operatorname{rank}\rho_W(\sigma_v-1)=2$. *Then* $\rho_W(\mathrm{Gal}(L/\mathbb{Q}))$ *is one of the groups* G_a, *up to conjugation in* $\mathcal{P}$. *If* $[\mathcal{W}]$ *is in* $\mathrm{Ext}^1_{[2],\underline{E}}(\mathcal{E},\mathcal{E})$, *then* $\mathrm{Gal}(\mathbb{Q}(\mathcal{W})/\mathbb{Q})$ *is conjugate to some* G_a.

Proof. By the Proposition $\rho_W(\sigma_v)$ is good and so is very good by assumption. Magma verifies that the G_a represent the six conjugacy classes of subgroups of $\mathcal{P}$ that project onto $\mathcal{S}_5$ and admit very good involutions. If $[\mathcal{W}]$ is a class in $\mathrm{Ext}^1_{[2],\underline{E}}(\mathcal{E},\mathcal{E})$, then the Proposition applies to $L=\mathbb{Q}(W)$, since $\mathfrak{f}_{\mathfrak{p}}(L/F)\le 4$ by Proposition 5.2.17 and $\operatorname{rank}\rho_W(\sigma_v-1)=2$ by **E3** of Definition 3.4. □

Definition 6.1.11. A class $[W]$ in $\mathrm{Ext}^1_{[2],\mathbb{Q}}(E,E)$ with $L=\mathbb{Q}(W)$ is a G_a*-class* if L/F is unramified outside $\{2,\infty\}$, $\mathfrak{f}_{\mathfrak{p}}(L/F)\le 4$ for $\mathfrak{p}\mid 2$ and $\operatorname{rank}\rho_W(\sigma_v-1)=2$, so that $\rho_W(\mathrm{Gal}(L/\mathbb{Q}))=G_a$ for some a by the corollary.

Lemma 6.1.12. *Let* $[W]$ *be a* G_a*-class with* $L=\mathbb{Q}(W)$.

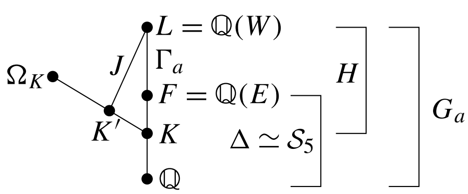
(i) *If* $[W']$ *is a* $G_{a'}$*-class, with* $L'=\mathbb{Q}(W')$, *then the Baer sum* $[W'']=[W]+[W']$ *is a* G_b*-class for some* b.

(ii) *If* $f_{a,b}:G_a\twoheadrightarrow G_b$ *exists in* (6.1.6), *then the Galois module for* $f_{a,b}\rho_W$ *represents a* G_b*-class.*

Proof. In (i), $[W]$ and $[W']$ correspond to classes $[\psi]$ and $[\psi']$ in $H^1(G_{\mathbb{Q}},\mathfrak{h})$ as in (B.1) and $[W'']$ belongs to the class of $\psi''=\psi+\psi'$. Since $L''=\mathbb{Q}(W'')$ is a subfield of the compositum LL', the ramification properties required of L'' in Definition 6.1.11 hold. Proposition 6.1.9 shows that $\rho(\sigma_v)$ is a good involution in G_a and so is very good, conjugate to $d(r)$ by Remark 6.1.8. Similarly for $\rho_{W'}(\sigma_v)$ in $G_{a'}$. Hence the representatives ψ and ψ' can be chosen to satisfy $\psi(\sigma_v)=\psi'(\sigma_v)=0$. We now have $\psi''(\sigma_v)=0$ and so $\operatorname{rank}\rho_{W''}(\sigma_v-1)=2$. By Corollary 6.1.10, $[W'']$ is a G_b-class for some b.

For (ii), let L' be the subfield of L fixed by $\rho_W^{-1}(\ker f_{a,b})$. Then $f_{a,b}\rho_W$ induces an isomorphism $\rho':\mathrm{Gal}(L'/\mathbb{Q})\to G_b$. The required ramification conditions hold for the subfield L' of L. As above, $\rho'(\sigma_v\mid L')$ is a good involution in G_b. Since $f_{a,b}$ is the identity on G_0 and $\rho_W(\sigma_v)$ is conjugate to $d(r)$ in G_0 so is $\rho'(\sigma_v\mid L')$. □

Let $K=\mathbb{Q}(r_1+r_2)$ be a pair-resolvent field for $F=\mathbb{Q}(E)$, as defined before Theorem 1.3, namely the fixed field of $\mathrm{Sym}\{1,2\}\times\mathrm{Sym}\{3,4,5\}$. Let $\Omega_K=\Omega_K^{(4)}$ be the maximal elementary 2-extension of K of modulus $\mathfrak{p}^4\infty$, where $\mathfrak{p}$ is the unique prime over 2 in K and ∞ allows ramification at all archimedean places. Refer to the following diagram of fields and Galois groups.



To simplify notation, also write $\mathfrak{p}$ for a place over 2 in L and for the restrictions of $\mathfrak{p}$ to subfields of L. Note that primes over 2 are unramified in F/K. Suppose that L is the Galois closure of $K'/\mathbb{Q}$. By

Lemma C.11 with M, F, K', K_1 and K there equal to the respective $\mathfrak{p}$-adic completions of L, F, K', K and $\mathbb{Q}$ here, $\mathfrak{f}_{\mathfrak{p}}(K'/K) = \mathfrak{f}_{\mathfrak{p}}(L/F)$.

Proposition 6.1.13. *Let K be a pair-resolvent of F. There is a bijection*

$$\{G_a\text{–classes } [W] \text{ with } a \in \{4,5,9\}\} \leftrightarrow \{\text{subfields } K' \subseteq \Omega_K \text{ quadratic over } K\}$$

such that $\mathbb{Q}(W)$ is the Galois closure of $K'/\mathbb{Q}$.

Proof. For $v \mid N$, $\mathcal{I}_v(F/K)$ acts on the left cosets of $\mathrm{Gal}(F/K)$ in $\mathrm{Gal}(F/\mathbb{Q})$ with four fixed points and three orbits of size 2. Thus $(N)\mathcal{O}_K = \mathfrak{a}\mathfrak{b}^2$ where $\mathfrak{a}$ and $\mathfrak{b}$ are square-free, relatively prime ideals of $\mathcal{O}_K$ of absolute norms N^4 and N^3 respectively.

Let $[W]$ be a G_a-class with a in $\{4,5,9\}$, $L = \mathbb{Q}(W)$ and $\rho_W : \mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\sim} G_a$. Then $H = \mathrm{Gal}(L/K)$ is the inverse image under $\pi : G_a \twoheadrightarrow \mathcal{S}_5$ of $\mathrm{Gal}(F/K)$. Choose $v \mid N$ so that if σ_v generates $\mathcal{I}_v(L/\mathbb{Q})$, then $\pi(\rho_W(\sigma_v)) = (12)$. By assumption $g = \rho_W(\sigma_v)$ is very good in G_a. Magma shows that among the subgroups of index 2 in H, exactly one, say J, has the property that the action of G_a on G_a/J is faithful and g has exactly 8 fixed points in this action. Hence $K' = L^J$ is a stem field for L and in view of the factorization of $(N)\mathcal{O}_K$, no prime over N ramifies in K'/K. If $v' \mid N$ is any other choice such that $\pi(\rho_W(\sigma_{v'})) = (12)$, then $\sigma_{v'}$ is conjugate to σ_v in H and therefore gives the same J, so also the same K'. Since $\mathfrak{f}_{\mathfrak{p}}(K'/K) = \mathfrak{f}_{\mathfrak{p}}(L/F) \le 4$ by definition of a G_a-class, K' is contained in Ω_K.

Conversely, let K' be a subfield of Ω_K quadratic over K, L the Galois closure of $K'/\mathbb{Q}$, $G = \mathrm{Gal}(L/\mathbb{Q})$, $H = \mathrm{Gal}(L/K)$ and $J = \mathrm{Gal}(L/K')$. Then L properly contains F, since each quadratic extension of K in F ramifies at some prime over N. By Proposition 6.1.9(ii), σ_v is a good involution in G. Since no prime over N ramifies in K'/K, the action of σ_v on G/J has eight fixed points. The following group-theoretic properties of G have been established:

(i) There is a surjection $\pi : G \to \mathcal{S}_5$ whose kernel has exponent 2 and is the radical of G.

(ii) The abelianization of G has order 2.

(iii) If H is the inverse image under π of the centralizer of a transposition in $\mathcal{S}_5$, then there is a subgroup J of index 2 in H such that the action of G on G/J is faithful.

(iv) There is a good involution g in G whose action on G/J has 8 fixed points.

We have (i) since the radical of $\mathrm{Gal}(L/\mathbb{Q})$ is $\mathrm{Gal}(L/F)$ and (ii) by Proposition 6.1.9(i).

In the Magma database of 1117 transitive groups of degree 20 only three satisfy (i)–(iv), namely G_a with a in $\{4,5,9\}$. Furthermore, if J is the stabilizer in $\mathcal{S}_{20}$ of any letter, then there is a unique conjugacy class of good involutions g in G such that g acts on G/J with exactly 8 fixed points. By applying this construction to $G = \mathrm{Gal}(L/\mathbb{Q})$, there is an isomorphism $\rho : \mathrm{Gal}(L/\mathbb{Q}) \to G_a$ such that $\rho(\sigma_v)$ is conjugate to g and has 8 fixed points when acting on $G_a/\rho(J)$. Computation now shows the following. If $a = 4$, then $\rho(\sigma_v)$ is conjugate to $d(r)$. If a is in $\{5,9\}$, then $\rho(\sigma_v)$ is conjugate to $d(r)$ or $d(r)\epsilon(r)$ where ϵ is the automorphism of (6.1.4). In the latter case, replace ρ by $\epsilon \circ \rho$. If W is the associated Galois module, then its class is a G_a-class. Because any automorphism of G_a preserving the conjugacy class of $d(r)$ is conjugation by an element of $\mathcal{P}$, the class $[W]$ is unique. □

Unless otherwise stated, $[W]$ now denotes a G_a-class and $L = \mathbb{Q}(W)$. Thus W represents a class in $\mathrm{Ext}^1_{R'}(\mathcal{E}, \mathcal{E})$, where $R' = \mathbb{Z}\big[\frac{1}{2N}\big]$. By the Mayer–Vietoris sequence (2.2), W prolongs to a group scheme $\mathcal{W}$ over $R = \mathbb{Z}\big[\frac{1}{N}\big]$ if and only if the image of $[W]$ in $\mathrm{Ext}^1_{\mathbb{Q}_2}(\mathcal{E}, \mathcal{E})$ agrees with that of a class from $\mathrm{Ext}^1_{\mathbb{Z}_2}(\mathcal{E}, \mathcal{E})$. If so, the other conditions in Definition 6.1.11 guarantee that $[\mathcal{W}]$ is in $\mathrm{Ext}^1_{\underline{E}}(\mathcal{E}, \mathcal{E})$. Recall that $\mathfrak{h} = \mathrm{Hom}_{\mathbb{F}_2}(E, E)$ and let $\psi : G_{\mathbb{Q}} \to \mathfrak{h}$ represent the class in $H^1(G_{\mathbb{Q}}, \mathfrak{h})$ associated to $[W]$, as in (B.1). Recall that at $\mathfrak{p} \mid 2$, the decomposition group $\mathcal{D}_{\mathfrak{p}}(F/\mathbb{Q})$ is isomorphic to $\Delta = \langle s, t\rangle$.

Lemma 6.1.14. *As a Δ-module, $\mathcal{D}_{\mathfrak{p}}(L/F)$ is isomorphic to E^b with $b \le 2$.*

Proof. We may assume $\mathcal{D}_{\mathfrak{p}}(L/F) \neq 1$. Computation shows that G_a contains no subgroup of order *and* exponent 40 whose projection to $\mathcal{S}_5$ has order 20. Conclude by using Proposition 5.3.6 and its Corollary 5.3.7. □

Remark 6.1.15. Let $[\psi]$ in $H^1(G_{\mathbb{Q}}, \mathfrak{h})$ correspond to the G_a-class $[W]$ and write $\psi_{|\mathcal{D}_{\mathfrak{p}}}$ for the restriction to the decomposition group $\mathcal{D}_{\mathfrak{p}}$ in $G_{\mathbb{Q}}$ at a fixed place $\mathfrak{p}$ over 2. The classes $[\mathcal{W}_{\mathbf{s}}]$ in $\mathrm{Ext}^1_{\mathbb{Z}_2}(\mathcal{E}, \mathcal{E})$ are classified by their Honda parameters $\mathbf{s}$ in $(\mathbb{F}_2)^5$. Let $[\psi_{\mathbf{s}}]$ in $H^1(G_{\mathbb{Q}_2}, \mathfrak{h})$ correspond to $[W_{\mathbf{s}}]$. Then $[W]$ is compatible with $[W_{\mathbf{s}}]$ if and only if:

$$[\psi_{|\mathcal{D}_{\mathfrak{p}}}] = [\psi_{\mathbf{s}}] \text{ in } H^1(G_{\mathbb{Q}_2}, \mathfrak{h}) \text{ for some Honda parameter } \mathbf{s}. \tag{6.1.16}$$

Let $F_{\mathfrak{p}}$ be the completion of F at $\mathfrak{p}$ and T the maximal elementary 2-extension of $F_{\mathfrak{p}}$ having conductor exponent 4. By Proposition 5.2.17, $\mathbb{Q}_2(W_{\mathbf{s}})$ is contained in T, while the completion $L_{\mathfrak{p}}$ is contained in T by definition of a G_a-class. In the diagram below, inflation is injective and restriction is injective by (5.3.8):

$$\begin{array}{ccccc} & & H^1(\mathcal{D}_{\mathfrak{p}}, \mathfrak{h}) & & \\ & & \big\downarrow \mathrm{inf} & & \\ 0 & \longrightarrow & H^1(\mathrm{Gal}(T/\mathbb{Q}_2), \mathfrak{h}) & \xrightarrow{\mathrm{res}} & \mathrm{Hom}_{\mathbb{F}_2[\Delta]}(\mathrm{Gal}(T/F_{\mathfrak{p}}, \mathfrak{h})). \end{array} \tag{6.1.17}$$

Hence, it suffices to compare the image χ of $[\psi_{|\mathcal{D}_{\mathfrak{p}}}]$ with the image $\chi_{\mathbf{s}}$ of $[\psi_{\mathbf{s}}]$ in $\mathrm{Hom}_{\mathbb{F}_2[\Delta]}(\mathrm{Gal}(T/F_{\mathfrak{p}}), \mathfrak{h})$. Note that the values of χ and $\chi_{\mathbf{s}}$ are corners in $\mathfrak{h}$. See Proposition 5.3.6 for specific generators g_0, g_1, g_2 of Γ as an $\mathbb{F}_2[\Delta]$-module. In particular, $\chi(g_0) = 0$ by Lemmas 6.1.14 and 5.3.9(iii). Thus W prolongs to a group scheme over $R = \mathbb{Z}\big[\frac{1}{N}\big]$ exactly if there is a Honda parameter $\mathbf{s}$ in Proposition 5.3.12 satisfying $\chi(g_j) = \chi_{\mathbf{s}}(g_j)$ for $j = 1, 2$.

Lemma 6.1.18. *Let $[W]$ be a G_a-class and $L = \mathbb{Q}(W)$.*

(i) *If $\mathfrak{f}_{\mathfrak{p}}(L/F) \le 2$ for $\mathfrak{p} \mid 2$, then W prolongs to a group scheme $\mathcal{W}$ over R.*

(ii) *If $a \in \{4, 5, 11\}$ and W prolongs to a group scheme over R, then $\mathfrak{f}_{\mathfrak{p}}(L/F) \le 2$.*

Proof. Refer to Remark 6.1.15 for notation. In item (i), we have $\chi(g_2) = 0$ by Lemma 5.3.9(ii). To match χ with $\chi_{\mathbf{s}}$ for some local Honda parameter $\mathbf{s}$, we therefore consider $\mathbf{s}$ in Proposition 5.3.12(i), also allowing $\mathbf{s} = 0$. As $\mathbf{s}$ varies, $\chi_{\mathbf{s}}(g_1)$ ranges over all possible corners of $\mathfrak{h}$ and we can find a unique $\mathbf{s}$ such that $\chi_{\mathbf{s}}(g_1) = \chi(g_1)$. Hence W prolongs to a group scheme $\mathcal{W}$ over R.

In item (ii), G_a does not contain γ_9 by (6.1.5). Then $\chi(g_2) = 0$, to match $\chi_{\mathbf{s}}(g_2)$ for some Honda parameter $\mathbf{s}$ in Proposition 5.3.12. Hence $\mathfrak{f}_{\mathfrak{p}}(L/F) \le 2$. ☐

Definition 6.1.19. Let K be a pair-resolvent of F and Ω_K the maximal elementary 2-extension of K unramified outside $\{2, \infty\}$ such that $\mathfrak{f}_{\mathfrak{p}}(\Omega_K/K) \le 4$ for $\mathfrak{p} \mid 2$. We say F is *amiable* if either (i) $\Omega_K = K$ or (ii) $[\Omega_K : K] = 2$ and $\mathfrak{f}_{\mathfrak{p}}(\Omega_K/K) = 4$.

Remark 6.1.20. For F to be amiable, all the following conditions are necessary: (i) The narrow class number of K is odd. (ii) If $a \in (1+\mathfrak{p}^9)K_{\mathfrak{p}}^{\times 2}$, then $a \in K^{\times 2}$, since $f_{\mathfrak{p}}(K(\sqrt{a})/K) \le 2$ by Lemma C.6. (iii) K is not totally real; otherwise rank $U_K/U_K^2 = 10$, but rank $U_{\mathfrak{p}}/(1+\mathfrak{p}^9)U_{\mathfrak{p}}^2 = 8$.

Proposition 6.1.21. *Let $\mathcal{E}$ be the group scheme introduced at the beginning of this section. Then* $\mathrm{Ext}^1_{[2],\underline{E}}(\mathcal{E}, \mathcal{E}) = 0$ *if and only if $F = \mathbb{Q}(E)$ is amiable.*

Proof. Suppose that F is amiable and let $[\mathcal{W}]$ be a nontrivial class in $\mathrm{Ext}^1_{[2],\underline{E}}(\mathcal{E}, \mathcal{E})$. By Corollary 6.1.10, $[W]$ is G_a-class with $a \ne 0$. If $a = 11$, then $\mathfrak{f}_{\mathfrak{p}}(L/F) \le 2$ by Lemma 6.1.18(ii). By diagram (6.1.6) and Lemma 6.1.12(ii), there is a G_5-class $[W']$ with $L' = \mathbb{Q}(W')$ contained in L. Proposition 6.1.13 provides a quadratic extension K' of K contained in Ω_K with $\mathfrak{f}_{\mathfrak{p}}(K'/K) = \mathfrak{f}_{\mathfrak{p}}(L'/F) \le \mathfrak{f}_{\mathfrak{p}}(L/F) \le 2$, contradicting the amiability of F. The same argument applies when $a = 4$ or 5. If $a = 15$ or 9, then $[W]$ gives rise to both a G_4-class and a G_5-class. Then Proposition 6.1.13 provides two distinct quadratic extensions of K contained in Ω_K, again contradicting the amiability of F.

Suppose that F is not amiable. Assume first that $[\Omega_K : K] = 2$ and let $[W]$ be the G_a-class corresponding to Ω_K/K by Proposition 6.1.13. By amiability, $\mathfrak{f}_{\mathfrak{p}}(\Omega_K/K) \le 2$ and so $\mathfrak{f}_{\mathfrak{p}}(L/F) = \mathfrak{f}_{\mathfrak{p}}(\Omega_K/K) \le 2$. Then Lemma 6.1.18(i) implies that W prolongs to a nontrivial class in $\mathrm{Ext}^1_{[2],\underline{E}}(\mathcal{E}, \mathcal{E})$. Next, assume that there is a G_a-class $[W]$ with $L = \mathbb{Q}(W)$ and a $G_{a'}$-class $[W']$ with $L' = \mathbb{Q}(W')$, coming from distinct quadratic extensions of K in Ω_K and satisfying $a, a' \in \{4, 5, 9\}$. Since a G_9-class gives rise to a G_4-class and a G_5-class, we need only consider the pairs (a, a') in $\{(4, 4), (5, 5), (4, 5)\}$. In the notation of Remark 6.1.15, let χ and χ' in $\mathrm{Hom}_{\mathbb{F}_2[\Delta]}(\mathrm{Gal}(T/F_{\mathfrak{p}}), \mathfrak{h})$ belong to W and W' respectively. Then the Baer sum $W'' = W + W'$ represents a G_b-class by Lemma 6.1.12 and $\chi'' = \chi + \chi'$ belongs to W''. By Lemma 6.1.18(i) and Lemma C.11, we may assume that $\mathfrak{f}_{\mathfrak{p}}(L/F) = \mathfrak{f}_{\mathfrak{p}}(L'/F) = 4$ and so $\chi(g_2)$ and $\chi'(g_2)$ are nontrivial, by Lemma 5.3.9(ii). In all these cases, only one nontrivial corner is available in (6.1.5), namely $\chi(g_2) = \gamma_a$ and $\chi'(g_2) = \gamma_{a'}$. If $a = a' = 4$ or 5, then $\chi''(g_2) = 0$ and so $\mathfrak{f}(L''/F) \le 2$. Thus W'' prolongs to a group scheme over $\mathbb{Z}\left[\frac{1}{N}\right]$. If $(a, a') = (4, 5)$, then $\chi''(g_2) = \gamma_4 + \gamma_5 = \gamma_9$, so χ'' is compatible with $\chi_{\mathbf{s}}$ for some $\mathbf{s}$ in Proposition 5.3.12(i) or (ii) and the corresponding group scheme exists. ☐

Theorem 6.1.22. *Let A be a favorable abelian surface of prime conductor N such that $F = \mathbb{Q}(A[2])$ is amiable. If B is a semistable abelian variety of dimension $2d$ and conductor N^d, with $B[2]$ filtered by $A[2]$, then B is isogenous to A^d.*

Proof. By Proposition 1.2, $\mathcal{E} = A[2]$ satisfies the conditions in Definition 3.4 for a Σ-category $\underline{E}$ with $\Sigma = \{\mathcal{E}\}$. Then Theorem 3.7 applies, since $\mathrm{Ext}_{[2],\underline{E}}(\mathcal{E}, \mathcal{E}) = 0$ by Proposition 6.1.21 and $\mathrm{End}(A) = \mathbb{Z}$ because A has prime conductor [Brumer and Kramer 2014]. □

6.2. *Elliptic curves of prime conductor, supersingular at 2.* We briefly note how Theorem 3.7 applies to elliptic curves. Let A be an elliptic curve of prime conductor N with supersingular reduction at 2 and $\mathcal{E} = A[2]$. Then $F = \mathbb{Q}(E)$ is an $\mathcal{S}_3$-extension and E is an irreducible Galois module even locally over $\mathbb{Q}_2$. The only two irreducible $\mathbb{F}_2[\mathcal{S}_3]$ modules are the trivial one and E.

Proposition 6.2.1. *Let K be a cubic subfield of $F = \mathbb{Q}(E)$ and let $\mathfrak{p}$ be the prime in K above 2. A necessary and sufficient condition for $\mathrm{Ext}^1_{[2],\underline{E}}(\mathcal{E}, \mathcal{E}) = 0$ is that there be no quadratic extension of K of dividing conductor $\mathfrak{p}^2 \cdot \infty$.*

Proof. Only two subgroups of the parabolic group $\mathcal{P}_{E,E}$ admit good involutions. One is isomorphic to $\mathcal{S}_3$ and corresponds to the split extension of $\mathcal{E}$ by itself because $H^1(\mathcal{S}_3, \mathrm{End}(E)) = 0$ while the second is isomorphic to $\mathcal{S}_4$. If M is the field of points of an extension of $\mathcal{E}$ by $\mathcal{E}$ annihilated by 2 and $\mathrm{Gal}(M/\mathbb{Q}) \simeq \mathcal{S}_4$, then M is the Galois closure of a quadratic extension of K unramified at primes over p. The bound for the local conductor over 2 is given in [Schoof 2003, Proposition 6.4] and Theorem 3.7 applies. A related proof is in [Schoof 2005] for $A = J_0(N)$ with $N = 11$ and 19. □

In the Cremona database, we find 2037 isogeny classes of elliptic curves supersingular at 2 and of prime conductor $N < 350000$. From the Brumer–McGuinness database [1990], we extract an additional 2422 isogeny classes for a total of 4459 such classes with $N \le 10^8$. Applying the proposition above, we find 847 elliptic curves A to which Theorem 3.7 applies.

Let A_1 and A_2 be elliptic curves of prime conductor N with each $\mathcal{E}_i = A_i[2]$ biconnected over $\mathbb{Z}_2$ and satisfying $\mathrm{Ext}^1_{[2],\underline{E}}(\mathcal{E}_i, \mathcal{E}_i) = 0$. Suppose that the cubic subfields K_i of $\mathbb{Q}(E_i)$ are nonisomorphic. Then $2\mathcal{O}_{K_1K_2}$ has the prime factorization $(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^3$. If K_1K_2 admits no quadratic extension of conductor dividing $(\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3)^2\infty$, then $\mathrm{Ext}^1_{\underline{E}}(\mathcal{E}_1, \mathcal{E}_2) = 0$. We found 42 conductors N with multiple A_i to which our results apply.

As an entertaining example, Cremona's database lists four elliptic curves of conductor 307, with $A_1 = 307A1$, $A_2 = 307C1$ and $A_3 = 307D1$ supersingular at 2. Their 2-division fields correspond to the three subfields of the ray class field of $k = \mathbb{Q}(\sqrt{-307})$ of modulus $2\mathcal{O}_k$.

Theorem 3.7 implies the following. Let B be a semistable abelian variety, good outside $N = 307$, with $B[2]^{ss} = A_1[2]^{n_1} \oplus A_2[2]^{n_2} \oplus A_3[2]^{n_3}$ for some n_i. Then B is isogenous to $A_1^{n_1} \times A_2^{n_2} \times A_3^{n_3}$. Note that we need not impose the conductor $f_N(B) = \sum n_i f_N(A_i) = \sum n_i$, thanks to Remark 3.9.

Appendix A: A cohomology computation in the old style

Let $T = \Lambda[G]$ be the group ring of a finite group G over a discrete valuation ring Λ with prime element π and finite residue field k of characteristic p. We consider a cocycle approach to $\mathrm{Ext}^1_{\Lambda[G]}(E, E)$. Let V and W be finitely generated T-modules such that $\pi V = \pi W = 0$. A *symmetric cocycle* is a function

$f : V \times V \to W$ satisfying

$$f(v_1, v_2) = f(v_2, v_1) \quad \text{and} \quad f(v_1, v_2) + f(v_1 + v_2, v_3) = f(v_1, v_2 + v_3) + f(v_2, v_3),$$

for v's in V, as in [Eilenberg and MacLane 1942, Theorem 7.1]. Coboundaries are symmetric cocycles such that

$$f(v_1, v_2) = g(v_1) + g(v_2) - g(v_1 + v_2),$$

for some function $g : V \to W$. The symmetric cocycle f is *enhanced* if there is a function $h : T \times V \to W$ satisfying the following for v's in V and r, s in T:

(i) $rf(v_1, v_2) - f(rv_1, rv_2) = h(r, v_1) + h(r, v_2) - h(r, v_1 + v_2)$.

(ii) $h(rs, v) = rh(s, v) + h(r, sv)$.

(iii) $f(rv, sv) = h(r + s, v) - h(r, v) - h(s, v)$.

The cohomology classes of enhanced cocycles form a k-vector space $\mathcal{D}(V, W)$.

Lemma A.1. *The functor from T-modules to abelian groups induces an exact sequence*

$$0 \to \mathrm{Ext}^1_{[\pi],T}(V, W) \to \mathrm{Ext}^1_T(V, W) = \mathcal{D}(V, W) \to \mathrm{Hom}_T(V, W),$$

where $\mathrm{Ext}^1_{[\pi],T}(V, W)$ consists of classes of extensions annihilated by π.

Proof. Let $0 \to W \xrightarrow{i} M \xrightarrow{j} V \to 0$ be an exact sequence of T-modules with $\pi V = \pi W = 0$. Let $\sigma : V \to M$ be a section of j such that $\sigma(0) = 0$. The associated cocycle is defined by $f(v_1, v_2) = \sigma(v_1) + \sigma(v_2) - \sigma(v_1 + v_2)$. If r is in T, then $h(r, v) = r\sigma(v) - \sigma(rv)$ turns f into an enhanced cocycle. For the converse, give $W \times V$ the structure of a T-module by setting

$$(w_1, v_1) + (w_2, v_2) = (w_1 + w_2 + f(v_1, v_2), v_1 + v_2), \quad r(w, v) = (rw + h(r, v), rv).$$

Hence $\mathrm{Ext}^1_T(V, W) = \mathcal{D}(V, W)$. Given f as above, let $\iota : V \to W$ be defined by $\iota(a) = h(\pi, a)$. Since $\pi(w, v) = (\iota(v), 0)$ and π is in the center of T, we conclude that ι is a T-homomorphism and that the sequence is exact. □

Using the lemma, we give a refined variant of [Schoof 2012b, Lemma 2.1]. Let F be a number field and R its ring of S-integers for a finite set S of primes.

Proposition A.2. *Let $\mathcal{V}$ and $\mathcal{W}$ be finite flat Λ-module schemes over R killed by π, with associated Galois modules V and W. Let $\mathrm{Ext}^1_{[\pi],R}(\mathcal{V}, \mathcal{W})$ denote the subgroup of $\mathrm{Ext}^1_R(\mathcal{V}, \mathcal{W})$ consisting of those extensions killed by π. Then there is a natural exact sequence*

$$0 \to \mathrm{Ext}^1_{[\pi],R}(\mathcal{V}, \mathcal{W}) \to \mathrm{Ext}^1_R(\mathcal{V}, \mathcal{W}) \to \mathrm{Hom}_{\mathrm{Gal}}(V, W).$$

If V is absolutely irreducible over k, then $\mathrm{End}_{\mathrm{Gal}}(V) = k$.

Proof. Apply Lemma A.1 with G the Galois group of a suitable finite extension of F. Then the passage from Galois modules to the associated group schemes is as in Schoof and so is left to the reader. □

Appendix B: Parabolic subgroups and an obstreperous cocycle

For any group G, consider representations ρ_{E_i} afforded by $\mathbb{F}_p[G]$-modules E_i for $i=1,2$. If g is in G and $\delta_i=\rho_{E_i}(g)$, then g acts on m in $\mathfrak{h}=\mathrm{Hom}_{\mathbb{F}_p}(E_2, E_1)$ by $g(m)=\delta_1 m \delta_2^{-1}$. In the category of $\mathbb{F}_p[G]$-modules, the extension classes of E_2 by E_1 under Baer sum form a group isomorphic to $H^1(G,\mathfrak{h})$. The exact sequence of $\mathbb{F}_p[G]$-modules $0\to E_1\to W\to E_2\to 0$ gives rise to a cocycle $\psi: G\to\mathfrak{h}$ such that

$$\rho_W(g)=\begin{bmatrix}\delta_1 & \psi(g)\delta_2\\ 0 & \delta_2\end{bmatrix} \tag{B.1}$$

and the class $[W]$ in $\mathrm{Ext}^1_{\mathbb{F}_p[G]}(E_2, E_1)$ corresponds to that of $[\psi]$ in $H^1(G,\mathfrak{h})$. If N is a normal subgroup of G contained in $\ker\rho_W$, then $[\psi]$ comes by inflation from a unique class in $H^1(G/N,\mathfrak{h})$, also denoted by $[\psi]$.

Note that $\rho_W(G)$ lies in a *parabolic* matrix group

$$\mathcal{P}=\mathcal{P}_{E_1,E_2}=\left\{g=\begin{bmatrix}\delta_1 & m\\ 0 & \delta_2\end{bmatrix} \mid \delta_i=\rho_{E_i}(g),\ m\in\mathrm{Mat}_{n_1,n_2}(\mathbb{F}_p)\right\} \tag{B.2}$$

with $n_i=\dim_{\mathbb{F}_p} E_i$. If $H_i=\{g\in G \mid g_{|E_i}=1\}$ and $\Delta_i=G/H_i$, then E_i is a faithful $\mathbb{F}_p[\Delta_i]$-module. Any normal subgroup H of G acting trivially on both E_1 and E_2 satisfies

$$\rho_W(H)\subseteq\left\{g=\begin{bmatrix}1 & m\\ 0 & 1\end{bmatrix}\in\mathcal{P} \mid m\in\mathrm{Mat}_{n_1,n_2}(\mathbb{F}_p)\right\}.$$

Since $H^1(H,\mathfrak{h})^{G/H}=\mathrm{Hom}_{\mathbb{F}_p[G/H]}(H,\mathfrak{h})$, the following sequence is exact:

$$0\to H^1(G/H,\mathfrak{h})\xrightarrow{\text{inf}} H^1(G,\mathfrak{h})\xrightarrow{\text{res}}\mathrm{Hom}_{\mathbb{F}_p[G/H]}(H,\mathfrak{h}). \tag{B.3}$$

Suppose that E_1 and E_2 are $G_{\mathbb{Q}}$-modules, $F=\mathbb{Q}(E_1,E_2)$ and $\Delta=\mathrm{Gal}(F/\mathbb{Q})$. If the extension $W=W_\psi$ belongs to a cocycle $\psi:\Delta\to\mathfrak{h}$ whose class in $H^1(\Delta,\mathfrak{h})$ is not trivial, then $\mathbb{Q}(W)=F$, even though W does not split as a Δ-module.

Example B.4. Let $p=2$ and $E=E_1=E_2$, with $\dim_{\mathbb{F}_2}(E)=2n$, so that $\mathfrak{h}$ is isomorphic to $\mathrm{Mat}_{2n}(\mathbb{F}_2)$. As in [Brumer and Kramer 2012, Remark 2.6], equip E with the irreducible symplectic representation of $\Delta\subset\mathrm{Sp}_{2n}(\mathbb{F}_2)$ isomorphic to $\mathcal{S}_m$, with transvections corresponding to transpositions and $m=2n+1$ or $2n+2$. When $n\geq 2$, there is a nontrivial class $[\psi]$ in $H^1(\Delta,\mathfrak{h})$ such that $\psi(g)=\epsilon(g)I_{2n}$, where $\epsilon(g)\in\mathbb{F}_2$ is the parity of the permutation g. This situation can occur when E is the kernel of multiplication by 2 on the Jacobian of a hyperelliptic curve of genus at least 2.

Suppose further that E has prime conductor N and that σ_v generates inertia in $F/\mathbb{Q}$ at $v\mid N$. Then σ_v is a transposition in $\mathcal{S}_m$, so $\psi(\sigma_v)=I_{2n}$ and it follows from (B.1) that rank $\rho_W(\sigma_v-1)=2n$. The extension $W=W_\psi$ prolongs to a group scheme over $\mathbb{Z}\left[\frac{1}{N}\right]$ satisfying **E1** and **E2**, since the local cohomology group $H^1(\mathcal{D}_{\mathfrak{p}}(F/\mathbb{Q}),\mathfrak{h})=0$ at $\mathfrak{p}\mid 2$, as in Lemma 5.3.3. However, the minimality assumption **E3** on our category $\underline{E}$ requires that rank $\rho_W(\sigma_v-1)=2$, namely the multiplicity of E in W^{ss}, so W is not in $\underline{E}$ when $n\geq 2$.

Appendix C: Some technical lemmas on local conductors

Let K be a finite extension of $\mathbb{Q}_p$ with uniformizer π_K, ring of integers $\mathcal{O}_K$ and absolute ramification index $e_K = \mathrm{ord}_{\pi_K}(p)$. Set

$$U_K^{(n)} = \{u \in \mathcal{O}_K^\times \mid \mathrm{ord}_{\pi_K}(u-1) \geq n\}. \tag{C.1}$$

See [Serre 1979, IV] for basic information about ramification groups and conductors. Let L/K be a finite Galois extension. The *index* of elements g in $G = \mathrm{Gal}(L/K)$ is given by $i_{L/K}(g) = \mathrm{ord}_{\pi_L}(g(\theta)-\theta)$ for any choice of θ in $\mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\theta]$. Then $\mathrm{ord}_{\pi_L}(g(a)-a) \geq i_{L/K}(g)$ for all a in $\mathcal{O}_K$. In Serre's *lower numbering* on ramification groups, $G_j = \{g \in G \mid i_{L/K}(g) \geq j+1\}$. Thus $G_{-1} = G$, G_0 is the inertia group, its fixed field is the maximal unramified extension of K inside L and the p-Sylow subgroup G_1 is the wild ramification subgroup of G. For g in G_0, we have $i_{L/K}(g) = \mathrm{ord}_{\pi_L}(g(\pi_L)-\pi_L)$. The Herbrand function is defined by

$$\varphi_{L/K}(x) = \int_0^x \frac{ds}{[G_0 : G_s]} \tag{C.2}$$

In Serre's *upper numbering*, $G^m = G_n$ with $m = \varphi_{L/K}(n)$.

Notation C.3. Let $c_{L/K} = \max\{j \mid G_j \neq 1\}$ and let $m_{L/K} = \varphi_{L/K}(c_{L/K})$. Thus $G^{m_{L/K}} \neq 1$ but $G^{m_{L/K}+\epsilon} = 1$ for all $\epsilon > 0$. When L/K is abelian, the conductor exponent $\mathfrak{f}(L/K)$ is the smallest integer $n \geq 0$ such that $U_K^{(n)}$ is contained in the norm group $N_{L/K}(L^\times)$.

We have $\mathfrak{f}(L/K) = m_{L/K}+1$ by [Serre 1979, XV, §2], with $c_{L/K} = m_{L/K} = -1$ and $\mathfrak{f}(L/K) = 0$ when L/K is unramified. If M/K is a Galois extension and the intermediate field L also is Galois over K, then $m_{L/K} \leq m_{M/K}$ because $\mathrm{Gal}(M/K)^\alpha \xrightarrow{\text{res}} \mathrm{Gal}(L/K)^\alpha$ is surjective for all α. Translation by an unramified extension of the base does not affect the conductor, as we next recall.

Lemma C.4. *If F/K is unramified, then $m_{LF/F} = m_{L/K}$. Additionally, if L/K is abelian, then $\mathfrak{f}(LF/F) = \mathfrak{f}(L/K)$.*

Proof. The restriction map $\mathrm{Gal}(LF/F) \xrightarrow{\text{res}} \mathrm{Gal}(L/L\cap F)$ is an isomorphism. Since F/K is unramified, π_L also is a prime element of LF. For all $s \geq 0$, it follows from the definition of the lower numbering that restriction induces an isomorphism $\mathrm{Gal}(LF/F)_s \xrightarrow{\sim} \mathrm{Gal}(L/L\cap F)_s = \mathrm{Gal}(L/K)_s$ Thus the Herbrand functions of LF/F and L/K agree and the rest is clear. □

Proposition C.5. *Let $L = K(t)$ be Galois over K, with $\mathrm{ord}_{\pi_L}(t) = -n$ prime to p and negative. If $g(t)-t$ is a unit for all $g \neq 1$ in G_0, then G_0 is an elementary abelian p-group and $\mathfrak{f}(L/K) = i_{L/K}(g) = n+1$.*

Proof. By assumption, nontrivial elements g of G_0 satisfy $g(t) = t+u$ with u a unit in $\mathcal{O}_L$ and $g(u) \equiv u \pmod{\pi_L}$. If g has order d, then

$$t = g^d(t) = t+u+g(u)+\cdots+g^{d-1}(u) \equiv t+du \pmod{\pi_L},$$

so $p \mid d$. Hence $G_0 = G_1$ is a p-group and so $i = i_{L/K}(g) \geq 2$. Furthermore, $\mathrm{ord}_\pi(g(a)-a) \geq i$ for all a in $\mathcal{O}_L$.

Set $\pi = \pi_L$, $\theta = 1/t = \alpha\pi^n$ and $g(\pi) - \pi = \beta\pi^i$, where α and β are units in $\mathcal{O}_L$. We have the following congruences modulo $\pi^{n+i}\mathcal{O}_L$:

$$\begin{aligned} g(\theta) - \theta = (g-1)(\alpha\pi^n) &= \alpha(g-1)(\pi^n) + g(\pi^n)(g-1)(\alpha) \\ &\equiv \alpha(g-1)(\pi^n) \\ &\equiv \alpha((\pi + \beta\pi^i)^n - \pi^n) \\ &\equiv \alpha\beta n\pi^{n-1+i} \end{aligned}$$

and therefore $\mathrm{ord}_\pi(g(\theta) - \theta) = n - 1 + i$. Explicitly,

$$g(\theta) - \theta = \frac{t - g(t)}{tg(t)} = -\frac{u}{tg(t)} = -u \cdot \theta g(\theta),$$

so $\mathrm{ord}_\pi(g(\theta) - \theta) = 2n$. Hence $i = n + 1$ and the lower ramification sequence has only one gap: $G_0 = G_n \supsetneq G_{n+1} = \{1\}$. By ramification theory, G_n is an elementary abelian p-group and we have $\mathfrak{f}(L/K) = \varphi_{L/K}(n) + 1 = n + 1$. □

Next, we recall the conductors of Kummer extensions of degree p.

Lemma C.6. *Let K contain $\boldsymbol{\mu}_p$ and $L = K(\kappa^{1/p})$ with $\kappa \in K^\times$. Then*

$$\mathfrak{f}(L/K) = \frac{pe_K}{p-1} + 1 \quad \textit{if } \mathrm{ord}_{\pi_K}(\kappa) \not\equiv 0 \bmod p$$

and this is maximal for cyclic extensions of K of degree p. If $\mathrm{ord}_{\pi_K}(\kappa - 1) = n$ with $1 \le n < pe_K/(p-1)$ and $n \not\equiv 0 \bmod p$, then $\mathfrak{f}(L/K) = pe_K/(p-1) - n + 1$.

Proof. In the first case, assume without loss of generality that $\mathrm{ord}_{\pi_K}(\kappa) = 1$, so $\theta = \kappa^{1/p}$ is a prime element for L. If $g \neq 1$ in $\mathrm{Gal}(L/K)$, then $g(\theta) - \theta = (\zeta - 1)\pi_L$ for some a p-th root of unity ζ and the conductor follows by definition.

In the second case, set $\kappa = 1 + u\pi_K^n$ with u in U_K and $\theta = \kappa^{1/p} - 1$. Then $g(\theta) = \zeta\kappa^{1/p} - 1 = \theta + (\zeta - 1)\kappa^{1/p}$, where θ satisfies $x^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j = u\pi_K^n$. Let $t = \theta/(\zeta - 1)$, to find that $g(t) - t = \kappa^{1/p}$ is a unit in L and t satisfies

$$z^p + \sum_{j=1}^{p-1} a_j z^j = \frac{u\pi_K^n}{(\zeta - 1)^p} \quad \text{with} \quad a_j = \binom{p}{j}(\zeta - 1)^{j-p}. \tag{C.7}$$

For $1 \le j \le p - 1$, we have

$$\mathrm{ord}_{\pi_K}(a_j) = e_K - (p - j)\frac{e_K}{p-1} = (j-1)\frac{e_K}{p-1} \ge 0.$$

Put $z = t$ in (C.7) and compare ordinals on both sides, using $p \nmid n$, to see that L/K is totally ramified of degree p and

$$\mathrm{ord}_L(t^p) = n\,\mathrm{ord}_{\pi_L}(\pi_K) - p\,\mathrm{ord}_{\pi_L}(\zeta - 1) = np - p\frac{pe_K}{p-1}.$$

Thus $\mathrm{ord}_p(t) = n - pe_K/(p-1)$ and $\mathfrak{f}(L/K)$ can be found by using Proposition C.5. □

Remark C.8. Since the choice of κ can be changed by multiplying by a suitable element of $K^{\times p}$, the only remaining cases are $n \geq pe_K/(p-1)$. If equality holds, then (C.7) gives an integral polynomial satisfied by t whose reduction modulo π_K has the form $z^p + \bar{a}a_1 z^{p-1} - \bar{b}$ with $b = u\pi^n(\zeta-1)^{-p}$. Since a_1 and b are unit in $\mathcal{O}_K$, this polynomial is separable and L/K is unramified, but possibly split. If $n > pe_K/(p-1)$, then κ is in $K^{\times p}$ and $L = K$.

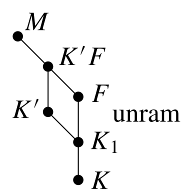
Lemma C.9. *Let L_i/K be Galois and let $m_i = m_{L_i/K}$ be the upper numbering of the last nontrivial ramification subgroup of* $\mathrm{Gal}(L_i/K)$. *If $M = L_1L_2$, then $m_{M/K} = \max\{m_1, m_2\}$ and if L is a subfield of M with L/K abelian, then $\mathfrak{f}(L/K) \leq m_{M/K} + 1$.*

Proof. If $m = \max\{m_1, m_2\}$, then $m_{M/K} \geq m$. But if g is in $\mathrm{Gal}(M/K)^\alpha$ with $\alpha > m$, then $g_{|L_i} = 1$ for $i = 1, 2$, so $g = 1$. Hence $m_{M/K} = m$. It follows that $m_{L/K} \leq m$ and therefore $\mathfrak{f}(L/K) \leq m + 1$. □

Lemma C.10. *Assume that F/K is Galois and L/F is abelian. Let M be the Galois closure of L/K. Then M/F is abelian and $\mathfrak{f}(M/F) = \mathfrak{f}(L/F)$.*

Proof. Since $m_{L/F} \leq m_{M/F}$, we have $\mathfrak{f}(L/F) \leq \mathfrak{f}(M/F)$. If τ is in $\mathrm{Gal}(M/K)$, then $\tau(L)/F$ is abelian and $\mathfrak{f}(\tau(L)/F) = \mathfrak{f}(L/F)$. But M is the compositum of all $\tau(L)$ as τ varies. Therefore, M/F is abelian and by Lemma C.9, $\mathfrak{f}(M/F) \leq \mathfrak{f}(L/F)$, giving equality. □

For the next lemma, refer to the following diagram:



Lemma C.11. *Let F be the Galois closure of K_1/K and assume that F/K_1 is unramified. Let K' be an abelian extension of K_1 and let M be the Galois closure of K'/K. Then M is abelian over F and $\mathfrak{f}(M/F) = \mathfrak{f}(K'/K_1)$.*

Proof. The field M contains F because K' contains K_1. Moreover, M is the Galois closure of $K'F/K$. Since K' is abelian over K_1, the extension $K'F/F$ is abelian. By Lemma C.10, with L there equal to $K'F$ here, we find that M/F is abelian and $\mathfrak{f}(M/F) = \mathfrak{f}(K'F/F)$. By Lemma C.4, translation of the base via an unramified extension does not change the conductor, so $\mathfrak{f}(K'F/F) = \mathfrak{f}(K'/K_1)$. Hence $\mathfrak{f}(M/F) = \mathfrak{f}(K'/K_1)$. □

When $L = K(V)$, where $\mathcal{V}$ is a finite flat group scheme over $\mathcal{O}_K$ of exponent p^n, Fontaine [1985] showed that $m_{L/K} \leq e_K(n + 1/(p-1)) - 1$. Now consider the conductor exponent of an intermediate abelian extension.

Proposition C.12. *Let $L = K(V)$ and suppose that $K \subseteq F \subseteq F' \subseteq L$, with F'/F abelian and the relative ramification index $e_{F/K}$ equal to the tame ramification degree $[G_0 : G_1]$ of L/K. Then $\mathfrak{f}(F'/F) \leq e_F(n + 1/(p-1)) - e_{F/K} + 1$.*

Proof. The fixed field L_1 of $H = G_1$ is the maximal subfield of L tamely ramified over K. Since $H_0 = G_1$ and $H_s = G_s$ for all $s > 0$, (C.2) gives

$$\varphi_{L/L_1}(x) = [G_0 : G_1]\varphi_{L/K}(x) = e_{F/K}\varphi_{L/K}(x), \quad \text{for all } x > 0.$$

We may assume that L properly contains L_1. Using $c_{L/L_1} = c_{L/K}$, we have

$$m_{F'L_1/L_1} \le m_{L/L_1} = \varphi_{L/L_1}(c_{L/L_1}) = e_{F/K}\varphi_{L/K}(c_{L/K}) = e_{F/K}m_{L/K}.$$

But F is contained in L_1 and L_1/F is unramified. Hence Lemma C.4 shows that $\mathfrak{f}(F'/F) = \mathfrak{f}(F'L_1/L_1) \le 1 + e_{F/K}m_{L/K}$. Conclude with Fontaine's bound. □

Appendix D: Some data

The quintic field F_0 is *amiable* if its Galois closure F is amiable as in Definition 6.1.19, so that the uniqueness in Theorem 6.1.22 applies. To check amiability, construct the pair-resolvent field K and ask Magma, under GRH, for the 2-rank of the ray class groups of K with the desired moduli, as in Theorem 1.3. A favorable abelian surface A is of *type* F_0 if $\mathbb{Q}(A[2])$ is the Galois closure of F_0. To find representatives for isogeny classes of abelian surfaces of prime conductor N, it suffices to search for Jacobians by [Brumer and Kramer 2014, Theorem 3.4.11]. If F is amiable, then it is not totally real by Remark 6.1.20. The Magma database of quintic fields contains 1919 favorable quintic fields that are not totally real. Their absolute discriminants are at most $5 \cdot 10^6$ and 714 of them are amiable. We know Jacobians for only 82 of the latter, but expect conductors of abelian surfaces to be sparse among integers.

We tabulate explicit information for favorable fields and curves with $N < 25000$ and summarize some data for $N < 10^{10}$. In all our tables, $[a_0, a_1, a_2, \ldots]$ denotes the polynomial $a_0 + a_1 x + a_2 x^2 + \cdots$, as in Magma.

Legend for Tables 1 and 2. Table 1 on the next two pages gives a defining polynomial $f(x)$ for each of the 172 favorable quintic fields F_0 of discriminant $\pm 16N$ with $N < 25000$. Table 2 on page 1068 consists of 75 curves $y^2 = g(x)$ whose Jacobians represent distinct known isogeny classes of favorable abelian surfaces of prime conductor $N < 25000$. If C is curve number 25, 63 or 64 in that table, its leading coefficient has the form $4m^3$. These curves exhibit *mild reduction* [Brumer and Kramer 2014, p. 1162], in that C is bad at $p \mid m$ but the reduction of $J(C)$ at p is the product of two elliptic curves.

In both tables, the column marked ϵ contains an α if F_0 is amiable. For each field F_0 in Table 1, the column marked #C contains one of the following:

- The line number of a curve in Table 2 such that g has a root in F_0.
- 0 if we can prove that no abelian surface of type F_0 exists by [Brumer and Kramer 2018].
- P if no nonlift paramodular form of that level exists, so no such surface is expected to exist.
- U if there is at most one isogeny class of that type, but it is unknown whether such an abelian surface actually exists.
- ν if F_0 is not amiable and we do not know whether or not any surface exists.

#F_0	$f(x)$	N	ϵ	#C	#F_0	$f(x)$	N	ϵ	#C
1	[–1, –1, –2, 0, 1, 1]	277	α	1	43	[–2, –2, 2, 4, 2, 1]	5309	α	U
2	[–1, 1, 0, 0, 1, 1]	349	α	2	44	[–1, –3, –6, –2, 1, 1]	5381		ν
3	[–1, 3, 0, –2, 1, 1]	461	α	3	45	[3, –1, 4, 6, 1, 1]	5437	α	0
4	[1, 3, 2, 2, 1, 1]	613	α	P	46	[–2, –4, 0, 2, 2, 1]	5651	α	26
5	[1, 1, 2, 0, 1, 1]	677	α	P	47	[2, 4, –4, –4, 2, 1]	5867		27
6	[2, 2, 2, 2, 2, 1]	797	α	4	48	[2, –4, 2, –2, 2, 1]	6277	α	U
7	[–2, 0, 0, 0, 2, 1]	971	α	5	49	[–1, –1, –8, –4, 1, 1]	6317	α	0
8	[1, 1, 0, –2, 1, 1]	997	α	6	50	[–3, –5, –6, 2, 1, 1]	6373	α	U
9	[–1, –3, 0, 4, 1, 1]	1051	α	7	51	[2, 4, 0, –2, 2, 1]	6397	α	0
10	[2, –2, –2, 0, 2, 1]	1061	α	U	52	[2, –2, 0, –2, 0, 1]	6491		28
11	[1, –1, 2, –2, 1, 1]	1109	α	9	53	[2, 0, 4, 6, 0, 1]	6701		0
12	[–1, 3, –2, 0, 1, 1]	1109	α	8	54	[–2, 2, 4, –4, 0, 1]	6763		29
13	[–2, –4, –2, 2, 2, 1]	1277	α	0	55	[–1, 9, –2, –6, 1, 1]	6907	α	U
14	[2, –4, 4, –2, 0, 1]	1597	α	0	56	[2, 6, 4, 0, 0, 1]	7013	α	U
15	[2, –2, 2, 0, 0, 1]	1637	α	10	57	[–2, 0, –4, –2, 2, 1]	7109		30
16	[1, –3, 0, 2, 1, 1]	1811	α	11	58	[2, –4, –2, 4, 2, 1]	7541	α	U
17	[–2, 2, 2, 4, 2, 1]	2069	α	U	59	[2, –2, 6, 0, 0, 1]	7549	α	U
18	[–2, 0, 2, –2, 0, 1]	2243	α	12	60	[–3, 7, 2, 6, 1, 1]	7589	α	U
19	[3, 5, 4, 4, 1, 1]	2269	α	U	61	[6, 2, –8, –4, 2, 1]	7723		ν
20	[–3, –1, –2, 2, 1, 1]	2341	α	13	62	[2, 6, 0, –6, 0, 1]	7877		31, 32, 33
21	[2, 4, 2, 2, 2, 1]	2557	α	0	63	[11, –1, –4, –4, 1, 1]	7963		ν
22	[2, 4, 0, –2, 0, 1]	2677	α	14	64	[–2, 4, 0, –2, 2, 1]	8243	α	34
23	[–2, 0, 2, 0, 0, 1]	2693		15	65	[2, 4, 2, 2, 0, 1]	8581		ν
24	[2, 4, 2, 0, 0, 1]	2909	α	U	66	[–1, –5, –4, 6, 1, 1]	8803		35
25	[6, 8, 8, 6, 2, 1]	3037	α	0	67	[–3, 13, –4, –6, 1, 1]	9091	α	36
26	[2, –2, 4, 0, 0, 1]	3109	α	U	68	[5, 7, 0, 0, 1, 1]	9781	α	U
27	[–2, 4, 2, –6, 0, 1]	3251	α	16	69	[7, 3, –6, –4, 1, 1]	9803		37
28	[1, 5, 2, 4, 1, 1]	3461	α	U	70	[2, –2, 4, 0, 2, 1]	9941	α	38
29	[–1, –3, –2, –2, 1, 1]	3499		17	71	[7, 1, 2, –2, 1, 1]	9949		0
30	[2, 0, 2, 0, 0, 1]	3557		18	72	[2, –8, 8, 0, 0, 1]	10037		39
31	[2, 2, 0, 0, 0, 1]	3637	α	19	73	[1, –3, –4, –2, 1, 1]	10163	α	U
32	[2, 6, 0, –4, 0, 1]	3701	α	20	74	[2, 4, 0, 6, 0, 1]	10253		0
33	[2, 0, 0, 2, 2, 1]	3853	α	0	75	[–2, 2, 2, –8, 0, 1]	10259		ν
34	[2, 0, 0, 2, 0, 1]	3989		21	76	[1, 3, 6, 2, 1, 1]	10453	α	U
35	[–2, –2, –2, 2, 2, 1]	3989	α	U	77	[3, –7, 10, –6, 1, 1]	10789		40
36	[–1, 5, –4, –4, 1, 1]	4003		0	78	[2, –2, 4, –4, 0, 1]	10837		41
37	[2, 2, –2, –2, 2, 1]	4157	α	22	79	[2, 2, 6, 4, 2, 1]	10853		42
38	[2, –6, 4, 0, 0, 1]	4219	α	U	80	[6, –4, 0, –2, 0, 1]	10949	α	43
39	[2, 2, 0, 2, 0, 1]	4517	α	23	81	[1, 1, 6, –6, 1, 1]	10957		ν
40	[2, 0, –6, –2, 2, 1]	5059	α	24	82	[–3, –1, 0, 0, 1, 1]	11117		44
41	[–1, 1, 0, –4, 1, 1]	5227		25	83	[–1, –5, –6, –4, 1, 1]	11131		ν
42	[2, 2, 2, 0, 0, 1]	5261	α	0	84	[5, 11, 0, –4, 1, 1]	11243	α	U

Table 1. Favorable quintic fields (legend on previous page; continuation on next page).

$\#F_0$	$f(x)$	N	ϵ	$\#C$	$\#F_0$	$f(x)$	N	ϵ	$\#C$
85	[−1, 5, −6, 6, 1, 1]	11261		0	129	[9, 5, −6, −4, 1, 1]	17029		ν
86	[−1, 3, 2, −4, 1, 1]	11579		45	130	[−7, 5, 4, −2, 1, 1]	17203		ν
87	[−3, 1, 0, 2, 1, 1]	11701		ν	131	[−2, 10, −12, −2, 2, 1]	17291		57
88	[2, −10, 14, −4, 0, 1]	11971		46, 47	132	[−15, 13, 6, −4, 1, 1]	17317		58
89	[13, 11, −6, −6, 1, 1]	12037		ν	133	[4, −4, 8, −2, 0, 1]	17341	α	U
90	[3, −1, −2, 0, 1, 1]	12109		ν	134	[−2, 0, 4, 2, 0, 1]	17341		0
91	[3, 11, 0, −4, 1, 1]	12301		ν	135	[−4, 4, 4, 0, 0, 1]	17389	α	59
92	[2, 10, 6, −2, 0, 1]	12541	α	U	136	[3, 7, 6, 4, 1, 1]	17597	α	0
93	[10, 6, −8, −4, 2, 1]	12757		ν	137	[14, 24, 4, −6, 0, 1]	17923		ν
94	[2, 2, 4, 2, 0, 1]	12781	α	U	138	[6, −4, 6, 0, 0, 1]	18077	α	60
95	[−3, 5, −2, −4, 1, 1]	12781	α	U	139	[−1, −3, −8, −4, 1, 1]	18181	α	0
96	[−3, −5, −10, −6, 1, 1]	12907	α	U	140	[−1, −5, −4, 2, 1, 1]	18691		0
97	[−3, 1, −6, −6, 1, 1]	12923	α	48	141	[1, 7, 2, −2, 1, 1]	18757		ν
98	[−1, −1, 2, −4, 1, 1]	13003	α	U	142	[10, 4, −8, −4, 2, 1]	18869		ν
99	[−2, 2, −2, 0, 2, 1]	13037	α	0	143	[−1, 3, −8, −8, 1, 1]	19051	α	U
100	[−2, 4, −2, −4, 2, 1]	13147	α	49	144	[−2, −2, 4, 4, 2, 1]	19211		61
101	[7, −1, −2, −4, 1, 1]	13147	α	50	145	[2, 0, 4, 4, 2, 1]	19429		63
102	[2, −4, 0, 0, 0, 1]	13259		51	146	[−2, −12, −22, −8, 2, 1]	19469	α	U
103	[3, −1, 4, −4, 1, 1]	13597		0	147	[−1, −5, −14, −8, 1, 1]	19531	α	64
104	[2, 8, 8, 6, 2, 1]	13597		ν	148	[4, 0, −8, 2, 2, 1]	19597		0
105	[1, 5, 2, −12, 1, 1]	13723		52	149	[4, 4, 0, 4, 2, 1]	20389		ν
106	[6, 4, 6, 4, 2, 1]	13829	α	U	150	[1, −3, 2, 4, 1, 1]	20533	α	U
107	[1, 1, −4, −6, 1, 1]	13963		ν	151	[−2, 6, 0, 2, 2, 1]	21061	α	U
108	[−2, 6, 2, −6, 0, 1]	13997		53	152	[−2, 2, 2, −4, 2, 1]	21211	α	65
109	[4, −4, 4, 0, 2, 1]	13997		ν	153	[−5, 11, 2, −12, 1, 1]	21283		0
110	[−9, −1, 4, 0, 1, 1]	14149		ν	154	[−6, −4, 4, −4, 0, 1]	21563		66
111	[15, 13, −6, −6, 1, 1]	14197		54	155	[−14, −18, −10, −2, 2, 1]	21739	α	U
112	[2, −2, 6, −2, 2, 1]	14293		ν	156	[18, 8, −12, −6, 2, 1]	21787		67
113	[−3, −1, −2, −2, 1, 1]	14629	α	U	157	[−3, −1, 2, 2, 1, 1]	22277		68
114	[−46, 48, 6, −14, 0, 1]	14779		ν	158	[−2, 8, −8, −6, 2, 1]	22291		69
115	[2, 4, 4, 4, 0, 1]	14821	α	U	159	[−1, −3, −8, 4, 1, 1]	22637		0
116	[−2, 4, 2, −2, 0, 1]	15013		ν	160	[−3, 13, 2, 10, 1, 1]	22709		ν
117	[1, −3, 2, −4, 1, 1]	15227		ν	161	[2, 0, −6, −4, 2, 1]	22787	α	U
118	[−2, 0, 2, 0, 2, 1]	15307		55	162	[1, 9, 6, 2, 1, 1]	22861		70
119	[−2, 2, 4, 4, 0, 1]	15373	α	U	163	[−5, 13, −4, −8, 1, 1]	23003		71
120	[3, 7, 0, 0, 1, 1]	15493	α	U	164	[−3, −1, −4, −4, 1, 1]	23059	α	U
121	[−2, 4, −2, 0, 2, 1]	15581		ν	165	[1, −3, −2, 4, 1, 1]	23131		72, 73
122	[5, 9, 4, 6, 1, 1]	15749		56	166	[2, −4, −2, 0, 2, 1]	23251		ν
123	[4, 0, 0, −2, 2, 1]	15749	α	U	167	[6, 4, 2, 4, 0, 1]	23669		ν
124	[2, −6, 2, 2, 2, 1]	15923	α	U	168	[−6, 2, 4, −2, 0, 1]	24109	α	0
125	[−2, 0, 10, 8, 0, 1]	16139		ν	169	[2, 8, 0, 6, 0, 1]	24469		74, 75
126	[2, −2, −10, −4, 2, 1]	16451		ν	170	[2, −4, 2, 2, 0, 1]	24533		ν
127	[1, 5, 2, 0, 1, 1]	16901	α	U	171	[−6, 4, 6, −6, 0, 1]	24611	α	U
128	[−6, 4, 2, −4, 0, 1]	16981	α	U	172	[−7, −5, −2, −2, 1, 1]	24763		ν

#C	#F_0	$g(x)$	N	ϵ	#C	#F_0	$g(x)$	N	ϵ
1	1	[1, –4, 8, –8, 0, 4]	277	α	39	72	[1, 0, 4, 0, 0, 4]	10037	
2	2	[1, –4, 4, 4, –8, 4]	349	α	40	77	[1, 12, 44, 52, 4, 4]	10789	
3	3	[1, 8, 20, 12, –8, 4]	461	α	41	78	[13, 4, –20, –8, 8, 4]	10837	
4	6	[1, 0, 0, 4, –4, 4]	797	α	42	79	[5, 12, 0, –12, 0, 4]	10853	
5	7	[1, 4, 0, –8, 0, 4]	971	α	43	80	[–7, 12, 4, 16, 4, 4]	10949	α
6	8	[1, 0, –4, 8, –8, 4]	997	α	44	82	[1, –4, 4, –4, 8, 4]	11117	
7	9	[1, –4, 4, 0, –4, 4]	1051	α	45	86	[1, 12, 44, 44, –4, 4]	11579	
8	11	[–79, –304, –560, –200, –4, 4]	1109	α	46	88	[1, 4, 0, –4, 4, 4]	11971	
9	12	[1, 4, 4, –4, –4, 4]	1109	α	47	88	[1461041,–565424,78052,–4092,8,4]	11971	
10	15	[1, 0, –4, 4, –4, 4]	1637		48	97	[1, 4, 0, –8, –4, 4]	12923	α
11	16	[5, –24, 44, –36, 8, 4]	1811	α	49	100	[1, 12, 32, 28, 8, 4]	13147	α
12	18	[1, 4, 4, 4, 8, 4]	2243	α	50	101	[1, –4, 4, –4, 4, 4]	13147	α
13	20	[–3, –4, 0, 8, 8, 4]	2341	α	51	102	[5, –28, 48, –24, –4, 4]	13259	
14	22	[5, –16, 20, –8, –4, 4]	2677	α	52	105	[1, –4, 0, 4, 8, 4]	13723	
15	23	[1, 0, 0, 4, 8, 4]	2693		53	108	[137, –356, 328, –116, 4, 4]	13997	
16	27	[1, 4, –8, –4, 4, 4]	3251	α	54	111	[9, 16, –4, –16, 0, 4]	14197	
17	29	[9, –40, 60, –32, 0, 4]	3499		55	118	[1, 4, –8, –4, 8, 4]	15307	
18	30	[1, 0, 0, 4, –8, 4]	3557		56	122	[1, 4, 4, 8, 8, 4]	15749	
19	31	[1, 0, 4, 0, 4, 4]	3637	α	57	131	[1, –4, 4, 0, –8, 4]	17291	
20	32	[161, –360, 284, –80, –4, 4]	3701	α	58	132	[–3, 8, –8, 8, –8, 4]	17317	
21	34	[1, –4, 4, 0, 0, 4]	3989		59	135	[1, 0, 0, –4, 4, 4]	17389	α
22	37	[–3, 8, –12, 12, –8, 4]	4157	α	60	138	[–3, –20, –40, –20, 4, 4]	18077	α
23	39	[1, –4, 8, –8, 4, 4]	4517	α	61	144	[–247, 552, –200, –136, 4, 4]	19211	
24	40	[–3, 8, 0, –12, 4, 4]	5059	α	62	144	[–7, 16, 4, –16, 0, 4]	19211	
25	41	[5, –20, –40, 240, –600, 500]	5227		63	145	[–3, 36, –144, 192, –108, 108]	19429	
26	46	[5185,–6384,2664,–396,–4,4]	5651	α	64	147	[–11, –44, 264, 440, 968, 5324]	19531	α
27	47	[73, –180, 152, –40, –8, 4]	5867		65	152	[–3, –4, 8, 4, –8, 4]	21211	α
28	52	[1, 4, 0, –8, 4, 4]	6491		66	154	[–21167, –18908, –5996, –712, 0, 4]	21563	
29	54	[–3, 4, 4, –8, 0, 4]	6763		67	156	[–3, –16, –28, –16, 4, 4]	21787	
30	57	[25, 28, –12, –16, 4, 4]	7109		68	157	[9, –32, 40, –20, 0, 4]	22277	
31	62	[41, –148, 160, –56, –4, 4]	7877		69	158	[1, –4, 8, –12, 4, 4]	22291	
32	62	[1, 8, 12, –8, –8, 4]	7877		70	162	[1, 4, 8, 4, 4, 4]	22861	
33	62	[73, –228, 232, –84, 0, 4]	7877		71	163	[5, –36, 76, –40, 4, 4]	23003	
34	64	[–591,–1160,–792,–204,–4,4]	8243	α	72	165	[1909, –2652, 1308, –236, –4, 4]	23131	
35	66	[1, –8, 20, –12, –8, 4]	8803		73	165	[1, 8, –12, –8, 8, 4]	23131	
36	67	[1, –8, 24, –28, 4, 4]	9091	α	74	169	[1, 8, 20, 16, 0, 4]	24469	
37	69	[1, –8, 16, –8, –4, 4]	9803		75	169	[7309, –8208, 3292, –504, 4, 4]	24469	
38	70	[1, 8, 20, 16, 8, 4]	9941	α					

Table 2. Curves $y^2 = g(x)$, their 2-division fields and conductors (legend on page 1065).

Legend for Tables 3 and 4. We know 276109 curves, including 10360 mild curves with $3 \le m \le 53$, whose Jacobians are favorable and nonisogenous of prime conductor $N < 10^{10}$, for a total of 275494 nonisomorphic fields. Table 3 summarizes the statistics. For $0 \le j \le 9$, the j-th column refers to N between $j \cdot 10^9$ and $(j+1) \cdot 10^9$. The rows A, F and α, respectively, give the number of abelian varieties, fields and amiable fields. It is remarkable that approximately 11.8% of the favorable fields are amiable, uniformly for each slice of size 10^9. For the reader's entertainment, Table 4 lists the curves we found with largest conductors below 10^{10} and amiable Jacobians.

j	0	1	2	3	4	5	6	7	8	9	Total
A	63563	35507	29047	25450	23684	22099	20500	19505	18773	17981	276109
F	63212	35429	28998	25417	23657	22079	20479	19493	18761	17969	275494
α	7632	4290	3362	2948	2799	2606	2375	2340	2189	2127	32668

Table 3. Amiable fields among favorable fields (legend immediately above).

$P(x)$	N	$P(x)$	N
$[-90, -184, -136, -39, -1, 1]$	9882329341	$[10, 22, 7, -7, 0, 1]$	9891907261
$[11, 26, -7, -8, 0, 1]$	9893121157	$[11, 17, 3, -4, -2, 1]$	9897613669
$[-8428, -6910, -2025, -226, -1, 1]$	9898501189	$[-21, 6, 10, -1, 1, 1]$	9911121709
$[87, -106, 56, -9, -2, 1]$	9934582709	$[-61, 50, 9, -13, 0, 1]$	9982174061
$[-33, 20, -1, 10, 1, 1]$	9987633941	$[-2, -3, -15, -9, 0, 1]$	9994370909

Table 4. Curves $y^2 = 1 + 4P(x)$ of large conductor with amiable fields (legend at top of page).

Note added in proof

The paramodular conjecture should be modified to accommodate comments and examples of Frank Calegari.

Definition. An abelian fourfold B is a *fake abelian surface* if $\mathrm{End}(B)$ is an order in a quaternion algebra over $\mathbb{Q}$.

Paramodular conjecture. *Let $\mathcal{A}_N$ be the set of isogeny classes of abelian surfaces $A/\mathbb{Q}$ of conductor N with $\mathrm{End}\, A = \mathbb{Z}$, let $\mathcal{B}_N$ be the set of isogeny classes of fake abelian surfaces $B/\mathbb{Q}$ of conductor N^2 and let $\mathcal{P}_N$ be the set of cuspidal, nonlift Siegel paramodular newforms f of genus 2, weight 2 and level N with rational Hecke eigenvalues, up to nonzero scaling. Then there is a bijection between $\mathcal{P}_N$ and $\mathcal{A}_N \cup \mathcal{B}_N$ such that*

$$L(C, s) = \begin{cases} L(f, s, \mathrm{spin}) & \text{if } C \in \mathcal{A}_N, \\ L(f, s, \mathrm{spin})^2 & \text{if } C \in \mathcal{B}_N. \end{cases}$$

Acknowledgements

The authors wish to express their gratitude to the anonymous referees for their extremely careful reading of the manuscript. Their valuable suggestions helped us clarify and improve the exposition. Magma [Bosma et al. 1997], obtained with the aid of the Simons Foundataion, was used in some of our computations.

References

[Abrashkin 1987] V. A. Abrashkin, "Galois modules of group schemes of period p over the ring of Witt vectors", *Izv. Akad. Nauk SSSR Ser. Mat.* **51**:4 (1987), 691–736, 910. In Russian; translated in *Izvestiya Math.* **31**:4 (1988), 1–46. MR Zbl

[Berger et al. 2015] T. Berger, L. Dembélé, A. Pacetti, and M. H. Şengün, "Theta lifts of Bianchi modular forms and applications to paramodularity", *J. Lond. Math. Soc.* (2) **92**:2 (2015), 353–370. MR Zbl

[Berthelot 1977] P. Berthelot, "Systèmes de Honda des schémas en F_q-vectoriels", *Bull. Soc. Math. France* **105**:3 (1977), 225–239. MR Zbl

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Brinon and Conrad 2009] O. Brinon and B. Conrad, "CMI summer school notes on p-adic Hodge Theory", lecture notes, Stanford Univerisy, 2009, Available at http://math.stanford.edu/~conrad/papers/notes.pdf.

[Brumer and Kramer 2001] A. Brumer and K. Kramer, "Non-existence of certain semistable abelian varieties", *Manuscripta Math.* **106**:3 (2001), 291–304. MR Zbl

[Brumer and Kramer 2004] A. Brumer and K. Kramer, "Semistable abelian varieties with small division fields", pp. 13–37 in *Galois theory and modular forms*, edited by K.-i. Hashimoto et al., Dev. Math. **11**, Kluwer Acad. Publ., Boston, MA, 2004. MR Zbl

[Brumer and Kramer 2012] A. Brumer and K. Kramer, "Arithmetic of division fields", *Proc. Amer. Math. Soc.* **140**:9 (2012), 2981–2995. MR Zbl

[Brumer and Kramer 2014] A. Brumer and K. Kramer, "Paramodular abelian varieties of odd conductor", *Trans. Amer. Math. Soc.* **366**:5 (2014), 2463–2516. MR Zbl

[Brumer and Kramer 2018] A. Brumer and K. Kramer, "Large 2-adic Galois image and non-existence of certain abelian surfaces over $\mathbb{Q}$", *Acta Arith.* **183**:4 (2018), 357–383. MR

[Brumer and McGuinness 1990] A. Brumer and O. McGuinness, "310716 elliptic curves of prime conductor", electronic reference, 1990, Available at http://www.math.columbia.edu/~om/.

[Calegari 2004] F. Calegari, "Semistable abelian varieties over $\mathbb{Q}$", *Manuscripta Math.* **113**:4 (2004), 507–529. MR Zbl

[Conrad 1999] B. Conrad, "Finite group schemes over bases with low ramification", *Compositio Math.* **119**:3 (1999), 239–320. MR Zbl

[Eilenberg and MacLane 1942] S. Eilenberg and S. MacLane, "Group extensions and homology", *Ann. of Math.* (2) **43** (1942), 757–831. MR Zbl

[Faltings 1983] G. Faltings, "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern", *Invent. Math.* **73**:3 (1983), 349–366. MR Zbl

[Fontaine 1975a] J.-M. Fontaine, "Groupes finis commutatifs sur les vecteurs de Witt", *C. R. Acad. Sci. Paris Sér. A-B* **280** (1975), Ai, A1423–A1425. MR Zbl

[Fontaine 1975b] J.-M. Fontaine, "Groupes p-divisibles sur les vecteurs de Witt", *C. R. Acad. Sci. Paris Sér. A-B* **280** (1975), Ai, A1353–A1356. MR Zbl

[Fontaine 1977] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Société Mathématique de France, Paris, 1977. Astérisque, No. 47-48. MR Zbl

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

[Grothendieck and Raynaud 1972] A. Grothendieck and M. Raynaud, *Modeles de neron et monodromie*, pp. 313–523, Springer, Berlin, Heidelberg, 1972. Zbl

[Johnson-Leung and Roberts 2012] J. Johnson-Leung and B. Roberts, "Siegel modular forms of degree two attached to Hilbert modular forms", *J. Number Theory* **132**:4 (2012), 543–564. MR Zbl

[Johnson-Leung and Roberts 2017] J. Johnson-Leung and B. Roberts, "Twisting of Siegel paramodular forms", *Int. J. Number Theory* **13**:7 (2017), 1755–1854. MR Zbl

[Kemper and Malle 1997] G. Kemper and G. Malle, "The finite irreducible linear groups with polynomial ring of invariants", *Transform. Groups* **2**:1 (1997), 57–89. MR Zbl

[Lang 1994] S. Lang, *Algebraic number theory*, 2nd ed., Graduate Texts in Mathematics **110**, Springer, 1994. MR Zbl

[Mac Lane 1963] S. Mac Lane, *Homology*, Grundlehren der math. Wissenschaften **114**, Springer, Berlin, 1963. MR Zbl

[Mazur 1977] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* 47 (1977), 33–186. MR Zbl

[Merriman and Smart 1993] J. R. Merriman and N. P. Smart, "Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point", *Math. Proc. Cambridge Philos. Soc.* **114**:2 (1993), 203–214. MR Zbl

[Milne 1972] J. S. Milne, "On the arithmetic of abelian varieties", *Invent. Math.* **17** (1972), 177–190. MR Zbl

[Ploner 2015] P. Ploner, "Computation of framed deformation functors", *J. Number Theory* **156** (2015), 21–37. MR Zbl

[Poor and Yuen 2015] C. Poor and D. S. Yuen, "Paramodular cusp forms", *Math. Comp.* **84**:293 (2015), 1401–1438. MR Zbl

[Raynaud 1974] M. Raynaud, "Schémas en groupes de type $(p, \dots, p)$", *Bull. Soc. Math. France* **102** (1974), 241–280. MR Zbl

[Schoof 2003] R. Schoof, "Abelian varieties over cyclotomic fields with good reduction everywhere", *Math. Ann.* **325**:3 (2003), 413–448. MR Zbl

[Schoof 2005] R. Schoof, "Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only", *Compos. Math.* **141**:4 (2005), 847–868. MR Zbl

[Schoof 2012a] R. Schoof, "On the modular curve $X_0(23)$", pp. 317–345 in *Geometry and arithmetic*, edited by C. Faber et al., Eur. Math. Soc., Zürich, Switzerland, 2012. MR Zbl

[Schoof 2012b] R. Schoof, "Semistable abelian varieties with good reduction outside 15", *Manuscripta Math.* **139**:1-2 (2012), 49–70. MR Zbl

[Serre 1979] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics **67**, Springer, 1979. MR Zbl

[Setzer 1981] B. Setzer, "Elliptic curves with good reduction everywhere over quadratic fields and having rational j-invariant", *Illinois J. Math.* **25**:2 (1981), 233–245. MR Zbl

[Shimura 1972] G. Shimura, "Class fields over real quadratic fields and Hecke operators", *Ann. of Math.* (2) **95** (1972), 130–190. MR Zbl

[Smart 1997] N. P. Smart, "S-unit equations, binary forms and curves of genus 2", *Proc. London Math. Soc.* (3) **75**:2 (1997), 271–307. MR Zbl

[Tate 1997] J. Tate, "Finite flat group schemes", pp. 121–154 in *Modular forms and Fermat's last theorem* (Boston, MA, 1995), edited by G. Cornell et al., Springer, New York, 1997. MR Zbl

Communicated by Brian Conrad
Received 2016-09-01 Revised 2017-08-20 Accepted 2017-10-23

brumer@fordham.edu *Department of Mathematics, Fordham University, Bronx, NY, United States*

kkramer@qc.cuny.edu *Department of Mathematics, Queens College (CUNY), Flushing, NY, United States*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Richard E. Borcherds	University of California, Berkeley, USA
Antoine Chambert-Loir	Université Paris-Diderot, France
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France
Brian D. Conrad	Stanford University, USA
Samit Dasgupta	University of California, Santa Cruz, USA
Hélène Esnault	Freie Universität Berlin, Germany
Gavril Farkas	Humboldt Universität zu Berlin, Germany
Hubert Flenner	Ruhr-Universität, Germany
Sergey Fomin	University of Michigan, USA
Edward Frenkel	University of California, Berkeley, USA
Andrew Granville	Université de Montréal, Canada
Joseph Gubeladze	San Francisco State University, USA
Roger Heath-Brown	Oxford University, UK
Craig Huneke	University of Virginia, USA
Kiran S. Kedlaya	Univ. of California, San Diego, USA
János Kollár	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne
Susan Montgomery	University of Southern California, USA
Shigefumi Mori	RIMS, Kyoto University, Japan
Martin Olsson	University of California, Berkeley, USA
Raman Parimala	Emory University, USA
Jonathan Pila	University of Oxford, UK
Anand Pillay	University of Notre Dame, USA
Michael Rapoport	Universität Bonn, Germany
Victor Reiner	University of Minnesota, USA
Peter Sarnak	Princeton University, USA
Joseph H. Silverman	Brown University, USA
Michael Singer	North Carolina State University, USA
Christopher Skinner	Princeton University, USA
Vasudevan Srinivas	Tata Inst. of Fund. Research, India
J. Toby Stafford	University of Michigan, USA
Pham Huu Tiep	University of Arizona, USA
Ravi Vakil	Stanford University, USA
Michel van den Bergh	Hasselt University, Belgium
Marie-France Vignéras	Université Paris VII, France
Kei-Ichi Watanabe	Nihon University, Japan
Shou-Wu Zhang	Princeton University, USA

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2018 is US $340/year for the electronic version, and $535/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2018 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 12 No. 5 2018

1937-0652(2018)12:5;1-C