TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 366, Number 5, May 2014, Pages 2463–2516
S 0002-9947(2013)05909-0
Article electronically published on November 21, 2013

PARAMODULAR ABELIAN VARIETIES OF ODD CONDUCTOR

ARMAND BRUMER AND KENNETH KRAMER

ABSTRACT. A precise and testable modularity conjecture for rational abelian surfaces A with trivial endomorphisms, $\mathrm{End}_{\mathbb{Q}} A = \mathbb{Z}$, is presented. It is consistent with our examples, our non-existence results and recent work of C. Poor and D. S. Yuen on weight 2 Siegel paramodular forms. We obtain fairly precise information on ℓ-division fields of *semistable* abelian varieties, mainly when $A[\ell]$ is reducible, by considering extension problems for group schemes of small rank.

CONTENTS

Received by the editors May 24, 2010 and, in revised form, July 4, 2012.
2010 *Mathematics Subject Classification.* Primary 11G10; Secondary 14K15, 11F46.
Key words and phrases. Abelian variety, finite flat group scheme, polarization, division field, paramodular group.
The research of the second author was partially supported by NSF grant DMS 0739346.

1. Introduction

The Langlands philosophy suggests that the L-series of an abelian surface A over $\mathbb{Q}$ might be that associated to a Siegel cuspidal eigenform of weight 2 with rational eigenvalues, for some unspecified group commensurable with $\mathrm{Sp}_4(\mathbb{Z})$. We recall from [58] that the ring of endomorphisms of abelian surfaces A can be either $\mathbb{Z}$ or an order in a quadratic number field k. The latter A are of GL_2-type, as defined by [46]. It is thus a consequence of the work of Khare and Winterberger [27] on the Serre conjecture that they are classically modular and their L-series are products of two L-functions attached to newforms on $\Gamma_0(N)$ or $\Gamma_1(N)$, depending on whether or not k is real. All examples of modularity known to us ([50], [36], [59]) involve surfaces of GL_2-type and depend on the lift from classical forms to Siegel modular forms created by Yoshida [70] for this purpose. Deep work by Tilouine ([64], [65]) and Pilloni ([37]) uses Hida families to obtain overconvergent p-adic modular forms associated to certain abelian surfaces under strong assumptions.

Our long term project, originally a study of genus two curves of prime conductor provoked by the thesis of Jaap Top [66], became a search for a precise and *testable* modularity conjecture for *all* abelian surfaces A defined over $\mathbb{Q}$ and *not* of GL_2-type, that is, those for which $\mathrm{End}_{\mathbb{Q}}(A) = \mathbb{Z}$. We believe we have found one.

The appropriate modular forms are on the paramodular group ([23], [16]) of level N, namely $K(N) = \gamma \mathrm{M}_4(\mathbb{Z})\gamma^{-1} \cap \mathrm{Sp}_4(\mathbb{Q})$, with $\gamma = \mathrm{diag}[1,1,N,1]$. Explicitly:

$$K(N) \quad = \quad \left\{ g \in \mathrm{Sp}_4(\mathbb{Q}) \;\middle|\; g = \begin{bmatrix} * & * & */N & * \\ N* & * & * & * \\ N* & N* & * & N* \\ N* & * & * & * \end{bmatrix} \right\},$$

where $*$ is an integer. The quotient of the Siegel upper half space $\mathfrak{H}_2$ by $K(N)$ is the coarse moduli space of abelian surfaces with $(1,N)$-polarization [3]. In order to study its Kodaira dimension, Gritsenko ([16], [17]) introduced a Hecke-equivariant lift from classical Jacobi forms $J_{k,N}$ to paramodular forms of weight k on $K(N)$, as a variant of the Saito-Kurokawa lift. These lifts violate the Ramanujan bounds and their L-series have poles, and so appear to be of no interest. In fact, they play a crucial role in the construction of the desired paramodular cuspforms [39]. In [48], *newforms* on $K(N)$ are defined as Hecke eigenforms perpendicular to the images of operators from paramodular forms on lower levels. We shall refer to those newforms of weight 2 perpendicular to the Gritsenko lifts as *non-lifts* on $K(N)$.

Let $\mathbb{T}_\ell(A) = \varprojlim A[\ell^n]$ be the Tate module of A. Motivated by results of [2], [47], [62] and by the compatibility with standard conjectures [56] on the Hasse-Weil L-series $L(A,s)$, we propose the following hypothesis.

Conjecture 1.1. *There is a one-to-one correspondence between isogeny classes of abelian surfaces $A_{/\mathbb{Q}}$ of conductor N with* $\mathrm{End}_{\mathbb{Q}} A = \mathbb{Z}$ *and weight* 2 non-lifts f *on $K(N)$ with rational eigenvalues, up to scalar multiplication. Moreover, the L-series of A and f should agree and the ℓ-adic representation of $\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell$ should be isomorphic to those associated to f for any ℓ prime to N.*

In contrast to Shimura's classical construction from elliptic newforms, no known method yields an abelian surface from a Siegel eigenform.

It is difficult to determine the number of non-lift newforms f on $K(N)$ and more than a few Euler factors of $L(f,s)$. Counting isogeny classes of surfaces of given conductor is even less accessible. However, it is easy to compute as many Euler factors as desired for an explicitly known abelian surface.

Throughout this paper, $\mathfrak{o}$ denotes the ring of integers of a totally real number field of degree d and $\mathfrak{l}$ a prime of $\mathfrak{o}$ above ℓ with residue field $\mathbb{F}_{\mathfrak{l}}$. The reader might, on first reading, keep in mind the most important case, namely $d = 1$ and so $\mathfrak{o} = \mathbb{Z}$. Our excuses for handling the more general situation are threefold. Our arguments applied without much extra effort, except slightly more notation. As explained below, they provide more evidence toward our conjectures. Finally, it seems an entertaining challenge to produce examples, for instance, of abelian fourfolds A with $\mathrm{End}_{\mathbb{Q}} A$ an order in a quadratic number field.

Definition 1.2. The abelian variety $A_{/\mathbb{Q}}$ is of $\mathfrak{o}$-*type* if $\mathrm{End}_{\mathbb{Q}} A \simeq \mathfrak{o}$. Its conductor has the shape $N_A = N^d$ (cf. Lemma 3.2.9), and the reduced conductor is $N_A^0 := N$. When $\dim A = 2d$, we say A is $(\mathfrak{o}, N)$-*paramodular*.

Remark 1.3.

i) An $\mathfrak{o}$-type abelian variety with $\dim A = d$ has real multiplication and so, by [27], is a quotient of $J_0(N)$, the Jacobian of the modular curve $X_0(N)$, where N is the *reduced* conductor.
ii) An $(\mathfrak{o}, N)$-*paramodular* abelian variety is $\mathbb{Q}$-simple, is *not* of GL_2-type and its Rosati involution acts trivially on $\mathfrak{o}$.
iii) A surface $A_{/\mathbb{Q}}$ is paramodular exactly when $\mathrm{End}_{\mathbb{Q}} A = \mathbb{Z}$, but $\mathrm{End}_{\overline{\mathbb{Q}}} A$ might be larger. If K is a quadratic field and $E_{/K}$ is an elliptic curve, not K-isogenous to its conjugate, then the Weil restriction $A = R_{K/\mathbb{Q}} E$ is paramodular.

Guided by the case of abelian varieties over $\mathbb{Q}$ with real multiplications, a more optimistic conjecture generalizing our earlier one is the following.

Conjecture 1.4. *Let f be a weight 2 non-lift for $K(N)$. Let $\mathfrak{o}$ be the maximal order in the totally real number field k_f generated by the Hecke eigenvalues of f. Then there is an $(\mathfrak{o}, N)$-paramodular abelian variety A_f with $L(A_f, s) = \prod_\sigma L(f^\sigma, s)$, where σ runs through the embeddings of k_f into $\mathbb{R}$. Conversely, an abelian variety A of $(\mathfrak{o}, N)$-paramodular type should be isogenous to A_f for a weight 2 non-lift newform f on $K(N)$.*

Current technology might verify our conjecture for Weil restrictions of elliptic curves (cf. [63]) and surfaces with $\mathrm{End}_{\overline{\mathbb{Q}}} A \supsetneq \mathbb{Z}$. In fact, [25][1] implies that if an elliptic curve over a real quadratic field is "Hilbert modular", then its Weil restriction is paramodular of the predicted level (see Appendix B). It is conceivable that our precise paramodular conjecture could be proved, assuming that the L-series of a paramodular surface is the L-series of a cuspidal automorphic representation of $\mathrm{GSp}_4(\mathbb{A}_{\mathbb{Q}})$.

To support the conjectures on the arithmetic side, we must prove that no $(\mathfrak{o}, N)$-paramodular variety A exists when no paramodular non-lift exists and produce a member of each isogeny class for each non-lift that does exist. For comparison, few results on non-existence or counts of elliptic curves of a given conductor N were known before modularity was proved, even though the issue reduces to S-integral points on the discriminant elliptic curves $c_4^3 - c_3^2 = 1728\Delta$, for Δ involving only primes of N. For abelian surfaces A, there is no analogous diophantine equation

[1]We thank Brooks Roberts for sending us their preprint upon receipt of our manuscript.

and the problem is exacerbated by the plethora of group schemes available as constituents of $A[\ell]$, as illustrated by Appendix A. The profusion of intricate lemmas reflects the existence of varieties satisfying conditions close to the ones we impose. We mention some of the subtleties encountered below.

i) When we show that there is no abelian surface of conductor N, our proof actually shows that there is no semistable $(\mathfrak{o}, N)$-paramodular abelian variety A with $|\mathbb{F}_{\mathfrak{l}}| = 2$. In some cases, Conjecture 1.4 and likely paramodular forms suggest that such $(\mathfrak{o}, N)$-paramodular A's of dimension at least four do exist, explaining why N was not eliminated.
ii) There are non-semistable abelian surfaces B such that $B[\ell] \simeq A[\ell]$ as Galois modules, for a putative semistable surface A.
iii) The conductor of $A[\ell]$ can be a proper divisor of the conductor of the abelian surface A. This makes it difficult to rule out divisors and multiples of conductors of existing abelian surfaces.

This paper mainly treats non-existence. The abelian variety $A_{/\mathbb{Q}}$ is semistable if, for each prime p, the connected component of the special fiber of its Néron model $\mathcal{A}$ fits into

$$0 \to \mathcal{T}_p \to \mathcal{A}_p^0 \to \mathcal{B}_p \to 0 \tag{1.5}$$

with $\mathcal{B}_p$ an abelian variety and $\mathcal{T}_p$ a torus. When A is semistable, deep results of Grothendieck [20] and Fontaine [15] imply that the number fields $\mathbb{Q}(A[\ell^n])$ have such tightly controlled ramification that their non-existence rules out certain conductors. For this reason we specialize to semistable abelian varieties.

Remark 1.6.

i) Lemma 3.2.9 shows that an $(\mathfrak{o}, N)$-paramodular variety is semistable if N is *squarefree*. This is not necessary: the conductor of a semistable paramodular surface with totally toroidal reduction at p is divisible by p^2.
ii) All endomorphisms of A are defined over $\mathbb{Q}$ when A is semistable [43]. In particular, a semistable paramodular variety is absolutely simple.

No algorithm to find all abelian surfaces of a given conductor is known, particularly those not $\mathbb{Q}$-isogenous to a Jacobian, so we looked for surfaces by whatever method we could. We include non-principally polarized surfaces and Jacobians $J(C)$ of a conductor N such that C has bad reduction consisting of two genus one curves meeting in one point at some primes $p \nmid N$ (see Appendix B). As a special case of Theorem 3.4.11, based on [27] and [21], a paramodular abelian surface of *prime* conductor is $\mathbb{Q}$-isogenous to a Jacobian.

As a concrete numerical application of our general results:

Proposition 1.7. *Suppose A is a semistable abelian surface with* odd *non-square conductor N.*

i) *If $N \leq 500$, then N can only be* $249, 277, 295, 349, 353, 389, 427, 461$*, for which examples are known, or* $415, 417$*, which should* not *occur.*
ii) *See Tables* 1 *and* 2 *for the data obtained for odd conductors $N < 1000$.*

The work of Poor and Yuen provides support for our conjecture. Tables of cusp forms of weight 2 on $K(N)$ for *primes* $N \leq 600$ are in [39]. For *all* conductors $N \leq 1000$ and a few other values, further evidence will be in [40].

We compare our results with theirs, including some still unpublished data. There are at least as many known or suspected paramodular non-lift newforms of weight two with rational eigenvalues as known isogeny classes of paramodular surfaces, including those not semistable or of even conductor. For almost all non-lifts f, we found an abelian surface A of the same conductor whose Euler factors agree with those of f at *very small* primes. Also, the parity of the rank of $A(\mathbb{Q})$ matches that predicted by the ϵ-factor of f. When we showed that no abelian surface of a given conductor $N < 1000$ exists, their data suggest that all weight 2 paramodular newforms with rational eigenvalues are Gritsenko lifts.

Suppose A has a polarization of degree prime to q and a torsion point of order q. Then there is a filtration on $A[q]$ with a subgroup and, by duality, a quotient of order q. Thus, the characteristic polynomial of Frobenius at a prime ℓ of good reduction is congruent to $H_\ell(x) = (1-x)(1-\ell x)(1-a_\ell x+\ell x^2) \bmod q$. By Serre's conjecture [27, 57], there is an eigenform g of weight 2 on $\Gamma_0(N)$ with Euler polynomial at ℓ congruent to $(1-a_\ell x+\ell x^2) \bmod \mathfrak{q}$ for some $\mathfrak{q} \mid q$. Since H_ℓ is the Euler factor of the Gritsenko lift $G(g)$ of a Jacobi form attached to g, this suggests the possibility of a congruence mod $\mathfrak{q}$ between the Fourier series of the non-lift f associated to A by our conjecture and $G(g)$. Such matching congruences were found in [39] and lend further supporting evidence.

While the data is far from complete, it seems convincing enough for publication and dissemination of the conjecture, at least as a challenge.

Recall that the Langlands dual group of GSp_{2g} is $\mathrm{SO}(2g+1)$. When interpreted on the split orthogonal group $\mathrm{SO}(g+1, g)$ and its associated homogenous space, the groups $\Gamma_0(N)$ for $g = 1$ and $K(N)$ for $g = 2$, which at first sight seem so different, are both instances of similar subgroups. Let L be an integral lattice with inner product. There is a natural map $\tau_L \colon \mathrm{SO}(L) \to \mathrm{O}(\hat{L}/L)$, where $\hat{L}$ is the dual lattice of L. The stable orthogonal group $\widetilde{\mathrm{O}}(L)$ is the intersection of the kernel of τ_L and the spinor map [18, 33]. Let $\mathbb{H}$ be the hyperbolic plane and consider the lattice $\mathbb{L}_g(N) = \mathbb{H}^g \perp \langle 2N \rangle$, where $\langle 2N \rangle$ is spanned by a vector of length $2N$. By [18, Prop. 1.2 and p. 485], $K(N)/\langle \pm 1 \rangle$ corresponds to $\widetilde{\mathrm{O}}(\mathbb{L}_2)$ under the identification of GSp_4 with $\mathrm{SO}(3,2)$. Similarly, $\Gamma_0(N)/\langle \pm 1 \rangle$ corresponds to $\widetilde{\mathrm{O}}(\mathbb{L}_1)$ in the identification of PSL_2 with $\mathrm{SO}(2,1)$. Upon learning this at the June 2010 Conference in his honor, B. Gross immediately generalized our conjecture to one for symplectic motives in a letter to Serre [19].

2. Overview of the paper

To avoid excessive repetition, we adhere to some conventions for the whole paper. For any finite set S of primes, let $\mathbb{Z}_S = \mathbb{Z}[\{p^{-1} \mid p \in S\}]$ and ℓ always be a prime not in S. Write p_v for the prime in $\mathbb{Z}$ below the valuation v. The constant group scheme of order ℓ over $\mathbb{Z}_S$ is denoted $\mathcal{Z}_\ell = \mathbb{Z}/\ell\mathbb{Z}$ and its Cartier dual is $\boldsymbol{\mu}_\ell$. We use $\mathfrak{o}$ for the Dedekind ring of integers in a totally real number field of degree d and $\mathfrak{l}$ for a prime ideal of $\mathfrak{o}$ over ℓ. An $\mathfrak{o}$-module scheme [61, p. 148] is an abelian group scheme $\mathcal{W}$ with a homomorphism from $\mathfrak{o}$ to $\operatorname{End} \mathcal{W}$. The associated Galois module is the $\mathfrak{o}$-module of points $W = \mathcal{W}(\overline{\mathbb{Q}})$. We have the one-dimensional $\mathbb{F}_\mathfrak{l}$-module schemes $\boldsymbol{\mu}_\mathfrak{l} = \boldsymbol{\mu}_\ell \otimes_{\mathbb{F}_\ell} \mathbb{F}_\mathfrak{l}$ and $\mathcal{Z}_\mathfrak{l} = (\mathbb{Z}/\ell\mathbb{Z}) \otimes_{\mathbb{F}_\ell} \mathbb{F}_\mathfrak{l}$, defined in [29, p. 46]. We reserve $\mathcal{Z}$ (resp. $\mathcal{M}$) for an étale (resp. multiplicative) $\mathfrak{l}$-primary $\mathfrak{o}$-module scheme over $\mathbb{Z}_S$, all of whose simple constituents are isomorphic to $\mathcal{Z}_\mathfrak{l}$ (resp. $\boldsymbol{\mu}_\mathfrak{l}$). We shall shorten this to "filtered by $\mathcal{Z}_\mathfrak{l}$'s" or "filtered by $\boldsymbol{\mu}_\mathfrak{l}$'s".

We often abbreviate "abelian variety" to "variety" since, aside from curves, they are the only varieties we consider. We henceforth assume that **all abelian varieties are semistable of $\mathfrak{o}$-type and isogenies are $\mathfrak{o}$-linear**, unless the contrary is explicitly stated. We denote by N_A the conductor of the abelian variety A.

For the cases originally studied in [6, 15, 51], the discriminants of the fields encountered were small enough to ensure that the only simple group schemes occurring were $\boldsymbol{\mu}_\ell$ and $\mathbb{Z}/\ell\mathbb{Z}$, with their extensions being split. To prove our non-existence results we need to consider other simple groups schemes and non-split extensions.

Accordingly, we generalize an important category introduced by Schoof in [51]. Fix a set S of primes and a prime $\mathfrak{l}$ in $\mathfrak{o}$ above ℓ not in S. Let $\underline{A}$ be the category of finite flat $\mathfrak{l}$-primary module schemes $\mathcal{W}$ over $\mathbb{Z}_S$. Let $\underline{D}$ be the full subcategory of those such that $(\sigma-1)^2 = 0$ on the associated Galois module W for all σ in the inertia groups of the places over S. Clearly, $\mathcal{Z}_\mathfrak{l}$ and $\boldsymbol{\mu}_\mathfrak{l}$ belong to $\underline{D}$.

Let A be a semistable abelian variety of $\mathfrak{o}$-type with good reduction outside S. As in [51], Grothendieck's semistable reduction theorem [20] implies that $A[\mathfrak{l}^n]$ and its subquotients belong to $\underline{D}$. The *exceptional* $\mathbb{F}_\mathfrak{l}$-module schemes are the simple constituents of $A[\mathfrak{l}]$ *not* isomorphic to $\mathcal{Z}_\mathfrak{l}$ or $\boldsymbol{\mu}_\mathfrak{l}$, if any. The associated Galois modules, also called *exceptional*, are thus the irreducibles whose $\mathbb{F}_\mathfrak{l}$-dimension is at least two. Let $\mathfrak{S}_\mathfrak{l}^{all}(A)$ be the multiset of simple $\mathbb{F}_\mathfrak{l}[G_\mathbb{Q}]$-modules in a composition series for $A[\mathfrak{l}]$ and $\mathfrak{S}_\mathfrak{l}(A)$ be the multiset of exceptionals, each with its multiplicity. By Proposition 3.2.10, $\mathfrak{S}_\mathfrak{l}^{all}(A)$ and $\mathfrak{S}_\mathfrak{l}(A)$ are isogeny invariants.

An $\mathfrak{l}$-primary $\mathfrak{o}$-module scheme in $\underline{D}$ is *prosaic* if all its simple constituents are one-dimensional $\mathbb{F}_\mathfrak{l}$-module schemes. To account for the obstruction to switching adjacent simple constituents in a composition series, the concept of a *nugget* is developed in §4. A *prosaic nugget* is an $\mathfrak{o}$-module scheme $\mathcal{W}$ such that $0 \subsetneq \mathcal{Z} \subsetneq \mathcal{W}$, with $\mathcal{Z}$ filtered by $\mathcal{Z}_\mathfrak{l}$'s and $\mathcal{W}/\mathcal{Z} = \mathcal{M}$ filtered by $\boldsymbol{\mu}_\mathfrak{l}$'s, and no increasing filtration of $\mathcal{W}$ has a $\boldsymbol{\mu}_\mathfrak{l}$ occurring before a $\mathcal{Z}_\mathfrak{l}$. See §4 for the more delicate notion and properties of a nugget with an exceptional subquotient.

Theorem 5.3 constrains the number of one-dimensional constituents of $A[\mathfrak{l}]$. Put $\Omega(n) = \sum_p \operatorname{ord}_p(n)$ and $\Omega_\ell(n) = \sum_{S_\ell} \operatorname{ord}_p(n)$, where $S_\ell = \{\text{primes } p \equiv \pm 1 \mod \tilde{\ell}\}$ with $\tilde{\ell} = 8$ if $\ell = 2$, $\tilde{\ell} = 9$ if $\ell = 3$ and $\tilde{\ell} = \ell$ otherwise. Then Corollary 5.4 gives

$$2 \dim A \leq \Omega(N_A) + \Omega_\ell(N_A)$$

when $\mathbb{Q}(A[\mathfrak{l}])$ is an ℓ-extension of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$. There are hyperelliptic Jacobians of small dimension for which $A[\ell]$ is prosaic and the upper bound is attained for $\ell = 2$.

Notation 2.1. Let $\mathfrak{I}_A$ be the category of abelian varieties $\mathbb{Q}$-isogenous to A, with isogenies as morphisms. If A is of $\mathfrak{o}$-type, $\mathfrak{I}_A^\mathfrak{l}$ is the subcategory of abelian varieties of $\mathfrak{o}$-type whose morphisms are $\mathfrak{o}$-isogenies with $\mathfrak{l}$-primary kernels.

In §6, we introduce the concept of a *mirage*. A mirage $\mathfrak{C}$ associates to each B in $\mathfrak{I}_A^\mathfrak{l}$ a set $\mathfrak{C}(B)$ of certain $\mathbb{F}_\mathfrak{l}$-module subschemes of $B[\mathfrak{l}]$, with natural maps induced by isogenies. As an example, $\mathfrak{C}(B)$ might be the set of $\mathbb{F}_\mathfrak{l}$-subschemes of $B[\mathfrak{l}]$ filtered by $\boldsymbol{\mu}_\mathfrak{l}$'s. Other choices depend on Grothendieck's filtration of the Tate module at semistable primes of bad reduction. We say that B is *obstructed* (with respect to $\mathfrak{C}$) if $\mathfrak{C}(B) = \{0\}$ and that $\mathfrak{C}$ is *unobstructed* if no B is obstructed.

Proposition 6.1.2 shows that if $\mathfrak{C}$ is unobstructed, then there is a B isogenous to A and a filtration $0 \subset \mathcal{W}_1 \subset \cdots \subset \mathcal{W}_s = B[\mathfrak{l}^r]$, with $\mathcal{W}_{i+1}/\mathcal{W}_i$ in $\mathfrak{C}(B/\mathcal{W}_i)$ for all i. We choose our mirages so that such a filtration cannot exist and then exploit the special properties that the obstructed members of $\mathfrak{I}_A^\mathfrak{l}$ satisfy. As one illustration, when $\mathbb{Q}(A[\mathfrak{l}])$ is a 2-extension for some $\mathfrak{l} \mid 2$ and all primes dividing N_A are 3 mod 4, we prove in Theorem 6.2.10 that $2 \dim A \le \Omega(N_A)$.

Some of the criteria in §§4–6 depend on arithmetic invariants of extensions of exceptional module schemes $\mathcal{E}$ in $\mathfrak{S}_{\mathfrak{l}}(A)$. These invariants depend on the arithmetic of the number fields generated by the points of such extensions. Those number fields are typically large Galois extensions which, in our applications, are the Galois closures of small cyclic extensions of tractable number fields with well controlled conductors. In §7, we estimate the latter when $\dim_{\mathbb{F}_{\mathfrak{l}}} E = 2$, to the point that Magma can be invoked. Similarly, when $\dim_{\mathbb{F}_2} A[\mathfrak{l}] = 4$, enough information on $\mathbb{Q}(E)$ is obtained that we could rely on the Bordeaux tables [10]. Finally, our data on paramodular varieties are summarized in the appendices.

3. Preliminaries

3.1. **Basics.** Let $\mathbb{F}$ be a finite field of characteristic ℓ, G a finite group and V a finite $\mathbb{F}[G]$-module. The contragredient $\widehat{V} = \operatorname{Hom}_{\mathbb{F}}(V, \mathbb{F})$ is an $\mathbb{F}[G]$-module via the action on V and the trace $\operatorname{Tr}_{\mathbb{F}/\mathbb{F}_\ell}$ induces an isomorphism $\widehat{V} \simeq \operatorname{Hom}_{\mathbb{F}_\ell}(V, \mathbb{F}_\ell)$. Now, let G be a quotient of $G_{\mathbb{Q}} = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by an open subgroup. Write $\mathbb{F}(1) = \mathbb{F} \otimes \omega$ for the Tate twist by the mod-ℓ cyclotomic character ω and let $V^* = \operatorname{Hom}_{\mathbb{F}}(V, \mathbb{F}(1))$. A non-degenerate additive pairing $[\ ,\ ]\colon V \times V \to \mathbb{F}_\ell(1)$ satisfying $[g(x), g(y)] = \omega(g)[x, y]$ for all g in G and $[\alpha x, y] = [x, \alpha y]$ for all α in $\mathbb{F}$ is equivalent to an $\mathbb{F}[G]$-isomorphism $V^* \simeq V$. We say that V is a symplectic Galois module if, in addition, the pairing is alternating. Then $\dim_{\mathbb{F}} V = 2n$ is even and, upon the choice of a symplectic basis, V yields a Galois representation into

$$\mathrm{R}_{2n}(\mathbb{F}) := \{g \in \mathrm{GSp}_{2n}(\mathbb{F}) \mid [gx, gy] = \omega(g)[x, y] \text{ for all } x, y \in V\}.$$

If W is an $\mathfrak{o}[G]$-module, let W^G be the submodule fixed pointwise by G. When V is simple, $\mathbf{m}_V(W)$ is the multiplicity of V in any composition series for W. The annihilator of an $\mathfrak{o}$-module M will be written as $\operatorname{ann}_{\mathfrak{o}} M$.

We use a capital calligraphic letter for a finite flat group scheme and the corresponding capital Roman letter for its Galois module of $\overline{\mathbb{Q}}$-points, e.g. $\mathcal{V}$ and V respectively. We write $\mathbb{Q}(V)$ for the field defined by the points of $V = \mathcal{V}(\overline{\mathbb{Q}})$. The Cartier dual of $\mathcal{V}$ is $\mathcal{V}^D = \operatorname{Hom}(\mathcal{V}, \mathbb{G}_m)$ and its Galois module is V^*.

What we need about abelian schemes and their polarizations over Dedekind domains may be found in the first few pages of [34] and [14]. Under our standing assumption that $A_{/\mathbb{Q}}$ is of $\mathfrak{o}$-type, with good reduction outside S, the group $A[\mathfrak{a}]$ of $\mathfrak{a}$-division points is an $\mathfrak{o}$-module scheme over $\mathbb{Z}_S$ for any ideal $\mathfrak{a}$ of $\mathfrak{o}$ prime to S.

The following result of Raynaud ([11], [41]) allows us to treat group schemes that occur as subquotients of known group schemes via their associated Galois modules. In essence, the generic fiber functor induces an isomorphism between the lattice of finite flat closed R-subgroup schemes of $\mathcal{V}$ and finite flat closed K-subgroup schemes of $\mathcal{V}_{|K}$, where K is the field of fractions of R.

Lemma 3.1.1. *Let R be a Dedekind domain with quotient field K and $\mathcal{V}$ 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 $(\mathcal{V}_2/\mathcal{V}_1)_{|K} \simeq W$.*

If $\mathcal{V}$ is an $\mathfrak{o}$-module scheme, then $\mathfrak{o}$-module scheme subquotients of $\mathcal{V}$ correspond to $\mathfrak{o}[G_{\mathbb{Q}}]$-module subquotients of V by this lemma. While we depend on this lemma, the reader could instead rely on the Mayer-Vietoris sequence of [51, Prop. 2.4].

Consider a strictly increasing filtration of $\mathfrak{o}$-module schemes over $\mathbb{Z}_S$,

$$\mathcal{F} = \{0 = \mathcal{W}_0 \subset \mathcal{W}_1 \subset \cdots \subset \mathcal{W}_s = \mathcal{W}\}, \tag{3.1.2}$$

where $\mathcal{W}$ is $\mathfrak{l}$-primary and the inclusions are closed immersions. We denote the list of successive quotients by $\mathbf{gr}\,\mathcal{F} = [\dots, \mathcal{W}_i/\mathcal{W}_{i-1}, \dots]$, often writing $\mathbf{gr}\,\mathcal{W}$ without explicitly naming the filtration from which it arose. When $\mathcal{F}$ is a composition series, the multiset of module schemes appearing in $\mathbf{gr}\,\mathcal{F}$ may depend on the choice of $\mathcal{F}$. By the Jordan-Hölder theorem, the corresponding multiset of irreducible Galois modules does not.

We say that $\mathcal{W}$ or $\mathcal{F}$ is *prosaic* if all the composition factors are isomorphic to $\mathcal{Z}_{\mathfrak{l}}$ or $\boldsymbol{\mu}_{\mathfrak{l}}$, i.e. their associated Galois modules are one-dimensional over $\mathbb{F}_{\mathfrak{l}}$.

Notation 3.1.3. Let $\mathcal{V}$ be an $\mathfrak{l}$-primary $\mathfrak{o}$-module scheme over $\mathbb{Z}_S$. By standard abuse, we write $\mathcal{V}^{et}$ for the maximal étale quotient of $\mathcal{V}_{|\mathbb{Z}_\ell}$ and $\mathcal{V}^m = ((\mathcal{V}^D)^{et})^D$ for the maximal multiplicative subgroup of $\mathcal{V}_{|\mathbb{Z}_\ell}$. Similarly, $\mathcal{V}^0 = (\mathcal{V}_{|\mathbb{Z}_\ell})^0$ will denote the connected component and $\mathcal{V}^b = \mathcal{V}^0/\mathcal{V}^m$ the biconnected subquotient. Once a place λ over ℓ is chosen, with decomposition group $\mathcal{D}_\lambda$, we use the symbols V^{et}, V^m, V^0 and V^b for the corresponding $\mathcal{D}_\lambda$-module.

We have the important result of Fontaine, as formulated in [29, Thm. 1.4] and stated here for finite flat $\mathfrak{l}$-primary $\mathfrak{o}$-module schemes $\mathcal{V}_1, \mathcal{V}_2$ over $\mathbb{Z}_S$.

Lemma 3.1.4. *If ℓ is odd and $V_1 \simeq V_2$ as Galois modules, then $\mathcal{V}_1 \simeq \mathcal{V}_2$. This holds for $\ell = 2$ if, in addition, $\mathcal{V}_1^{et} = \mathcal{V}_2^{et} = 0$ or $\mathcal{V}_1^m = \mathcal{V}_2^m = 0$.*

We recall some information about Cartier duality of $\mathfrak{o}$-module schemes over $\mathbb{Z}_S$.

Lemma 3.1.5. *Let $\mathcal{W} \subseteq \mathcal{V}$ be finite flat $\mathfrak{o}$-module schemes over $\mathbb{Z}_S$. Any isomorphism $f : \mathcal{V}^D \simeq \mathcal{V}$ induces a pairing on the Galois module V. The submodule scheme of $\mathcal{V}$ corresponding to $W^\perp$ is $\mathcal{W}^\perp = f((\mathcal{V}/\mathcal{W})^D)$ and $\mathcal{W}^D$ is isomorphic to $\mathcal{V}/\mathcal{W}^\perp$. If W is totally isotropic, $\mathcal{W}^\perp/\mathcal{W}$ is isomorphic to its Cartier dual.*

Proof. The dual of the exact sequence $0 \to \mathcal{W} \to \mathcal{V} \to \mathcal{V}/\mathcal{W} \to 0$ is

$$0 \to (\mathcal{V}/\mathcal{W})^D \to \mathcal{V}^D \to \mathcal{W}^D \to 0.$$

Hence the Galois module corresponding to $f((\mathcal{V}/\mathcal{W})^D)$ is $W^\perp$. If $\mathcal{W}_1 \subset \mathcal{W}_2$, then

$$0 \to (\mathcal{V}/\mathcal{W}_2)^D \to (\mathcal{V}/\mathcal{W}_1)^D \to (\mathcal{W}_2/\mathcal{W}_1)^D \to 0.$$

Apply this with $\mathcal{W}_1 = \mathcal{W}$ and $\mathcal{W}_2 = \mathcal{W}^\perp$ to verify the last claim. ∎

Lemma 3.1.6. *Let W be a symplectic $\mathfrak{o}[G_{\mathbb{Q}}]$-module and let V be an irreducible submodule.*

i) *Then V is annihilated by some prime $\mathfrak{l}$ of $\mathfrak{o}$ and one of the following holds:*
   a) *V is non-singular and $W = V \perp V^\perp$, or*
   b) *V is totally isotropic, $V^\perp/V$ is non-singular and $W/V^\perp \simeq V^* = \mathrm{Hom}(V, \boldsymbol{\mu}_\ell)$.*

ii) *If V is cyclic as an $\mathfrak{o}$-module, then V is totally isotropic.*

iii) *If W is semisimple, all irreducible submodules of W are non-singular precisely when W contains no non-zero totally isotropic submodule.*

Proof. Since V is irreducible, $V \cap V^{\perp} = 0$ or V and (i) easily follows. If V is cyclic as an $\mathfrak{o}$-module, it is one-dimensional over $\mathbb{F}_{\mathfrak{l}} = \mathfrak{o}/\mathfrak{l}$. For any a, b in $\mathbb{F}_{\mathfrak{l}}$, we can solve $c^2 + d^2 = ab$ in $\mathbb{F}_{\mathfrak{l}}$. Then the alternating pairing on W satisfies $\langle ax, bx \rangle = \langle cx, cx \rangle + \langle dx, dx \rangle = 0$, proving (ii). Suppose that W is semisimple. If W has no totally isotropic submodule, then every irreducible submodule is non-singular by (i). The converse in (iii) is clear. □

Lemma 3.1.7. *Let $\mathcal{W}$ be a self-dual $\mathbb{F}$-module scheme over $\mathbb{Z}_S$ whose $\mathbb{F}[G_{\mathbb{Q}}]$-module W is symplectic and has a unique simple constituent E such that* $\dim E \geq 2$. *Then there is a self-dual subquotient $\mathcal{E}$ of $\mathcal{W}$ with Galois module E.*

Proof. Use induction on the size of W. Let $\mathcal{X}$ be a simple submodule scheme of $\mathcal{W}$. If $\mathcal{X}$ is one-dimensional, then X is isotropic, and by induction applied to $\mathcal{V} = \mathcal{X}^{\perp}/\mathcal{X}$, we may suppose there is *no* one-dimensional Galois submodule in W. Thus $X \simeq E$. If X is isotropic, then $\mathcal{X}^D \simeq \mathcal{W}/\mathcal{X}^{\perp}$, a contradiction. If X is non-singular, then $X^{\perp}$ has no one-dimensional Galois submodule and so $W = X$, and we are done. □

Warning: The subgroup scheme corresponding to a self-dual Galois submodule W is not necessarily isomorphic to its Cartier dual.

3.2. **Tate module and conductor.** Let A be semistable of $\mathfrak{o}$-type and dimension g. Fix a prime λ in $\overline{\mathbb{Q}}$ over the prime ℓ of good reduction. Let $\ell\mathfrak{o} = \prod_{\mathfrak{l}} \mathfrak{l}^{e_{\mathfrak{l}}}$ and $f_{\mathfrak{l}} = [\mathbb{F}_{\mathfrak{l}} : \mathbb{F}_{\ell}]$. Then $\mathfrak{o}_{\ell} := \mathfrak{o} \otimes \mathbb{Z}_{\ell} = \prod_{\mathfrak{l}} \mathfrak{o}_{\mathfrak{l}}$. Let $\mathbb{T}_{\ell}(A)$ be the Tate module and $\mathbb{T}_{\mathfrak{l}}(A) = \varprojlim A[\mathfrak{l}^n]$. The actions of $\mathfrak{o}_{\ell}$ and Galois commute.

Lemma 3.2.1. *We have* $\operatorname{rank}_{\mathfrak{o}_{\mathfrak{l}}} \mathbb{T}_{\mathfrak{l}}(A) = 2g/d$. *For fixed λ, $\mathbb{T}_{\mathfrak{l}}(A)^m$ and $\mathbb{T}_{\mathfrak{l}}(A)^{et}$ are pure free $\mathfrak{o}_{\mathfrak{l}}$-submodules of the same rank, which may vary with $\mathfrak{l}$.*

Proof. We know from [44] that $\mathbb{T}_{\ell}(A) = \prod_{\mathfrak{l}} \mathbb{T}_{\mathfrak{l}}(A)$ is a free $\mathfrak{o}_{\ell}$-module of rank $2g/d$. From the canonical isomorphism to the Tate module of the reduction, $\mathbb{T}_{\mathfrak{l}}(A)^{et}$ is a free $\mathfrak{o}_{\mathfrak{l}}$-module. As a free quotient, $\mathbb{T}_{\mathfrak{l}}(A)^{et}$ is a direct summand, and so is pure. By Cartier duality, $\mathbb{T}_{\mathfrak{l}}(\widehat{A})^m$ is free of the same rank. Corresponding to any $\mathfrak{o}$-polarization, there is an isogeny $A \to \widehat{A}$ preserving the multiplicative component and so $\mathbb{T}_{\mathfrak{l}}(A)^m$ and $\mathbb{T}_{\mathfrak{l}}(\widehat{A})^m$ also have the same rank. To show that $\mathbb{T}_{\mathfrak{l}}(A)^m$ is pure, one may use the fact that it is the submodule of $\mathbb{T}_{\mathfrak{l}}(A)$ orthogonal to $\mathbb{T}_{\mathfrak{l}}(\widehat{A})^0$. □

Since $\mathfrak{o}$ acts by functoriality on the connected component of the special fiber of the Néron model of A, the dimensions of $\mathcal{T}_p$ and $\mathcal{B}_p$ in (1.5) are multiples of d.

Notation 3.2.2. Write $t_p = \dim \mathcal{T}_p$ for the toroidal dimension at p and $\tau_p = t_p/d$. By semistability, the reduced conductor of A is $N_A^0 = \prod_p p^{\tau_p}$.

We review some results of Grothendieck (cf. [20], [6]). Since $L_{\infty} = \mathbb{Q}(A[\ell^{\infty}])$ depends only on the isogeny class of A, the dual variety $\widehat{A}$ has the same ℓ^{∞}-division field. Let v be a place over p and $\mathcal{D}_v$ its decomposition group inside $\operatorname{Gal}(L_{\infty}/\mathbb{Q})$. The inertia group $\mathcal{I} = \mathcal{I}_v \subseteq \mathcal{D}_v$ acts on $A[\ell^{\infty}]$ and $A[\mathfrak{l}^{\infty}]$ through its maximal tame quotient, a pro-ℓ cyclic group $\langle \sigma_v \rangle$ whose generator satisfies $(\sigma_v - 1)^2 = 0$. The fixed space $M_f(A, v, \ell) = \mathbb{T}_{\ell}(A)^{\mathcal{I}}$ is a pure $\mathfrak{o}_{\ell}$-submodule of $\mathbb{T}_{\ell}(A)$. The toric space $M_t(A, v, \ell)$ is the $\mathfrak{o}_{\ell}$-submodule of $\mathbb{T}_{\ell}(A)$ orthogonal to $M_f(\widehat{A}, v, \ell)$ under the natural pairing of $\mathbb{T}_{\ell}(A)$ with $\mathbb{T}_{\ell}(\widehat{A})$. Moreover, $(\sigma_v - 1)\mathbb{T}_{\ell}(A)$ has finite index in $M_t(A, v, \ell)$. Define $M_f(A, v, \mathfrak{l})$ and $M_t(A, v, \mathfrak{l})$ either analogously or by tensoring with $\mathfrak{o}_{\mathfrak{l}}$. Our earlier remarks together with the $\mathfrak{o}_\ell[\mathcal{D}_v]$-isomorphisms $M_t(A,v,\ell) \simeq \mathbb{T}_\ell(\mathcal{T}_p)$ and $M_f(A,v,\ell)/M_t(A,v,\ell) \simeq \mathbb{T}_\ell(\mathcal{B}_p)$ imply that

$$\operatorname{rank}_{\mathfrak{o}_\mathfrak{l}} M_t(A,v,\mathfrak{l}) = \operatorname{rank}_{\mathfrak{o}_\mathfrak{l}}(\sigma_v - 1)\mathbb{T}_\mathfrak{l}(A) = \frac{t_p}{d} = \tau_p. \tag{3.2.3}$$

The restriction of σ_v to $\mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q})$ generates a subgroup of order 1 or ℓ.

Remark 3.2.4. The image $\overline{M}_t$ of $M_t(A,v,\mathfrak{l})$ in $A[\mathfrak{l}]$ is an $\mathbb{F}_\mathfrak{l}[\mathcal{D}_v]$-submodule such that $\dim_{\mathbb{F}_\mathfrak{l}} \overline{M}_t = \tau_p$, even if σ_v acts trivially on $A[\mathfrak{l}]$. Hence, τ_p is bounded from below by the least dimension of any simple $\mathbb{F}_\mathfrak{l}[\mathcal{D}_v]$-constituent of $A[\mathfrak{l}]$.

Write $\mathfrak{f}_p(V)$ for the Artin conductor exponent at p of the finite $\mathfrak{o}_\mathfrak{l}[G_\mathbb{Q}]$-module V and N_V for its global Artin conductor. If $\mathcal{I}$ acts tamely, $\mathfrak{f}_p(V) = \operatorname{length}_{\mathfrak{o}_\mathfrak{l}} V/V^{\mathcal{I}}$. Denote by Frob_v a choice of arithmetic Frobenius.

Lemma 3.2.5. *Let $0 \to V_1 \to V \xrightarrow{\pi} V_2 \to 0$ be an exact sequence of finite $\mathfrak{o}_\mathfrak{l}[\mathcal{D}_v]$-modules, with v a prime above $p \neq \ell$. Suppose $\mathcal{I}_v$ acts on V via a pro-ℓ cyclic group $\langle\sigma\rangle$ and $(\sigma-1)^2(V) = 0$. Let $M_i = (\sigma-1)(V_i)$ and $\widetilde{V}_i = V_i^{\langle\sigma\rangle}/M_i$. Then*

i) *there is a well-defined $\mathfrak{o}_\mathfrak{l}[\Phi]$-map $\overline{\delta}\colon \widetilde{V}_2 \to \widetilde{V}_1(-1)$, where $\Phi = \mathrm{Frob}_v$, and*
ii) *$\mathfrak{f}_p(V) = \mathfrak{f}_p(V_1) + \mathfrak{f}_p(V_2) + \operatorname{length}_{\mathfrak{o}_\mathfrak{l}} \mathrm{Im}(\overline{\delta})$.*

Proof. By the snake lemma, we have the exact sequence of Φ-modules

$$0 \to V_1^{\langle\sigma\rangle} \to V^{\langle\sigma\rangle} \to V_2^{\langle\sigma\rangle} \xrightarrow{\delta} V_1/M_1, \tag{3.2.6}$$

where δ is induced by $y \rightsquigarrow (\sigma-1)(x)$, with $y = \pi(x)$. Since $(\sigma-1)^2(V) = 0$, we see that $\delta(M_2) \equiv 0 \pmod{M_1}$ and we obtain the $\mathfrak{o}_\mathfrak{l}$-map $\overline{\delta}$. Then (ii) follows.

To see that $\overline{\delta}$ is a Φ-map, note that Φ raises to the p^{th} power on $\mathcal{I}_v$ and that $\sigma^{p-1} + \cdots + 1$ is multiplication by p on $(\sigma-1)(V)$ to obtain $\Phi\overline{\delta} = p\,\overline{\delta}\Phi$. □

Lemma 3.2.7. *Let $\mathcal{I}_v$ act on the $\mathbb{F}_\mathfrak{l}[\mathcal{D}_v]$-module V via $\langle\sigma\rangle$ with $(\sigma-1)^2(V) = 0$. Then $\mathfrak{f}_p(V^*) = \mathfrak{f}_p(V)$. If $\dim_{\mathbb{F}_\mathfrak{l}} V \leq 3$ and V is ramified at v, then $\mathfrak{f}_p(V) = 1$.*

Proof. In the natural pairing $\widehat{V} \times V \to \mathbb{F}_\mathfrak{l}$, we have $\widehat{V}^{\langle\sigma\rangle} = ((\sigma-1)V)^\perp$, since σ is trivial on μ_ℓ. Hence $\mathfrak{f}_p(V) = \dim V/V^{\langle\sigma\rangle} = \dim(\sigma-1)V = \dim \widehat{V}/\widehat{V}^{\langle\sigma\rangle} = \mathfrak{f}_p(\widehat{V})$. The last claim follows from $(\sigma-1)V \subseteq V^\sigma$. □

The inclusion $M_f(A,v,\mathfrak{l})/\mathfrak{l}^r M_f(A,v,\mathfrak{l}) \hookrightarrow A[\mathfrak{l}^r]^{\mathcal{I}}$ implies that

$$\begin{aligned} \mathfrak{f}_p(A[\mathfrak{l}^r]) &= \operatorname{length}_{\mathfrak{o}_\mathfrak{l}}(A[\mathfrak{l}^r]/A[\mathfrak{l}^r]^{\mathcal{I}}) \\ &\leq r \operatorname{length}_{\mathfrak{o}_\mathfrak{l}} A[\mathfrak{l}] - r \operatorname{rank}_{\mathfrak{o}_\mathfrak{l}} M_f(A,v,\mathfrak{l}) \\ &\leq r\frac{2g}{d} - r\left(\frac{2g}{d} - \frac{t_p}{d}\right) = r\frac{t_p}{d} = r\tau_p. \end{aligned} \tag{3.2.8}$$

Lemma 3.2.9. *Let A be a $\mathbb{Q}$-simple abelian variety, not necessarily semistable, with $\mathfrak{o} \subseteq \mathrm{End}_\mathbb{Q} A$. Then the conductor $N_A = N^d$ for some integer N.*

i) *If N is squarefree, then A is semistable and the quotient field of $\mathfrak{o}$ is a maximal commutative subfield of $\mathrm{End}^0_\mathbb{Q} A = \mathrm{End}_\mathbb{Q} A \otimes \mathbb{Q}$.*
ii) *If A is semistable and $g = \dim A$ is prime, then either $\mathrm{End}\, A = \mathbb{Z}$ or A is classically modular.*

Proof. Since A is $\mathbb{Q}$-simple, $D = \mathrm{End}^0_{\mathbb{Q}} A$ is a division algebra with center a CM field K. Let $\dim_K D = m^2$ and $[K:\mathbb{Q}] = r$, so that a maximal commutative subfield of D has degree mr over $\mathbb{Q}$. The conductor formula, applied to the ℓ-adic representation as in [57], with ℓ sufficiently large, shows that the exponents in the conductor must be multiples of mr and of d. Because $\mathfrak{o}$ is a maximal order, were $\mathrm{End}_{\mathbb{Q}} A$ to contain $\mathfrak{o}$ properly, the conductor exponent would be a multiple of d. Similarly, if A is not semistable at p, the conductor exponent of A at p is at least $2d$ by [20, §4]. This proves (i).

For (ii), semistability implies $\mathrm{End}^0 A = \mathrm{End}^0_{\mathbb{Q}} A$ by [43]. Since the invariant differentials form a D-module, g is a multiple of rm^2, so $D = K$. If K is not $\mathbb{Q}$, then $[K:\mathbb{Q}] = g$. When g is odd, K is totally real and A has RM. The same holds when $g = 2$ because Shimura [58] showed that for a surface, $\mathrm{End}\, A$ cannot be an order in a *complex* quadratic number field. Finally, A is a simple factor of $J_0(N)^{new}$, with $N_A = N^g$, by [27]. □

Proposition 3.2.10. *If A and B are $\mathfrak{o}$-isogenous $\mathfrak{o}$-type abelian varieties and $\mathfrak{l}$ is a prime ideal of $\mathfrak{o}$, then $\mathfrak{S}^{all}_{\mathfrak{l}}(B) = \mathfrak{S}^{all}_{\mathfrak{l}}(A)$.*

Proof. By the Jordan-Holder theorem, $\mathfrak{S}^{all}_{\mathfrak{l}}(A)$ does not depend on the choice of composition series for $A[\mathfrak{l}]$. We use induction on the order of the kernel U of the $\mathfrak{o}$-isogeny $f : A \to B$. If $U[\mathfrak{l}]$ is trivial, f induces an isomorphism of $A[\mathfrak{l}]$ to $B[\mathfrak{l}]$. If not, let α be an element of $\mathfrak{o}$ with $\mathrm{ord}_{\mathfrak{l}}(\alpha) = 1$ and consider a composition series

$$0 \subset V_1 \subset \cdots \subset V_r \subset \cdots \subset V_n = A[\ell] \subset V_{n+1} \cdots \subset V_{n+r} \subset \cdots \subset V_{2n} = A[\ell^2],$$

chosen so that $V_r = U[\mathfrak{l}]$ and $\alpha V_{n+i} = V_i$ for $i \le n$. Visibly, for $C = A/V_r$, we have $\mathfrak{S}^{all}_{\mathfrak{l}}(A) = \mathfrak{S}^{all}_{\mathfrak{l}}(C)$. Moreover, $\mathfrak{S}^{all}_{\mathfrak{l}}(C) = \mathfrak{S}^{all}_{\mathfrak{l}}(B)$ by induction hypothesis, since the kernel of the induced isogeny $C \to B$ is U/V_r. Hence $\mathfrak{S}^{all}_{\mathfrak{l}}(B) = \mathfrak{S}^{all}_{\mathfrak{l}}(A)$. □

3.3. **Ramification.** We recall Serre's convention [55, Ch. IV] for the ramification numbering. Let L/K be a Galois extension of ℓ-adic fields with Galois group G. Denote the ring of integers of L by $\mathcal{O}_L$ and a prime element by λ_L. Set

$$G_n = \{\sigma \in G \mid \mathrm{ord}_{\lambda_L}(\sigma(x) - x) \ge n + 1 \text{ for all } x \in \mathcal{O}_L\},$$

so that G_0 is the inertia group and $[G_0 : G_1]$ is the degree of tame ramification. Recall the Herbrand function: if $m \le u \le m + 1$, then

$$\varphi_{L/K}(u) = \frac{1}{|G_0|}(\,|G_1| + \cdots + |G_m| + (u - m)|G_{m+1}|\,). \tag{3.3.1}$$

We restate the famous result of Abrashkin [1] and Fontaine [15] on ramification groups, but use the upper numbering of Serre, namely $G^m = G_n$, with $m = \varphi_{L/K}(n)$. Fontaine's numbering is larger by 1.

Lemma 3.3.2. *Let $\mathcal{V}$ be a finite flat group scheme of exponent ℓ over $\mathbb{Z}_\ell$, $L = \mathbb{Q}_\ell(V)$ and $G = \mathrm{Gal}(L/\mathbb{Q}_\ell)$. If $\alpha > 1/(\ell - 1)$, then G^α acts trivially on V. Moreover, the root discriminant r_L of $L/\mathbb{Q}_\ell$ satisfies*

$$r_L := |d_{L/\mathbb{Q}_\ell}|^{\frac{1}{[L:\mathbb{Q}_\ell]}} < \ell^{1+\frac{1}{\ell-1}}.$$

We now return to the global situation, with $\mathcal{V}$ an $\mathfrak{o}$-module scheme over $\mathbb{Z}_S$ and λ a place of $\overline{\mathbb{Q}}$ over $\ell \notin S$. The set T_V of *bad primes* of V consists exactly of those dividing N_V, namely the finite primes $p \neq \ell$ that ramify in $\mathbb{Q}(V)$.

Definition 3.3.3. Fix a finite set S of primes and $\mathfrak{l}$ a prime of $\mathfrak{o}$ over ℓ not in S. An $\mathfrak{l}$-primary $\mathfrak{o}$-module scheme over $\mathbb{Z}_S$ is *acceptable* if it is a subquotient of $A[\mathfrak{l}^n]$ for some semiabelian scheme A over $\mathbb{Z}$ with good reduction outside S and an action $\iota : \mathfrak{o} \hookrightarrow \mathrm{End}_{\mathbb{Q}} A$.

Definition 3.3.4. An $\mathbb{F}_{\mathfrak{l}}[G_{\mathbb{Q}}]$-module V is *semistable* if $L = \mathbb{Q}(V)$ satisfies

i) the inertia group $\mathcal{I}_\lambda(L/\mathbb{Q})^\alpha = 1$ for each λ over ℓ and all $\alpha > 1/(\ell-1)$, and
ii) $\mathcal{I}_v(L/\mathbb{Q}) = \langle \sigma_v \rangle$, with $(\sigma_v - 1)^2(V) = 0$ for each place v dividing N_V.

The Galois module of an acceptable $\mathbb{F}_{\mathfrak{l}}$-module scheme is semistable.

Remark 3.3.5.

i) Acceptable $\mathfrak{l}$-primary $\mathfrak{o}$-module schemes form a full subcategory $\underline{A}$ of the category $\underline{D}$ of Schoof, as generalized in §2 above. The definition of the Baer sum shows that $\mathrm{Ext}^1_{\underline{A}}(\mathcal{U}_1, \mathcal{U}_2)$ is a subgroup of $\mathrm{Ext}^1_{\underline{D}}(\mathcal{U}_1, \mathcal{U}_2)$ when $\mathcal{U}_i$ are acceptable.

ii) Our notion makes Lemma 3.1.1 available. It seems difficult to check when an object in $\underline{D}$ is acceptable. In our applications, the extensions considered are subquotients of $A[\mathfrak{l}^n]$ for a fixed abelian variety and so are themselves acceptable.

Remark 3.3.6. Let $\mathcal{V}$ be an acceptable $\mathbb{F}_{\mathfrak{l}}$-module scheme with $\dim V = 1$. The ramification degree of primes over S in $\mathbb{Q}(V)/\mathbb{Q}$ divides ℓ, but $\mathrm{Gal}(\mathbb{Q}(V)/\mathbb{Q})$ is a subgroup of $\mathbb{F}_{\mathfrak{l}}^\times$, so abelian of order prime to ℓ. Thus $\mathbb{Q}(V) \subseteq \mathbb{Q}(\boldsymbol{\mu}_\ell)$ and we conclude that $\mathcal{V}$ is isomorphic to $\mathcal{Z}_{\mathfrak{l}}$ or its Cartier dual $\boldsymbol{\mu}_{\mathfrak{l}}$ by [29, Prop. 1.5].

Notation 3.3.7. Write $\mathrm{rad}(m)$ for the product of the distinct prime factors of m.

Proposition 3.3.8. *Let $\mathcal{W}$ be an acceptable $\mathfrak{l}$-primary $\mathfrak{o}$-module scheme with $\mathfrak{l} \mid 2$. If* $\mathrm{rad}(N_W)$ *divides one of the integers in* $\mathfrak{T}_0 = \{13, 15, 17, 21, 39, 41, 65\}$, *then $\mathcal{W}$ is prosaic.* (GRH is assumed for $\mathrm{rad}(N_W) \geq 39$.)

Proof. Let F be the field generated by i and the square roots of the primes dividing N_W. Any simple constituent V of W is a semistable $\mathbb{F}_{\mathfrak{l}}[G_{\mathbb{Q}}]$-module. Use the refined Odlyzko bounds in [8, Table 2] to conclude that $F(V)/F$ is an abelian extension whose conductor is bounded by [8, Lemma 5.8]. Magma ray class group computations show that $\mathrm{Gal}(\mathbb{Q}(V)/\mathbb{Q})$ is a 2-group and thus $\dim_{\mathbb{F}_{\mathfrak{l}}} V = 1$. By Remark 3.3.6, $\mathcal{V} \simeq \mathcal{Z}_{\mathfrak{l}}$ or $\boldsymbol{\mu}_{\mathfrak{l}}$, so $\mathcal{W}$ is filtered by $\mathcal{Z}_{\mathfrak{l}}$'s and $\boldsymbol{\mu}_{\mathfrak{l}}$'s, as claimed. □

Definition 3.3.9. An irreducible semistable $\mathbb{F}_{\mathfrak{l}}[G_{\mathbb{Q}}]$-module E is *exceptional* if $\dim_{\mathbb{F}_{\mathfrak{l}}} E \geq 2$. The $\mathbb{F}_{\mathfrak{l}}$-module scheme $\mathcal{E}$ is *exceptional* if its generic fiber is. When considering a specific exceptional $\mathcal{E}$, we write $F = \mathbb{Q}(E)$, $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ and T_E for the exact set of primes dividing the conductor N_E of E.

By convention, $\mathcal{Z}$ and $\mathcal{M}$ are acceptable $\mathfrak{o}$-module schemes over $\mathbb{Z}_S$, filtered by $\mathcal{Z}_{\mathfrak{l}}$'s and $\boldsymbol{\mu}_{\mathfrak{l}}$'s respectively, with ℓ not in S. Clearly then $\mathbb{Q}(Z)/\mathbb{Q}$ and $\mathbb{Q}(M)/\mathbb{Q}(\boldsymbol{\mu}_\ell)$ are ℓ-extensions unramified outside S.

Lemma 3.3.10. *Let $0 \to \mathcal{Z} \to \mathcal{V} \to \mathcal{X} \to 0$ be an exact sequence of $\mathfrak{o}$-module schemes over $\mathbb{Z}_S$, T the set of bad primes of X and $L = \mathbb{Q}(V)$. Then:*

i) *$L/\mathbb{Q}(X)$ is unramified at places λ over ℓ;*
ii) *λ splits in $L/\mathbb{Q}(Z, X)$ if $\mathcal{X}$ is connected over $\mathbb{Z}_\ell$;*
iii) *$L/\mathbb{Q}(X)$ is unramified outside $(S - T) \cup \{\infty\}$ if $\mathfrak{l}\mathcal{V} = 0$;*
iv) *$L/\mathbb{Q}(\boldsymbol{\mu}_\ell)$ is an ℓ-extension if $\mathcal{X} = \mathcal{M}$;*

v) $\mathbb{Q}(Z) = \mathbb{Q}$ *and* $\mathcal{Z}$ *is constant if* $N_Z = 1$ *and in particular if* $N_V = N_X$*;*
vi) *if* $0 \to \mathcal{V} \to \mathcal{W} \to \mathcal{M} \to 0$ *is exact and* $N_V = N_W$*, then* $\mathcal{M}^D$ *is constant.*

Proof. Any σ in $\mathcal{I}_\lambda(L/\mathbb{Q}(X))$ acts trivially on X and trivially on $V^{et} = V/V^0$, so $(\sigma - 1)(V) \subseteq Z$ and $(\sigma - 1)(V) \subseteq V^0$. Since $\mathcal{Z}$ is étale at λ and $\mathcal{V}^0$ is connected, we have $(\sigma - 1)(V) \subseteq Z \cap V^0 = \{0\}$. This proves (i).

In (ii), the exact sequence defining $\mathcal{V}$ splits over $\mathbb{Z}_\ell$, since $\mathcal{V}^0 \simeq \mathcal{X}$, and so the primes over ℓ split in $L/\mathbb{Q}(X, Z)$. In (iii), the ramification degree of each p in S divides ℓ. Hence $\mathbb{Q}(X)$ already accounts for all the ramification over each p in T. In (iv), $\mathrm{Gal}(L/\mathbb{Q}(\boldsymbol{\mu}_\ell))$ is an extension of ℓ-groups and therefore is an ℓ-group.

In (v), $\mathcal{Z}$ is étale locally at ℓ and $N_Z = 1$, so $\mathbb{Q}(Z)$ is unramified everywhere. Thus, $\mathbb{Q}(Z) = \mathbb{Q}$ and $\mathcal{Z}$ prolongs to a constant $\mathbb{F}_\mathfrak{l}$-module scheme over $\mathbb{Z}$, as in [29, Prop. 1.5, Prop. 3.1]. If $N_V = N_X$, then $N_Z = 1$ by Lemma 3.2.5.

By Cartier duality, (vi) holds. □

Lemma 3.3.11. *Let* V *be a semistable* $\mathbb{F}_\mathfrak{l}[G_\mathbb{Q}]$*-module, with* $\mathfrak{l} \,|\, 2$*,* $L = \mathbb{Q}(V)$ *and* $G = \mathrm{Gal}(L/\mathbb{Q})$*. For* each *bad prime* p *of* V*, pick* one *place* v *and a generator* σ_v *of* $\mathcal{I}_v(L/\mathbb{Q})$*. Let* U *consist of these involutions and* σ_∞ *a complex conjugation. In general,* G *is generated by the conjugates of* U *and simply by* U *when* G *is a* 2*-group.*

Proof. By semistability, σ_v is an involution. Since the fixed field of the conjugates of U is $\mathbb{Q}$, they generate G. If G is a 2-group and U does not generate G, then U lies in a subgroup of index 2 whose fixed field is $\mathbb{Q}(\sqrt{2})$, violating Lemma 3.3.2. □

Remark 3.3.12. The Artin symbol $(-1, \mathbb{Q}_2^{ab}/\mathbb{Q}_2)$ is trivial on $\mathbb{Q}_2^{nr}$ and inverts 2-power roots of unity. Let W be a Galois submodule of $\mathbb{T}_\mathfrak{l}(A)$ or of $A[\mathfrak{l}^r]$, with $\mathfrak{l}|2$. Fix a place λ over 2 in $L = \mathbb{Q}(W)$ and let L_0 be the maximal abelian subfield of the completion L_λ. Let σ_λ in $\mathcal{D}_\lambda(L/\mathbb{Q})$ extend $(-1, L_0/\mathbb{Q}_2)$ to L_λ. Then σ_λ acts by inversion on W^m and trivially on W^{et}. If $W^b = 0$, then $W^{et} \simeq W/W^m$ and $\sigma_\lambda^2 = 1$ in $\mathcal{D}_\lambda(L/\mathbb{Q})$. In the previous lemma, σ_∞ may be replaced by σ_λ. The next lemma shows how σ_λ detects ramification in $W[\mathfrak{l}]$.

Lemma 3.3.13. *Let* $\tilde{L}_0$ *be the maximal abelian subfield of a* 2*-extension* $\tilde{L}/\mathbb{Q}_2$ *with* $\mathrm{Gal}(\tilde{L}/\mathbb{Q}_2)^\alpha = 1$ *for all* $\alpha > 1$*. The Artin symbol* $a = (-1, \tilde{L}_0/\mathbb{Q}_2)$ *is trivial if and only if* $\tilde{L}$ *is unramified.*

Proof. By restriction, $\mathrm{Gal}(\tilde{L}_0/\mathbb{Q}_2)^\alpha = 1$ for $\alpha > 1$, so $U^{(2)} = 1 + 4\mathbb{Z}_2$ is contained in $N_{\tilde{L}_0/\mathbb{Q}_2}(\tilde{L}_0^\times)$ by [55, XV,§2,Cor. 1]. We have $a = 1$ if and only if $-1 \in N_{\tilde{L}_0/\mathbb{Q}_2}(\tilde{L}_0^\times)$. If so, all units of $\mathbb{Q}_2$ are norms and $\tilde{L}_0/\mathbb{Q}_2$ is unramified. Then $\tilde{L}_0/\mathbb{Q}_2$ is cyclic, so $\tilde{L} = \tilde{L}_0$ by Burnside's theorem. The converse is proved similarly. □

3.4. **Polarizations.** Here we extend some results on polarizations from [30], [68] and [21]. We say that (A, φ) is $\mathfrak{o}$-polarized if $\mathrm{End}\, A = \mathfrak{o}$ and the polarization on A induces an $\mathfrak{o}$-linear isogeny $\varphi : A \to \widehat{A}$. Thus $\boldsymbol{\kappa} = \ker \varphi$ is a Cartier self-dual group scheme whose points form an $\mathfrak{o}[G_\mathbb{Q}]$-module. Throughout this section, $\mathfrak{n}$ is an $\mathfrak{o}$-ideal annihilating $\boldsymbol{\kappa}$. If the positive integer n is contained in $\mathfrak{n}$, we have the Weil pairing $\bar{e}_\mathfrak{n} : A[\mathfrak{n}] \times \widehat{A}[\mathfrak{n}] \to \boldsymbol{\mu}_n$ with $\bar{e}_\mathfrak{n}(\theta a, a') = \bar{e}_\mathfrak{n}(a, \theta a')$ for all θ in $\mathfrak{o}$. Define $\bar{e}_\mathfrak{n}^\varphi(a, a') = \bar{e}_\mathfrak{n}(a, \varphi(a'))$ to obtain an alternating pairing $A[\mathfrak{n}] \times A[\mathfrak{n}] \to \boldsymbol{\mu}_n$ which induces a perfect alternate pairing induced on $A[\mathfrak{n}]/\boldsymbol{\kappa}$. We also have a perfect alternating pairing $\bar{e}^\varphi : \boldsymbol{\kappa} \times \boldsymbol{\kappa} \to \boldsymbol{\mu}_n$ such that

$$\bar{e}^\varphi(a, a') = \bar{e}_\mathfrak{n}(a, \varphi(\alpha')) \quad \text{whenever} \quad a' = n\alpha', \tag{3.4.1}$$

independent of the choices (cf. [30, p. 135]). The order of $\boldsymbol{\kappa}$ is the degree of the polarization and the square of its Pfaffian.

Definition 3.4.2. An $\mathfrak{o}$-isogeny $f : A \to B$ acts on the $\mathfrak{o}$-polarization ϕ of B by $f^*\phi = \hat{f}\phi f$. Write $(A, \varphi) \succ (B, \phi)$ if $\varphi = f^*\phi$ and f is not an isomorphism. Say (A, φ) is *minimally* $\mathfrak{o}$*-polarized* if it is minimal with respect to this ordering.

The next lemma is essentially a restatement of [30, Prop. 16.8].

Lemma 3.4.3. *Suppose that* Λ *is a proper, totally isotropic* $\mathfrak{o}[G_{\mathbb{Q}}]$*-submodule of* $\boldsymbol{\kappa}$ *and let* $f : A \to B = A/\Lambda$ *be the canonical map. Then there is an* $\mathfrak{o}$*-polarization* ϕ*, such that* $(A, \varphi) \succ (B, \phi)$*. Moreover,* $\ker \phi = f(\Lambda^\perp) \simeq \Lambda^\perp/\Lambda$*, where* $\Lambda^\perp$ *is the orthogonal complement of* Λ *with respect to* $\bar{e}^\varphi$*, and* $|\ker \phi| = |\boldsymbol{\kappa}|/|\Lambda|^2$*.*

Proposition 3.4.4. *Let* (A, φ) *be minimally* $\mathfrak{o}$*-polarized. Then* $\boldsymbol{\kappa} = \ker \varphi$ *is an orthogonal direct sum of simple* $\mathfrak{o}[G_{\mathbb{Q}}]$*-modules, symplectic for* $\bar{e}^\varphi$*, on which* $G_{\mathbb{Q}}$ *acts non-trivially. Further, the annihilator ideal* $\mathfrak{a} = \mathrm{ann}_{\mathfrak{o}}(\boldsymbol{\kappa})$ *is squarefree.*

Proof. By Lemma 3.4.3, $\boldsymbol{\kappa}$ contains no $\mathfrak{o}[G_{\mathbb{Q}}]$-submodule totally isotropic for the $\bar{e}^\varphi$ pairing. Then Lemma 3.1.6 implies that each irreducible submodule V of $\boldsymbol{\kappa}$ is symplectic, with non-trivial Galois action. Use $\boldsymbol{\kappa} = V \perp V^\perp$ to continue by induction. Since $\boldsymbol{\kappa}$ is semisimple, its $\mathfrak{o}$-annihilator is squarefree. ☐

Corollary 3.4.5.

i) *For each* V *in* $\mathfrak{S}_{\mathfrak{l}}^{all}(A)$*, we have* $\mathbf{m}_V(A[\mathfrak{l}]) = \mathbf{m}_{V^*}(A[\mathfrak{l}])$*.*
ii) *Let* $\mathfrak{S}_{\mathfrak{l}}(A) = \{E\}$ *with* E *remaining irreducible as a* $\mathcal{D}_\lambda$*-module. Then some subquotient* $\mathcal{E}$ *of* $A[\mathfrak{l}^\infty]$ *is Cartier self-dual and biconnected.*

Proof. (i) Thanks to Proposition 3.2.10, we may assume that (A, φ) is minimally $\mathfrak{o}$-polarized. If $\mathfrak{a} = \mathrm{ann}_{\mathfrak{o}}(\ker \varphi)$ is prime to $\mathfrak{l}$, then $A[\mathfrak{l}]$ is its own Cartier dual. If not, $\mathfrak{l}$ exactly divides $\mathfrak{a}$ by Proposition 3.4.4 and then $\boldsymbol{\kappa}[\mathfrak{l}]$ and $A[\mathfrak{l}]/\boldsymbol{\kappa}[\mathfrak{l}]$ are isomorphic to their own Cartier duals. Since each constituent V of a symplectic module W satisfies $\mathbf{m}_V(W) = \mathbf{m}_{V^*}(W)$, we have $\mathbf{m}_V(A[\mathfrak{l}]) = \mathbf{m}_{V^*}(A[\mathfrak{l}])$.

(ii) Let B be minimally $\mathfrak{o}$-polarized in the isogeny class of A. Then $B[\mathfrak{l}]$ is Cartier self-dual or we have an exact sequence $0 \to \boldsymbol{\kappa} \to B[\mathfrak{l}] \to \boldsymbol{\kappa}' \to 0$ with $\boldsymbol{\kappa}$ and $\boldsymbol{\kappa}'$ both self-dual. Lemma 3.1.7 yields a self-dual subquotient $\mathcal{E}$ of $A[\mathfrak{l}]$. The filtration of $\mathcal{E}_{|\mathbb{Z}_\ell}$ by multiplicative, biconnected and étale subquotients proves our claim. ☐

Remark 3.4.6. The field obtained by adjoining all irreducible $\mathfrak{o}[G_{\mathbb{Q}}]$-constituents of $A[\mathfrak{l}]$ is an isogeny invariant. Taking (A, φ) to be minimally $\mathfrak{o}$-polarized as above, either $A[\mathfrak{l}]$ or $(\ker \varphi)[\mathfrak{l}]$ is Cartier self-dual, and so $\boldsymbol{\mu}_\ell \subseteq \mathbb{Q}(A[\mathfrak{l}])$.

Lemma 3.4.7. *Let* (A, φ) *be minimally* $\mathfrak{o}$*-polarized,* $\boldsymbol{\kappa} = \ker \varphi$ *and* $\mathfrak{a} = \mathrm{ann}_{\mathfrak{o}}(\boldsymbol{\kappa})$*. Let* θ *be a totally positive element of* $\mathfrak{o}$ *dividing* $\mathfrak{a}$ *and write* $\mathfrak{a} = \theta\mathfrak{b}$*.*

i) *There is an* $\mathfrak{o}$*-polarization* ϕ *on* $B = A/\boldsymbol{\kappa}[\theta]$*, such that* $\ker \phi$ *is isomorphic to* $(A[\theta]/\boldsymbol{\kappa}[\theta]) \oplus \boldsymbol{\kappa}[\mathfrak{b}]$*.*
ii) *If* $|\boldsymbol{\kappa}|$ *is minimal for* $\mathfrak{I}_A^{\mathfrak{l}}$ *and* $\mathfrak{l} = (\theta)$ *is a prime dividing* $\mathfrak{a}$*, then* $2 \dim_{\mathbb{F}_{\mathfrak{l}}} \boldsymbol{\kappa}[\mathfrak{l}] \leq \dim_{\mathbb{F}_{\mathfrak{l}}} A[\mathfrak{l}]$*. Further, some composition factor of* $A[\mathfrak{l}]/\boldsymbol{\kappa}[\mathfrak{l}]$ *is symplectic.*

Proof. By Proposition 3.4.4, $\mathfrak{a}$ is squarefree, so $\mathfrak{b}$ is prime to θ. Since θ is totally positive, it is a sum of squares in the fraction field of $\mathfrak{o}$. It follows that $\psi = \varphi\theta$ is a polarization on A whose kernel obviously contains $\boldsymbol{\kappa}$. Let $\Lambda = \boldsymbol{\kappa}[\theta]$ and let

$\Lambda^\perp \subseteq \ker\psi$ be its orthogonal complement under the $\bar{e}^\psi$ pairing (3.4.1). Given a in Λ and a' in $\ker\psi$, write $a' = \theta\alpha'$. By the definitions of the pairings, we have

$$\bar{e}^\psi(a,a') = \bar{e}_{\mathfrak{n}}(a,\psi(\alpha')) = \bar{e}_{\mathfrak{n}}(a,\varphi(\theta\alpha')) = \bar{e}^\varphi(a,\theta a').$$

Since the orthogonal complement of Λ with respect to the $\bar{e}^\varphi$ pairing on $\boldsymbol{\kappa}$ is $\boldsymbol{\kappa}[\mathfrak{b}]$, we find that $\Lambda^\perp = \{a' \in \ker\psi \mid \theta a' \in \boldsymbol{\kappa}[\mathfrak{b}]\}$. But multiplication by θ is an isomorphism on $\boldsymbol{\kappa}[\mathfrak{b}]$. Hence $\Lambda^\perp = A[\theta] + \boldsymbol{\kappa}[\mathfrak{b}] \supseteq \Lambda$, and so Λ is totally isotropic for the $\bar{e}^\psi$ pairing. By Lemma 3.4.3, there is an induced polarization ϕ on B, such that $\ker\phi \simeq \Lambda^\perp/\Lambda = (A[\theta] + \boldsymbol{\kappa}[\mathfrak{b}])/\boldsymbol{\kappa}[\theta]$. This proves (i).

Now let $(C,\gamma) \preccurlyeq (B,\phi)$ be $\mathfrak{o}$-minimal. Then any irreducible submodule of $\ker\gamma$ is non-singular by Proposition 3.4.4 and (ii) follows from minimality of $|\boldsymbol{\kappa}|$. ☐

Lemma 3.4.8. *Let (A,φ) and (B,ϕ) be $\mathfrak{o}$-polarized, with B in $\mathfrak{I}_A^{\mathfrak{l}}$. If $\boldsymbol{\kappa} = \ker\varphi$ has minimal order for $\mathfrak{I}_A^{\mathfrak{l}}$, then $\mathfrak{a} = \mathrm{ann}_{\mathfrak{o}}(\boldsymbol{\kappa})$ divides $\mathfrak{a}' = \mathrm{ann}_{\mathfrak{o}}(\ker\phi)$ provided*

- i) *each prime factor $\mathfrak{l}$ of $\mathfrak{a}$ has a totally positive generator and*
- ii) *$\mathbf{m}_E(A[\mathfrak{l}]) = 1$ whenever E in $\mathfrak{S}_{\mathfrak{l}}(A)$ has non-trivial Galois action and admits a symplectic pairing.*

The second condition is fulfilled when the reduced conductor of A is squarefree.

Proof. We argue as in [21, p. 213ff]. Let $\psi = f^*\phi = \hat{f}\phi f$ be the polarization on A induced by the $\mathfrak{o}$-isogeny $f\colon A \to B$. Write $\Phi = \ker f$, so $\ker\hat{f}$ is isomorphic to $\Phi^* = \mathrm{Hom}(\Phi, \mathbb{G}_{\mathrm{m}})$. We can find α and β in $\mathfrak{o}$ such that $\beta\varphi = \alpha\psi$. By Proposition 3.4.4, the $\mathfrak{l}$-primary part of $\boldsymbol{\kappa}$ is semisimple and annihilated by $\mathfrak{l}$. Furthermore, any simple component E is symplectic, with non-trivial Galois action. For V in $\mathfrak{S}_{\mathfrak{l}}(A)$, the multiplicity $\mathbf{m}_V$ is additive on short exact sequences and $\mathbf{m}_V(A[\mathfrak{l}])$ is isogeny invariant. It follows that

$$\mathbf{m}_V(\Phi) + \mathbf{m}_V(\Phi^*) + \mathbf{m}_V(\ker\phi) = \mathrm{ord}_{\mathfrak{l}}(\beta/\alpha)\mathbf{m}_V(A[\mathfrak{l}]) + \mathbf{m}_V(\boldsymbol{\kappa}[\mathfrak{l}]). \tag{3.4.9}$$

Suppose $\mathfrak{l}$ does not divide $\mathfrak{a}'$. Put $V = E$ in (3.4.9) to show that $\mathrm{ord}_{\mathfrak{l}}(\beta/\alpha)$ is odd. By Lemma 3.4.7, $A[\mathfrak{l}]/\boldsymbol{\kappa}[\mathfrak{l}]$ has an irreducible symplectic constituent E' with non-trivial Galois action. By assumption, $\mathbf{m}_{E'}(A[\mathfrak{l}]) = 1$, so $\mathbf{m}_{E'}(\boldsymbol{\kappa}[\mathfrak{l}]) = 0$ and then $\mathbf{m}_{E'}(\ker\phi)$ is odd. Hence $\mathfrak{l}$ divides $\mathfrak{a}'$. Indeed, $\mathfrak{a}$ divides $\mathfrak{a}'$ because $\mathfrak{a}$ is squarefree. ☐

Corollary 3.4.10. *There is at most one symplectic module in $\mathfrak{S}_{\mathfrak{l}}(A)$ if one of the following holds, with N the reduced conductor of A and p a prime:*

- i) *$N = p$ and $\ell \le 19$, or*
- ii) *$\ell = 2$, $N = mp$ and $\mathrm{rad}(m)$ divides a Q in $\mathfrak{T}_0$ of Proposition 3.3.8.*

Proof. Under (i) or (ii), Proposition 3.3.8 shows that p must appear in the conductor of any member of $\mathfrak{S}_{\mathfrak{l}}(A)$. But $\mathfrak{f}_p(A[\mathfrak{l}]) \le 1$ by (3.2.8). ☐

Theorem 3.4.11. *Let A be a semistable $(\mathfrak{o}, mp)$-paramodular abelian variety, with $\mathrm{rad}(m) \le 10$ and prime $p \ge 11$. If the strict ideal class group of $\mathfrak{o}$ is trivial, then A is $\mathfrak{o}$-isogenous over $\mathbb{Q}$ to a principally polarized abelian variety. In particular, A is $\mathbb{Q}$-isogenous to a Jacobian if it is a surface.*

Proof. Assume that A is an $\mathfrak{o}$-linear polarization φ whose kernel $\boldsymbol{\kappa} \ne 0$ has minimal order for the isogeny class. Let $\mathfrak{l}$ be a prime of $\mathfrak{o}$ dividing $\mathfrak{a} = \mathrm{ann}_{\mathfrak{o}}(\boldsymbol{\kappa})$ and let ℓ lie below $\mathfrak{l}$ in $\mathbb{Z}$. Proposition 3.4.4 implies that both $W = \boldsymbol{\kappa}[\mathfrak{l}]$ and $W' = A[\mathfrak{l}]/\boldsymbol{\kappa}[\mathfrak{l}]$ have irreducible constituents of dimension at least 2 over $\mathbb{F} = \mathfrak{o}/\mathfrak{l}$. By Lemma

3.2.1, $A[\mathfrak{l}]$ is four-dimensional over $\mathbb{F}$. Thus W and W' admit odd *irreducible* Galois representations into $\mathrm{GL}_2(\mathbb{F})$. By semistability and Lemma 3.2.5, the conductors of W and W' are squarefree.

We consider three cases. If ℓ is prime to pm, the group schemes $\mathcal{W}$ and $\mathcal{W}'$ are finite flat over $\mathbb{Z}_\ell$. The conductor exponents at p satisfy $\mathfrak{f}_p(W) + \mathfrak{f}_p(W') \leq \mathfrak{f}_p(A[\mathfrak{l}]) \leq 1$, thanks to (3.2.8). Hence the conductor n_0 of one of them is prime to p, and so n_0 divides $\mathrm{rad}(m)$. By [27], the corresponding Galois module gives rise to a cusp form of weight 2 on $\Gamma_0(n_0)$, contradicting $n_0 \leq 10$.

If $\ell = p$, we work over $\mathbb{Z}_p$. The action of $\mathfrak{o}$ extends to the Néron model and $\tau_p(A) = 1$. We infer from [32, Ch. 4][2] that there is a finite flat $\mathbb{F}$-module subscheme $\mathcal{F}$ of $A[\mathfrak{l}]$ of dimension 3. Since $\mathcal{W}$ is irreducible it must be contained in $\mathcal{F}$. The conductor of W is prime to p by definition. We conclude as above.

When ℓ divides m, the Galois module W or W' whose conductor n_0 is prime to p either has weight 2 or has weight $\ell + 1$, but can be twisted to have weight 2 and level ℓn_0. Since $J_1(\mathrm{rad}(m))$ has genus 0, we again have a contradiction.

When A is a surface, its conductor precludes being isogenous to a product of two elliptic curves. Since we may assume A to be principally polarized, we conclude from [69] that it is a Jacobian. $\square$

3.5. **Cohomology.** If X and Y are finite $\mathbb{F}[G]$-modules, then $\mathrm{Ext}^1_{\mathbb{F}[G]}(X, Y)$ is isomorphic to $H^1(G, \mathrm{Hom}_{\mathbb{F}}(X, Y))$, as in [4, 12]. The cohomology class corresponding to an exact sequence of $\mathbb{F}[G]$-modules,

$$0 \to Y \to V \xrightarrow{\pi} X \to 0, \tag{3.5.1}$$

is represented by a 1-cocycle c, with $c_g(x) = (gi - i)(x) = g(i(g^{-1}x)) - i(x)$, where $g \in G$ and $i \in \mathrm{Hom}_{\mathbb{F}}(X, V)$ is any section of π.

Lemma 3.5.2. *Let $X' = \pi(V^G)$ and $Y' = Y \cap \mathfrak{a}_G V$, where $\mathfrak{a}_G$ is the augmentation ideal in $\mathbb{F}[G]$. The following sequences are $\mathbb{F}[G]$-split exact:*

i) $0 \to Y \to \pi^{-1}(X') \to X' \to 0,$ *with* $\dim_{\mathbb{F}} X^G/X' \leq \dim_{\mathbb{F}} H^1(G, Y)$,

ii) $0 \to Y/Y' \to V/Y' \to X \to 0,$ *with* $\dim_{\mathbb{F}} Y'/\mathfrak{a}_G Y \leq \dim_{\mathbb{F}} H^1(G, \widehat{X})$.

Proof. The cohomology sequence $0 \to Y^G \to V^G \xrightarrow{\pi} X^G \xrightarrow{\delta} H^1(G, Y)$ implies our bound on $\dim X^G/X'$. If W is a complement in V^G for Y^G, then $\pi^{-1}(X') = Y + V^G = Y \oplus W$ provides a splitting in (i).

The homology sequence $H_1(G, X) \xrightarrow{\partial} Y/\mathfrak{a}_G Y \to V/\mathfrak{a}_G V \to X/\mathfrak{a}_G X \to 0$ shows that $\dim Y'/\mathfrak{a}_G Y \leq \dim H_1(G, X) = \dim H^1(G, \widehat{X})$, by duality. If W is an $\mathbb{F}$-subspace of V containing $\mathfrak{a}_G V$, then W is a Galois module. We may choose W so that $V/\mathfrak{a}_G V = ((Y + \mathfrak{a}_G V)/\mathfrak{a}_G V) \oplus (W/\mathfrak{a}_G V)$. Then $V/Y' = (Y/Y') \oplus (W/Y')$ is a splitting in (ii). Alternatively, observe that (i) and (ii) are dual statements. $\square$

Let $\{G_i\}$ be a collection of subgroups of G. For each i, let $\overline{Y}_i$ be a G_i-quotient of Y and X_i a G_i-submodule of X. Put $\boldsymbol{\kappa}_1 = \ker\{H^1(G, Y) \to \prod H^1(G_i, \overline{Y}_i)\}$ and $\boldsymbol{\kappa}_2 = \ker\{H^1(G, \widehat{X}) \to \prod H^1(G_i, \widehat{X}_i)\}$, where the maps are induced by restriction.

Corollary 3.5.3. *Let $Y_i^{\mathrm{ker}} = \ker\{Y \to \overline{Y}_i\}$ and $\overline{V}_i = V/Y_i^{\mathrm{ker}}$.*

i) *If the sequences $0 \to \overline{Y}_i \to \overline{V}_i \to X \to 0$ are $\mathbb{F}[G_i]$-split exact for all i, then $\dim X^G/X' \leq \dim \boldsymbol{\kappa}_1$, where $X' = \pi(V^G)$.*

[2] We thank J. de Jong for this reference.

ii) *If the sequences* $0 \to Y \to \pi^{-1}(X_i) \to X_i \to 0$ *are* $\mathbb{F}[G_i]$*-split exact for all* i, *then* $\dim Y'/\mathfrak{a}_G Y \le \dim \boldsymbol{\kappa}_2$, *where* $Y' = Y \cap \mathfrak{a}_G Y$.

Proof. i) By the splitting, π induces a surjection $\overline{V}^{G_i} \twoheadrightarrow X^{G_i}$. It follows from the diagram below that the image of ∂ is contained in $\boldsymbol{\kappa}_1$. But $X^G/X' \simeq \text{Image}\ \partial$.

$$\begin{array}{ccccc} V^G & \xrightarrow{\pi} & X^G & \xrightarrow{\partial} & H^1(G,Y) \\ \downarrow & & \downarrow & & \downarrow \text{res} \\ \overline{V}_i^{G_i} & \xrightarrow{\pi} & X^{G_i} & \xrightarrow{0} & H^1(G_i, \overline{Y}_i)\ . \end{array}$$

ii) Similarly, the diagram below shows that δ vanishes on $C = \sum$ cores $H_1(G_i, X_i)$:

$$\begin{array}{ccccc} H_1(G_i, \pi^{-1}(X_i)) & \longrightarrow & H_1(G_i, X_i) & \xrightarrow{0} & Y/\mathfrak{a}_{G_i} Y \\ & & \text{cores}\downarrow & & \downarrow \\ & & H_1(G, X) & \xrightarrow{\delta} & Y/\mathfrak{a}_G Y \end{array}$$

Hence $\dim Y'/\mathfrak{a}_G Y = \dim \text{Image}\ \delta \le \dim H_1(G,X)/C = \dim \boldsymbol{\kappa}_2$, where the last equality holds by duality. □

Remark 3.5.4. Let G_0 be the subgroup of G acting trivially on both X and Y in (3.5.1) and let $\Delta = G/G_0$. Assume $\text{char}(\mathbb{F}) = \ell$ and write $\mathfrak{H} = \text{Hom}_{\mathbb{F}}(X, Y)$. Then the image of $[c]$ under the restriction map

$$H^1(G, \mathfrak{H}) \xrightarrow{\text{res}} H^1(G_0, \mathfrak{H})^{\Delta} = \text{Hom}_{\mathbb{F}_\ell[\Delta]}(G_0, \mathfrak{H})$$

is an $\mathbb{F}_\ell[\Delta]$-homomorphism $\tilde{c}:\ G_0 \to \mathfrak{H}$, with $\tilde{c}_g(x) = (gi - i)(x)$ for all g in G_0 and x in X. If G_0 acts faithfully on V, then $\tilde{c}$ is injective. Indeed, if $\tilde{c}_g = 0$, then g acts trivially on both Y and $i(X)$, so $g = 1$ on $V = Y + i(X)$. Let

$$Y'' = \mathfrak{a}_{G_0} V = \mathfrak{a}_{G_0}(Y + i(X)) = \mathfrak{a}_{G_0} i(X) = \text{span}\{\tilde{c}_g(X) \mid g \text{ in } G_0\}.$$

Then $Y'' \subseteq Y$ and $0 \to Y/Y'' \to V/Y'' \to X \to 0$ is $\mathbb{F}[G_0]$-split exact.

4. Nuggets

4.1. **Introducing nuggets.** If the $\mathfrak{o}$-module scheme $\mathcal{V}$ has a subscheme isomorphic to $\mathcal{Z}_\mathfrak{l}$ with quotient isomorphic to $\boldsymbol{\mu}_\mathfrak{l}$ and $\text{Ext}^1_{\underline{D}}(\boldsymbol{\mu}_\mathfrak{l}, \mathcal{Z}_\mathfrak{l}) = 0$, then $\mathcal{V}$ admits a filtration with graded pieces in reverse order. More generally, when considering increasing filtrations of $\mathfrak{o}$-module schemes, we refer to "moving $\mathcal{Z}_\mathfrak{l}$ to the right" and "moving $\boldsymbol{\mu}_\mathfrak{l}$ to the left" when modifying filtrations in that way. To account for the failure of splitting and the existence of exceptional $\mathfrak{o}$-module schemes, we introduce the weight $\mathbf{w}(\mathcal{F})$ of a filtration, using several invariants which we now define.

Let $\mathcal{W}$ be an $\mathfrak{l}$-primary $\mathfrak{o}$-module scheme and $\mathcal{F}$ a composition series for $\mathcal{W}$. Let $\mathbf{t}_m(\mathcal{F})$ be the multiplicity of $\boldsymbol{\mu}_\mathfrak{l}$ in $\mathbf{gr}\,\mathcal{F}$ and $\mathbf{t}_e(\mathcal{F})$ that of $\mathcal{Z}_\mathfrak{l}$. Then $\mathbf{t}_m(\mathcal{F})$ and $\mathbf{t}_e(\mathcal{F})$ are determined by the Galois module $W = \mathcal{W}(\overline{\mathbb{Q}})$ if $\ell > 2$. The sum $\mathbf{t}_m(\mathcal{F}) + \mathbf{t}_e(\mathcal{F})$ is the number of trivial $\mathbb{F}_\mathfrak{l}[G_\mathbb{Q}]$-constituents of W when $\ell = 2$.

Notation 4.1.1. Set $\epsilon_0(\mathcal{W}) = \mathbf{t}_m(\mathcal{F}) + \mathbf{t}_e(\mathcal{F})$ for any composition series $\mathcal{F}$ of $\mathcal{W}$. This depends only on the Galois module W.

For a fixed λ over ℓ, we write $\mathbf{t}_m^\lambda(\mathcal{F})$ (resp. $\mathbf{t}_e^\lambda(\mathcal{F})$) as the multiplicity of $\boldsymbol{\mu}_\mathfrak{l}$ (resp. $\mathcal{Z}_\mathfrak{l}$) in any composition series for $\mathcal{W}_{|\mathbb{Z}_\ell}$. They are local invariants of $\mathcal{W}$ by Lemma 3.1.4. When $\mathcal{F}$ is prosaic, $\mathbf{t}_m^\lambda(\mathcal{F}) = \mathbf{t}_m(\mathcal{F})$ and $\mathbf{t}_e^\lambda(\mathcal{F}) = \mathbf{t}_e(\mathcal{F})$.

For a simple $\mathfrak{o}$-module scheme $\mathcal{Y}$, put $\mathbf{w}(\mathcal{Y}) = \mathbf{t}_e^\lambda(\mathcal{Y})\mathbf{t}_m^\lambda(\mathcal{Y})$. Let $\mathbf{x}(\mathcal{F})$ be the number of exceptional constituents and set

$$\alpha(\mathcal{F}) = \mathbf{t}_e^\lambda(\mathcal{F}) + \mathbf{x}(\mathcal{F}) \quad \text{and} \quad \beta(\mathcal{F}) = \mathbf{t}_m^\lambda(\mathcal{F}) + \mathbf{x}(\mathcal{F}).$$

Definition 4.1.2. Let $\mathcal{F}' = \{0 = \mathcal{W}_0 \subset \cdots \subset \mathcal{W}_{s-1}\}$ be a filtration as in (3.1.2) and $\mathcal{Y} = \mathcal{W}_s/\mathcal{W}_{s-1}$. Define inductively

$$\mathbf{w}(\mathcal{F}) = \mathbf{w}(\mathcal{F}') + \mathbf{w}(\mathcal{Y}) + \begin{cases} \alpha(\mathcal{F}') & \text{if } \mathcal{Y} = \boldsymbol{\mu}_{\mathfrak{l}}, \\ \mathbf{t}_e(\mathcal{F}')\beta(\mathcal{Y}) & \text{if } \mathcal{Y} \text{ is exceptional}, \\ 0 & \text{if } \mathcal{Y} = \mathcal{Z}_{\mathfrak{l}}. \end{cases}$$

Lemma 4.1.3.

i) *For $\mathcal{V} \subset \mathcal{W}$, let $\mathcal{F}_1$ and $\mathcal{F}_2$ be filtrations of $\mathcal{V}$ and $\mathcal{W}/\mathcal{V}$, respectively, and write $\mathcal{F}_1\mathcal{F}_2$ for the induced filtration of $\mathcal{W}$. Then*

$$\mathbf{w}(\mathcal{F}_1\mathcal{F}_2) = \mathbf{w}(\mathcal{F}_1) + \mathbf{w}(\mathcal{F}_2) - \mathbf{t}_e(\mathcal{F}_1)\mathbf{t}_m(\mathcal{F}_2) + \alpha(\mathcal{F}_1)\mathbf{t}_m(\mathcal{F}_2) + \mathbf{t}_e(\mathcal{F}_1)\beta(\mathcal{F}_2).$$

ii) *If $\mathcal{F}$ is a prosaic filtration of $\mathcal{W}$, then $\mathbf{w}(\mathcal{F}) \leq \mathbf{t}_e(\mathcal{F})\mathbf{t}_m(\mathcal{F})$ with equality only if all the $\mathcal{Z}_{\mathfrak{l}}$ are on the left and all the $\boldsymbol{\mu}_{\mathfrak{l}}$ on the right.*

iii) *If $\mathcal{F}^D$ is the filtration of $\mathcal{W}^D$ induced by $\mathcal{F}$ via Cartier duality, then $\mathbf{w}(\mathcal{F}) = \mathbf{w}(\mathcal{F}^D)$.*

Proof. The claims follow easily by induction on the length of a filtration, except perhaps for the second part of (ii). There, it suffices to check that if $\mathcal{F} = \mathcal{F}'\mathcal{Y}$, with $\mathcal{Y}$ simple, then equality holds for $\mathcal{F}$ if and only if it holds for $\mathcal{F}'$ and $\mathcal{Y} = \mathcal{Z}_{\mathfrak{l}}$. □

Definition 4.1.4. A filtration on the $\mathfrak{l}$-primary $\mathfrak{o}$-module scheme $\mathcal{W}$ is *special* if:

i) $0 \subset \mathcal{Z} \subset \mathcal{W}$ with $\mathcal{Z} \neq 0$ étale and $\mathcal{W}/\mathcal{Z} = \mathcal{M} \neq 0$ multiplicative, or

ii) $0 \subseteq \mathcal{Z} \subset \mathcal{V} \subseteq \mathcal{W}$, with $\mathcal{V}/\mathcal{Z} = \mathcal{E}$ exceptional and at least one of $\mathcal{Z}$ or $\mathcal{W}/\mathcal{V} = \mathcal{M}$ not trivial. Then we have the short exact sequences

$$0 \to \mathcal{Z} \to \mathcal{V} \to \mathcal{E} \to 0 \quad \text{and} \quad 0 \to \mathcal{V} \to \mathcal{W} \to \mathcal{M} \to 0. \tag{4.1.5}$$

Lemma 4.1.6. *Let $0 \to \mathcal{Z} \to \mathcal{V} \to \mathcal{X} \to 0$ be exact, with $\mathcal{Z}$ filtered by $\mathcal{Z}_{\mathfrak{l}}$'s, $\mathcal{X}$ connected or exceptional and $\mathfrak{l}\,\mathcal{X} = 0$. Set $\mathcal{Z}' = \mathcal{Z}[\mathfrak{l}]$, $\overline{\mathcal{V}} = \mathcal{V}/\mathcal{Z}'$ and $\overline{\mathcal{Z}} = \mathcal{Z}/\mathcal{Z}'$.*

i) *The sequence $0 \to \overline{\mathcal{Z}} \to \overline{\mathcal{V}} \to \mathcal{X} \to 0$ is split exact.*

ii) *If $\mathfrak{l}\,\mathcal{Z} = 0$, then $\mathfrak{l}\,\mathcal{V} = 0$.*

iii) *If $\mathcal{W}$ admits a special filtration with $\mathcal{Z}$ and $\mathcal{M}$ killed by $\mathfrak{l}$, then $\mathfrak{l}\,\mathcal{W} = 0$.*

Proof. By the snake lemma, $0 \to \mathcal{Z}' \to \mathcal{V}[\mathfrak{l}] \xrightarrow{f} \mathcal{X} \to \mathcal{Z}/\mathfrak{l}\,\mathcal{Z}$. If $\mathcal{X}$ is exceptional, f is surjective by irreducibility of the Galois module X. If $\mathcal{X}$ is connected, its image in the étale group scheme $\mathcal{Z}/\mathfrak{l}\,\mathcal{Z}$ is trivial, also proving surjectivity of f. Thus the subgroup $\mathcal{V}[\mathfrak{l}]/\mathcal{Z}'$ of $\overline{\mathcal{V}}$ is isomorphic to $\mathcal{X}$ and provides a splitting in (i). Surjectivity of f further implies the isomorphism $\overline{\mathcal{Z}} \simeq \mathcal{V}/\mathcal{V}[\mathfrak{l}]$, from which (ii) follows.

In (iii), we may now assume $\mathcal{V}/\mathcal{Z}$ is exceptional and $\mathfrak{l}\,\mathcal{V} = 0$. The snake lemma for multiplication by $\mathfrak{l}$ gives $0 \to \mathcal{V} \to \mathcal{W}[\mathfrak{l}] \to \mathcal{M} \to \mathcal{V}$. Then the Mayer-Vietoris sequence [51] shows that $\mathrm{Hom}_R(\mathcal{M}, \mathcal{V}) = \mathrm{Hom}_R(\mathcal{M}, \mathcal{Z}) = 0$. The first equality holds by considering the Galois modules and the second because over $\mathbb{Z}_\ell$, $\mathcal{M}$ is connected, while $\mathcal{Z}$ is étale. □

Remark 4.1.7. If $\mathcal{V}_1$ and $\mathcal{V}_3$ are annihilated by $\mathfrak{l}$ and if V_1 and V_3 have no Galois constituents in common, then the exactness of $0 \to \mathcal{V}_1 \to \mathcal{V}_2 \to \mathcal{V}_3 \to 0$ implies that $\mathcal{V}_2$ is annihilated by $\mathfrak{l}$ as well.

Proposition 4.1.8. *Suppose that $\mathcal{W}$ admits a filtration $\mathcal{F} = \mathcal{F}_1\mathcal{E}\mathcal{F}_2$ with $\mathcal{F}_i$ prosaic. Then $\mathbf{w}(\mathcal{F}) \le \mathbf{t}_e^\lambda(\mathcal{W})\mathbf{t}_m^\lambda(\mathcal{W}) + \epsilon_0(\mathcal{W})$ with equality if and only if $\mathcal{F}$ is special.*

Proof. We apply Lemma 4.1.3 and find

$$\begin{aligned}
\mathbf{w}(\mathcal{F}) &= \mathbf{w}(\mathcal{F}_1) + \mathbf{w}(\mathcal{E}) + \mathbf{w}(\mathcal{F}_2) + \mathbf{t}_e(\mathcal{F}_1)\mathbf{t}_m(\mathcal{F}_2) + \alpha(\mathcal{E})\mathbf{t}_m(\mathcal{F}_2) + \mathbf{t}_e(\mathcal{F}_1)\beta(\mathcal{E})\\
&\le \mathbf{t}_e^\lambda(\mathcal{W})\mathbf{t}_m^\lambda(\mathcal{W}) - \mathbf{t}_e^\lambda(\mathcal{E})\mathbf{t}_m(\mathcal{F}_1) - \mathbf{t}_m^\lambda(\mathcal{E})\mathbf{t}_e(\mathcal{F}_2) - \mathbf{t}_e(\mathcal{F}_2)\mathbf{t}_m(\mathcal{F}_1)\\
&\qquad\qquad\qquad\qquad\qquad + \mathbf{t}_e(\mathcal{F}_1) + \mathbf{t}_m(\mathcal{F}_2)\\
&\le \mathbf{t}_e^\lambda(\mathcal{W})\mathbf{t}_m^\lambda(\mathcal{W}) + \epsilon_0(\mathcal{W}).
\end{aligned}$$

By Lemma 4.1.3, the first inequality is strict unless $\mathbf{gr}\,\mathcal{F}_i = [\mathcal{Z}_\mathfrak{l}^{a_i}\,\boldsymbol{\mu}_\mathfrak{l}^{b_i}]$, and then $\epsilon_0(\mathcal{W}) = a_1+b_1+a_2+b_2$ while $\mathbf{t}_e(\mathcal{F}_1)+\mathbf{t}_m(\mathcal{F}_2) = a_1+b_2$. Hence the last inequality is strict, unless $b_1 = 0 = a_2$. □

Definition 4.1.9. An $\mathfrak{o}$-module scheme $\mathcal{W}$ is a *nugget* if either it is exceptional or it satisfies the following two properties:

i) $\mathcal{W}$ has no $\mathfrak{o}$-subscheme isomorphic to $\boldsymbol{\mu}_\mathfrak{l}$ and no quotient isomorphic to $\mathcal{Z}_\mathfrak{l}$.
ii) $\mathcal{W}$ has a *special* filtration $\mathcal{F}$. No other filtration has strictly lower weight.

If the nugget $\mathcal{W}$ has no exceptional subquotient, it is called a *prosaic nugget.* We usually keep the filtration $\mathcal{F}$ implicit.

The Cartier dual of a nugget $\mathcal{W}$ is a nugget and Lemma 4.1.6 shows that $\mathfrak{l}\mathcal{W} = 0$. Let $\mathcal{Z}'$ and $\mathcal{M}'$ be $\mathfrak{o}$-module subschemes of $\mathcal{Z}$ and $\mathcal{M}$, with both $\overline{\mathcal{Z}} = \mathcal{Z}/\mathcal{Z}'$ and $\mathcal{M}'$ non-zero if $\mathcal{W}$ is prosaic. Write $\mathcal{W}'$ for the pre-image of $\mathcal{M}'$ in $\mathcal{W}$ and set $\overline{\mathcal{V}} = \mathcal{V}/\mathcal{Z}'$ and $\overline{\mathcal{W}} = \mathcal{W}'/\mathcal{Z}'$. Then $0 \subseteq \overline{\mathcal{Z}} \subseteq \overline{\mathcal{V}} \subseteq \overline{\mathcal{W}}$ is a special filtration, with $\overline{\mathcal{W}}/\overline{\mathcal{V}} \simeq \mathcal{M}'$. Lemma 4.1.6(ii) and Proposition 4.1.8 imply that the subquotient $\overline{\mathcal{W}}$ is a nugget, referred to as a *subnugget* of $\mathcal{W}$ by abuse. A prosaic nugget $\mathcal{W}$ has a subquotient nugget $\mathcal{W}'$ with $\mathbf{gr}\,\mathcal{W}' = [\mathcal{Z}_\mathfrak{l}\boldsymbol{\mu}_\mathfrak{l}]$, called the *core*, which may depend on the chosen special filtration. By Lemma 3.3.10, $\mathbb{Q}(W')$ is an elementary ℓ-extension of $\mathbb{Q}(\mu_\ell)$, split over ℓ and unramified outside $N_{W'}$.

Corollary 4.1.10. *If a nugget $\mathcal{W}$ contains a prosaic $\mathfrak{o}$-module subscheme $\mathcal{Y}$ with $N_Y = 1$, then $\mathcal{Y} \simeq \mathcal{Z}_\mathfrak{l}^r$.*

Proof. Since $\mathcal{Y}$ is prosaic, each constituent of Y is a one-dimensional $\mathbb{F}_\mathfrak{l}[G_\mathbb{Q}]$-module and the corresponding subquotient of $\mathcal{Y}$ is isomorphic to $\mathcal{Z}_\mathfrak{l}$ or $\boldsymbol{\mu}_\mathfrak{l}$ by Remark 3.3.6. Once we show that $\mathcal{Y}$ is étale at ℓ, the claim holds by Lemma 3.3.10(v). Let $\mathcal{F}'$ be a special filtration of $\mathcal{W}$ of minimal weight, as in Definition 4.1.9(ii).

If $\mathcal{W}$ is not prosaic, we have a filtration $\mathcal{F} = \mathcal{F}_1\mathcal{E}\mathcal{F}_2$ of $\mathcal{W}$, with $\mathcal{Y} \subseteq \mathcal{F}_1$. Since $\mathcal{F}'$ is special, $\mathbf{w}(\mathcal{F}')$ attains the upper bound in Proposition 4.1.8. Minimality of $\mathbf{w}(\mathcal{F}')$ implies that $\mathbf{w}(\mathcal{F}) = \mathbf{w}(\mathcal{F}')$, so $\mathcal{F}$ is also special. But then $\mathcal{F}_1$, and *a fortiori* $\mathcal{Y}$, is filtered by $\mathcal{Z}_\mathfrak{l}$'s. When $\mathcal{W}$ is prosaic, replace Proposition 4.1.8 by Lemma 4.1.3(ii) in this argument. □

Proposition 4.1.11. *Any $\mathfrak{l}$-primary $\mathfrak{o}$-module scheme $\mathcal{W}$ has a filtration*

$$0 \subseteq \mathcal{W}_0 \subseteq \mathcal{W}_1 \subseteq \cdots \subseteq \mathcal{W}_{r-1} \subseteq \mathcal{W}_r = \mathcal{W},$$

with $\mathcal{W}_0$ filtered by $\boldsymbol{\mu}_\mathfrak{l}$'s, $\mathcal{W}/\mathcal{W}_{r-1}$ filtered by $\mathcal{Z}_\mathfrak{l}$'s and $\mathcal{W}_{i+1}/\mathcal{W}_i$ a nugget for $i = 0, ..., r-2$. Such a filtration will be called a nugget filtration.

Proof. Denote by $\mu(\mathcal{Y})$ any maximal subscheme of $\mathcal{Y}$ filtered by $\boldsymbol{\mu}_\mathfrak{l}$'s. Dividing by $\mu(\mathcal{W})$, we may assume that $\mathcal{W}$ has no $\boldsymbol{\mu}_\mathfrak{l}$ submodule. For such $\mathcal{W}$, we prove the claim by induction, by producing a nugget $\mathcal{V} \subseteq \mathcal{W}$ with $\mu(\mathcal{W}/\mathcal{V}) = 0$.

i) Suppose there is a subscheme $\mathcal{Z}$ of $\mathcal{W}$ such that $\mathbf{gr}\,\mathcal{Z} = [\mathcal{Z}_{\mathfrak{l}}^r]$, with $r \geq 1$ and $\boldsymbol{\mu}(\mathcal{W}/\mathcal{Z}) \neq 0$. Choose one with r minimal and let $\mathcal{V}$ be the pullback of $\mu(\mathcal{W}/\mathcal{Z})$. By minimality of r and Lemma 4.1.3(ii), $\mathcal{V}$ is a prosaic nugget.

ii) Next, suppose for all subschemes $\mathcal{Z}$ of $\mathcal{W}$ filtered by $\mathcal{Z}_{\mathfrak{l}}$'s we have $\mu(\mathcal{W}/\mathcal{Z}) = 0$. If there is a subscheme $\mathcal{X}$ of $\mathcal{W}$ having a filtration with grading $[\mathcal{Z}_{\mathfrak{l}}^s\,\mathcal{E}]$, where $s \geq 0$ and $\mathcal{E}$ is exceptional, choose $\mathcal{X}$ to minimize $\mathbf{t}_e^\lambda(\mathcal{X})$. Thus the pullback $\mathcal{V}$ of $\mu(\mathcal{W}/\mathcal{X})$ has a special filtration and $\mu(\mathcal{W}/\mathcal{V}) = 0$. Minimality of $\mathbf{t}_e^\lambda(\mathcal{X})$ shows that $\mathcal{V}$ has no $\mathcal{Z}_{\mathfrak{l}}$ quotient, so $\mathcal{V}$ is a nugget by Proposition 4.1.8.

iii) When the only simple factors of $\mathcal{W}$ are $\mathcal{Z}_{\mathfrak{l}}$'s, we are done. □

4.2. **Prosaic nuggets.** We generalize [52, Cor. 4.2], allowing for $\mathfrak{o}$-action and several bad primes. In this section, $\mathbb{F} = \mathbb{F}_{\mathfrak{l}}$ and N is prime to ℓ. Recall that $\tilde{\ell} = 8$, 9 or ℓ if $\ell = 2$, 3 or $\ell \geq 5$ respectively. Let $\varpi(N)$ denote the number of distinct prime factors p of N. When $\ell = 2$ or 3, set $\varpi_\ell(N) = \varpi(N)$ if all p dividing N satisfy $p \equiv \pm 1 \bmod \tilde{\ell}$ and $\varpi_\ell(N) = \varpi(N) - 1$ otherwise. When $\ell \geq 5$, define

$$\varpi_\ell(N) = \#\{\text{primes } p \text{ dividing } N \mid p \equiv \pm 1 \bmod \ell\}.$$

Write $p^* = (-1)^{(p-1)/2}p$ for p odd.

Proposition 4.2.1. *With $R = \mathbb{Z}[1/N]$, we have* $\dim_{\mathbb{F}} \operatorname{Ext}^1_R(\boldsymbol{\mu}_{\mathfrak{l}}, \mathcal{Z}_{\mathfrak{l}}) = \varpi_\ell(N)$.

Proof. Proceed as in the proof of [52, Prop. 4.1] and use the Mayer-Vietoris sequence of [51, Cor. 2.4] to obtain the exact sequence

$$0 \to \operatorname{Ext}^1_R(\boldsymbol{\mu}_{\mathfrak{l}}, \mathcal{Z}_{\mathfrak{l}}) \to \operatorname{Ext}^1_{R[1/\ell]}(\boldsymbol{\mu}_{\mathfrak{l}}, \mathcal{Z}_{\mathfrak{l}}) \to \operatorname{Ext}^1_{\mathbb{Q}_\ell}(\boldsymbol{\mu}_{\mathfrak{l}}, \mathcal{Z}_{\mathfrak{l}}), \tag{4.2.2}$$

in which the last two terms may be studied via extensions of Galois modules.

Let L be the maximal elementary abelian ℓ-extension of $F = \mathbb{Q}(\boldsymbol{\mu}_\ell)$ such that L/F is unramified outside N and split over λ_F. Set $G = \operatorname{Gal}(L/\mathbb{Q})$, $G_0 = \operatorname{Gal}(L/F)$ and $\Delta = \operatorname{Gal}(F/\mathbb{Q})$.

By Lemma 4.1.6(iii), an extension $\mathcal{V}$ of $\boldsymbol{\mu}_{\mathfrak{l}}$ by $\mathcal{Z}_{\mathfrak{l}}$ over R is killed by $\mathfrak{l}$. If V is the associated $\mathbb{F}[G_{\mathbb{Q}}]$-module, Lemma 3.3.10 implies that $\mathbb{Q}(V)$ is contained in L. Conversely, if V is an $\mathbb{F}[G]$-module extending $\boldsymbol{\mu}_{\mathfrak{l}}$ by the trivial Galois module $\mathbb{F}$, then V arises, by (4.2.2), from an R-group scheme $\mathcal{V}$ as above. It thus suffices to determine $\operatorname{Ext}^1_{\mathbb{F}[G]}(\boldsymbol{\mu}_{\mathfrak{l}}, \mathbb{F}) \simeq H^1(G, \mathbb{F}(-1))$; cf. §3.5.

Since Δ has order prime to ℓ, inflation-restriction shows that

$$H^1(G, \mathbb{F}(-1)) = \operatorname{Hom}_{\mathbb{F}_\ell}(G_0, \mathbb{F}(-1))^\Delta = \mathbb{F} \otimes \operatorname{Hom}_{\mathbb{F}_\ell}(G_0, \mathbb{F}_\ell(-1))^\Delta.$$

Let X be the subgroup of $F^\times$ whose elements satisfy: (i) $x \in F_\lambda^{\times\,\ell}$ and (ii) $\operatorname{ord}_{\mathfrak{q}}(x) \equiv 0 \bmod \ell$ for all $\mathfrak{q}$ not dividing N. By Kummer theory, we have a perfect Δ-pairing $G_0 \times \overline{X} \to \mathbb{F}(1)$, where $\overline{X} = X/F^{\times\,\ell}$. It follows that $\operatorname{Hom}_{\mathbb{F}_\ell}(G_0, \mathbb{F}_\ell(-1))^\Delta$ is isomorphic to the ω^2-component $\overline{X}_{\omega^2}$, where ω is the mod-ℓ cyclotomic character.

Let $\overline{Y} = Y/F^{\times\,\ell}$, where Y is the subgroup of $F^\times$ satisfying only (ii) above. Write $\mathcal{C}$ for the ideal class group of F and $\overline{U}$ for the image in $\overline{Y}$ of the group of units. The natural action of Δ on the prime ideals $\mathfrak{p}$ of F dividing p induces an action on $J_p = \prod_{\mathfrak{p}|p} \mathbb{Z}/\ell\mathbb{Z}$. Schoof shows that $\dim_{\mathbb{F}_\ell}(J_p)_{\omega^2} = 1$ if $p \equiv \pm 1 \bmod \ell$ and 0 otherwise. In particular, if $\ell = 2$ or 3, then $\dim J_p = 1$ for all p.

We have the exact sequence of $\mathbb{F}_\ell[\Delta]$-modules

$$1 \to \mathcal{C}[\ell] \xrightarrow{h} \overline{Y}/\overline{U} \xrightarrow{i} \prod_{p|N} J_p \xrightarrow{j} \mathcal{C}/\mathcal{C}^\ell,$$

with i induced by $y \rightsquigarrow (\mathrm{ord}_\mathfrak{p}\, y)$ and j by $(c_\mathfrak{p}) \rightsquigarrow \prod_\mathfrak{p} \mathfrak{p}^{c_\mathfrak{p}}$. As for h, if the ideal $\mathfrak{a}^\ell = (y)$ is principal, then y is in Y and h is induced by $\mathfrak{a} \rightsquigarrow y$.

If $\ell \geq 5$, the ω^2-component of $\mathcal{C}[\ell^\infty]$ vanishes by the reflection principle and Herbrand's theorem [67, Thms. 6.17, 10.9]. Hence $\dim_{\mathbb{F}_\ell}(\overline{Y}/\overline{U})_{\omega^2} = \varpi_\ell(N)$. If $\ell = 2$ or 3, we have $\dim_{\mathbb{F}_\ell}(\overline{Y}/\overline{U})_{\omega^2} = \varpi(N)$.

Let U_λ be the group of local units in the completion F_λ and use bars to denote the respective multiplicative groups modulo ℓ^{th} powers. Embedding to the completion induces a map of $\overline{Y} \to U_\lambda F_\lambda^{\times\ell}/F_\lambda^{\times\ell} \simeq \overline{U}_\lambda$ and we have the exact sequence

$$1 \to \overline{U} \cap \overline{X} \to \overline{X} \to \overline{Y}/\overline{U} \xrightarrow{\beta} \overline{U}_\lambda/\overline{U}.$$

If $\ell = 2$ or 3, then $\overline{U} \cap \overline{X} = 1$ by direct calculation. Moreover, $\dim_{\mathbb{F}_\ell} \mathrm{Image}\, \beta = 0$ if $p \equiv \pm 1 \pmod{\tilde{\ell}}$ for all p dividing N and 1 otherwise. This implies our claim.

If $\ell \geq 5$, then $\dim_{\mathbb{F}_\ell} \overline{U}_{\omega^2} = 1$ and $(\overline{U}_\lambda/\overline{U})_{\omega^2} = 1$ by [67, Thms. 8.13, 8.25]. It follows that the non-trivial elements of $\overline{U}_{\omega^2}$ are not ℓ^{th} power locally, and so $\overline{U}_{\omega^2} \cap \overline{X} = 1$. This concludes the proof. □

Corollary 4.2.3. *Suppose $0 \to \mathcal{Z}_\mathfrak{l} \to \mathcal{V} \to \boldsymbol{\mu}_\mathfrak{l} \to 0$ is a non-split extension. Then either N_V is divisible by some prime $p \equiv \pm 1 \bmod \tilde{\ell}$ or else $\ell \leq 3$ and N_V is divisible by at least two primes.*

Remark 4.2.4. Let $\mathcal{V}$ be a prosaic nugget with $\mathbf{gr}\, \mathcal{V} = [\mathcal{Z} \boldsymbol{\mu}_\mathfrak{l}]$ and $\mathbf{gr}\, \mathcal{Z} = [\mathcal{Z}_\mathfrak{l}\, \mathcal{Z}_\mathfrak{l}]$. Let p, q be primes, with p dividing the conductor N' of the core and $(q, N') = 1$. Then generators of inertia at $v \,|\, p$ and $w \,|\, q$ can be put in the form

$$\sigma_v = \begin{bmatrix} 1 & a_v & b_v \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \sigma_w = \begin{bmatrix} 1 & a_w & b_w \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \tag{4.2.5}$$

We have $a_v = 0$ because $(\sigma_v - 1)^2 = 0$. Hence either $\mathcal{Z} \simeq \mathcal{Z}_\mathfrak{l}^2$ or $a_w \neq 0$ for some q dividing N_V. Since $\mathbb{Q}(Z)/\mathbb{Q}$ is an elementary ℓ-extension unramified at ℓ, Kronecker-Weber implies that any prime ramified in $\mathbb{Q}(Z)$ is 1 mod ℓ. Any Frobenius Φ_v at v normalizes σ_v and so acts trivially on Z.

Lemma 4.2.6. *Let S contain exactly one prime $p \equiv \pm 1 \bmod \tilde{\ell}$ and let $\mathcal{V}$ be a prosaic nugget over $\mathbb{Z}_S$. Then $\dim V = 2$, $N_V = p$ and $\mathcal{V}$ prolongs to an $\mathfrak{o}$-module scheme over $\mathbb{Z}[1/p]$ under any of the following conditions:*

i) *$\ell \geq 5$ and $S - \{p\}$ consists of primes $q \not\equiv \pm 1 \bmod \tilde{\ell}$.*
ii) *$\ell = 3$, $S = \{p, q\}$ with $q \equiv 2, 5 \bmod 9$, or $q \equiv 4, 7 \bmod 9$ and $p^{\frac{q-1}{3}} \not\equiv 1\,(q)$.*
iii) *$\ell = 2$, $S = \{p, q\}$ with $q^* \equiv 5\,(8)$ and the Hilbert symbol $(p^*, q^*)_\pi = -1$ for some place π.*

Proof. If $\dim V > 2$, dualize or pass to a subnugget if necessary, to get $\mathbf{gr}\, \mathcal{V} = [\mathcal{Z}\, \boldsymbol{\mu}_\mathfrak{l}]$, with $\mathbf{gr}\, \mathcal{Z} = [\mathcal{Z}_\mathfrak{l}\, \mathcal{Z}_\mathfrak{l}]$. Then any core of $\mathcal{V}$ has conductor p by Proposition 4.2.1.

We prove next that $\mathbb{Q}(Z) = \mathbb{Q}$. For (i) and (ii), this follows from the remark above. For (iii), note that Φ_v acts trivially on $\mathbb{Q}(Z)$ but non-trivially on the cubic subfield of $\mathbb{Q}(\boldsymbol{\mu}_q)$. For (iv), if not, then $\mathbb{Q}(Z) = \mathbb{Q}(\sqrt{q^*})$ and $\mathbb{Q}(V)$ is a D_4 field whose existence requires $(p^*, q^*)_\pi = 1$ for all places π, as explained below.

For v over p, $Y = (\sigma_v - 1)(V)$ is a Galois submodule of Z with corresponding subscheme $\mathcal{Y} \simeq \mathcal{Z}_\mathfrak{l}$. But then the core $\mathcal{V}/\mathcal{Y}$ is unramified at p. □

We now suppose $\mathfrak{l} \,|\, 2$. When writing $\mathbb{Q}(\sqrt{d})$ and its character χ_d, we assume d is squarefree. Recall that for p prime, $\chi_d(p)$ is the Legendre symbol $\left(\frac{d}{p}\right)$. Let $D_4^r(d_1, d_2)$ be the set of D_4-extensions $M/\mathbb{Q}$ such that

i) $|\mathcal{I}_v(M/\mathbb{Q})| \le 2$ at odd v, $\mathcal{I}_\lambda(M/\mathbb{Q})^\alpha = 1$ for all $\alpha > 1$ at even λ and
ii) the subfields fixed by the Klein 4-groups in $\mathrm{Gal}(M/\mathbb{Q})$ are $\mathbb{Q}(\sqrt{d_1})$ and $\mathbb{Q}(\sqrt{d_2})$, with d_1, d_2 odd and coprime.

For d_1, d_2 as in (ii), such an M exists exactly if $d_1x^2 + d_2y^2 = 1$ is solvable in $\mathbb{Q}$, i.e. for all π, the Hilbert symbols $(d_1, d_2)_\pi = 1$; cf. [24, 42]. Let $k = \mathbb{Q}(\sqrt{d_1 d_2})$ and let d_3 be the product of the odd p such that some v over p ramifies in M/k.

Notation 4.2.7. Let $D_4(d_1, d_2) \supseteq D_4^{nr}(d_1, d_2) \supseteq D_4^{sp}(d_1, d_2)$ be the following subsets of $D_4^r(d_1, d_2)$. In the first $d_3 = 1$, in the second $M/\mathbb{Q}$ is unramified over 2 and in the third M/k splits completely over 2.

Lemma 4.2.8. *If M' is in $D_4^r(d_1, d_2)$, then some twist M of M' is in $D_4(d_1, d_2)$. If $d_1 \equiv d_2 \equiv 1\,(4)$, we may even arrange that M be in $D_4^{nr}(d_1, d_2)$.*

Proof. If $d_3 \neq 1$, adjust its sign so $d_3 \equiv 1\,(4)$ and let $L = M'(\sqrt{d_3})$. Because $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ is the maximal abelian subfield of M', we have $\sqrt{d_3} \notin M'$. Hence $G = \mathrm{Gal}(L/\mathbb{Q}) \simeq D_4 \times C_2$ and the central involution of $\mathrm{Gal}(M'/\mathbb{Q})$ may be extended to $c \in \mathrm{Gal}(L/\mathbb{Q}(\sqrt{d_3}))$. If τ generates $\mathrm{Gal}(M'(\sqrt{d_3})/M')$, then the center of G is $\langle c, \tau\rangle = \mathrm{Gal}(L/K)$. For each prime p dividing d_3, there is a place v over p ramified in M'/K and in $K(\sqrt{d_3})/K$. Hence $\mathcal{I}_v(L/\mathbb{Q}) = \langle c\tau\rangle$ and the subfield M of L fixed by $c\tau$ satisfies our claim, since $c\tau$ is central.

Suppose $d_1 \equiv d_2 \equiv 1\,(4)$, M' is in $D_4(d_1, d_2)$ and $\lambda \,|\, 2$ ramifies in M'. Set $L = M'(i)$ and observe that $\mathcal{D}_\lambda(L/\mathbb{Q})$ is abelian. By Lemma 3.3.13, $g = (-1, L_\lambda/\mathbb{Q}_2)$ restricts non-trivially to $\mathrm{Gal}(M'/K)$ and to $\mathrm{Gal}(K(i)/K)$, so $g = c\tau$ and $M = L^{\langle c\tau\rangle}$ is in $D_4^{nr}(d_1, d_2)$. ☐

Proposition 4.2.9. *Let $V \supsetneq V_1 \supsetneq V_2 \supsetneq 0$ be semistable $\mathbb{F}[G_\mathbb{Q}]$-modules with $\dim_\mathbb{F} V = 3$. Set $X = V/V_2$, $K = \mathbb{Q}(V_1, X)$ and $L = \mathbb{Q}(V)$.*

i) *Then $\gcd(N_{V_1}, N_X) = 1$ and no prime dividing $N_{V_1} N_X$ ramifies in L/K.*
ii) *If $\mathbb{Q}(V_1) = \mathbb{Q}(\sqrt{d_1})$ and $\sqrt{d_2}$ is in $\mathbb{Q}(X)$, then $(d_1, d_2)_\pi = 1$ for all π.*

Proof. The shape (4.2.5) of the generators of inertia at bad places proves (i). Then d_1 and d_2 are coprime and they are odd by Definition 3.3.4.

Let σ_i be an involution of $G = \mathrm{Gal}(L/\mathbb{Q})$, non-trivial on $\mathbb{Q}(\sqrt{d_i})$. By matrix verification, σ_1 is trivial on X, and σ_2 is trivial on V_1 and centralizes the elementary 2-group $H = \mathrm{Gal}(L/\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}))$, while their commutator $c = [\sigma_1, \sigma_2] \neq 1$. The centralizer of σ_1 is trivial on X and so fixes $\sqrt{d_2}$. Using a commutator identity, this implies that $c \notin [\sigma_1, H] = \{\, [\sigma_1, h] \,|\, h \in H\}$. There is a maximal subgroup J of H containing $[\sigma_1, H]$ but not c. Since J is normal in H and $G = \langle \sigma_1, \sigma_2, H\rangle$, J is normal in G. Now $M = L^J$ is in $D_4^r(d_1, d_2)$. ☐

Corollary 4.2.10. *Let $\mathcal{V}$ be an $\mathbb{F}$-module scheme with $\mathbf{gr}\,\mathcal{V} = [\mathcal{Z}_\mathfrak{l}\, \boldsymbol{\mu}_\mathfrak{l}\, \boldsymbol{\mu}_\mathfrak{l}]$ and V its Galois module. Then 2 is unramified in $\mathbb{Q}(X)$ and splits in both $\mathbb{Q}(V_1)/\mathbb{Q}$ and $\mathbb{Q}(V)/\mathbb{Q}(X)$. If $\mathbb{Q}(V_1) = \mathbb{Q}(\sqrt{d_1})$ and $\sqrt{d_2} \in \mathbb{Q}(X)$, then $d_1 \equiv 1\,(8)$ and $d_2 \equiv 1\,(4)$. If $N_V = |d_1 d_2|$ and neither $d_i = 1$, then L contains a $D_4^{sp}(d_1, d_2)$ field.*

Proof. The grading on $\mathcal{V}$ implies that 2 is unramified in L and splits in $\mathbb{Q}(V_1)$. Hence $d_2 \equiv 1\,(4)$ and $d_1 \equiv 1\,(8)$. Moreover, even places split in $L/\mathbb{Q}(X)$ by Lemma 3.3.10(ii). Since $d_1 \equiv 1\,(8)$, they also split in $L/\mathbb{Q}(\sqrt{d_1 d_2})$. If $N_V = |d_1 d_2|$, then the field M defined in the proof above is in $D_4^{sp}(d_1, d_2)$. □

4.3. **Invariants of nuggets.** First we recall a result from [22, Chap. VII, §1].

Lemma 4.3.1. *Let χ be the character of an irreducible $\mathbb{F}[\Delta]$-module E and $\mathbb{F}_\chi = \mathbb{F}_\ell(\chi(g) \mid g \in \Delta)$. Write $\dot{E}$ for E, viewed as an $\mathbb{F}_\ell[\Delta]$-module. There is an irreducible $\mathbb{F}_\ell[\Delta]$-module X such that $\dot{E} = X^a$, with $a = [\mathbb{F} : \mathbb{F}_\chi]$, and*

i) *$X \otimes_{\mathbb{F}_\ell} \mathbb{F} = \bigoplus E^\eta$ is a direct sum of non-isomorphic conjugate representations, with η running over $\mathrm{Gal}(\mathbb{F}_\chi/\mathbb{F}_\ell)$;*
ii) *$(\mathrm{End}_{\mathbb{F}_\ell[\Delta]} X) \otimes_{\mathbb{F}_\ell} \mathbb{F} = \mathrm{End}_{\mathbb{F}[\Delta]}(X \otimes_{\mathbb{F}_\ell} \mathbb{F}) \simeq (\mathrm{End}_{\mathbb{F}[\Delta]} E)^b$ with $b = [\mathbb{F}_\chi : \mathbb{F}_\ell]$.*

Viewed as an $\mathbb{F}_\ell[\Delta]$-module, $\widehat{E} = \mathrm{Hom}_{\mathbb{F}}(E, \mathbb{F}) \simeq \widehat{X}^a$, where $\widehat{X} = \mathrm{Hom}_{\mathbb{F}_\ell}(X, \mathbb{F}_\ell)$, and similarly, $E^* = \mathrm{Hom}_{\mathbb{F}_\ell}(X, \boldsymbol{\mu}_\ell) \simeq X^{*\,a}$.

Notation 4.3.2. Let E be an exceptional $\mathbb{F}[G_\mathbb{Q}]$-module, T its set of bad primes and X an irreducible constituent of $\dot{E}$. Set $F = \mathbb{Q}(E) = \mathbb{Q}(\widehat{E})$ and $\Delta = \mathrm{Gal}(F/\mathbb{Q})$. For $S \supseteq T$, let $\Lambda_E(S)$ be the maximal elementary ℓ-extension Λ of F such that

i) Λ/F is unramified outside $\{\infty\} \cup (S \backslash T)$ and
ii) $\mathrm{Gal}(\Lambda/F) \simeq \widehat{X}^r$ as an $\mathbb{F}_\ell[\Delta]$-module.

Let $r_E(S)$ be the multiplicity of $\widehat{X}$ in $\mathrm{Gal}(\Lambda_E(S)/F)$ and $\Gamma_E(S) = \mathrm{Gal}(\Lambda_E(S)/\mathbb{Q})$.

We introduce invariants of nuggets over $\mathbb{Z}_S$ which have $\mathcal{E}$ as a subquotient, where $\mathcal{E}$ is an $\mathbb{F}$-module scheme with Galois module E and $\mathbb{F} = \mathbb{F}_\mathfrak{l}$. Let $\mathcal{Z} \simeq \mathcal{Z}_\mathfrak{l}^n$ and let $0 \to \mathcal{Z} \to \mathcal{V} \to \mathcal{E} \to 0$ be an exact sequence of acceptable $\mathbb{F}$-module schemes over $\mathbb{Z}_S$. Put $G = \mathrm{Gal}(\mathbb{Q}(V)/\mathbb{Q})$ and let $[c]$ in $H^1(G, \mathrm{Hom}_\mathbb{F}(E, Z))$ be the obstruction to the splitting of the Galois module sequence:

$$0 \to Z \to V \xrightarrow{\pi} E \to 0. \tag{4.3.3}$$

Remark 3.5.4 and Lemma 3.3.10 imply that $L = \mathbb{Q}(V)$ is contained in $\Lambda_E(S)$.

The next two lemmas contain local conditions at ℓ and the primes p dividing N_E implied by semistability of V.

Lemma 4.3.4. *Let $\mathcal{I}_v(L/\mathbb{Q}) = \langle \sigma_v \rangle$ and $M_v = (\sigma_v - 1)(E)$ for v over $p \,|\, N_E$. The exact sequence $0 \to Z \to \pi^{-1}(M_v) \to M_v \to 0$ consists of trivial $\mathbb{F}[\mathcal{I}_v]$-modules. If $\mathfrak{f}_p(V) = \mathfrak{f}_p(E)$, it is $\mathbb{F}[\mathcal{D}_v]$-split.*

Proof. It is clear that $\pi^{-1}(M_v) = (\sigma_v - 1)(V) + Z$ and $\mathcal{I}_v$ acts trivially because $(\sigma_v - 1)^2(V) = 0$. If $\mathfrak{f}_p(V) = \mathfrak{f}_p(E)$, then π induces an isomorphism of the $\mathbb{F}[\mathcal{D}_v]$-modules $(\sigma_v - 1)(V)$ and M_v, since they have the same $\mathbb{F}$-dimension. This gives us the $\mathbb{F}[\mathcal{D}_v]$-splitting. □

Lemma 4.3.5. *Let $0 \to \mathcal{Z} \to \mathcal{V} \to \mathcal{X} \to 0$ be an exact sequence of $\mathbb{F}$-module schemes over $\mathbb{Z}_\ell$ with $\mathcal{Z}$ étale. Fix λ over ℓ in $\mathbb{Q}(V)$ and consider the exact sequences of $\mathcal{D}_\lambda$-modules: $0 \to Z \to V \xrightarrow{\pi} X \to 0$ and $0 \to Z \to \pi^{-1}(X^0) \to X^0 \to 0$. The first is $\mathbb{F}[\mathcal{I}_\lambda]$-split and the second is $\mathbb{F}[\mathcal{D}_\lambda]$-split.*

Proof. The second sequence splits because $\mathcal{Z}^0 = 0$, so $\pi^{-1}(X^0) = Z + V^0$ is a direct sum. Now let $j : V \to V^{et}$ be the natural map with kernel V^0. Since the étale sequence $0 \to j(Z) \to V^{et} \to X^{et} \to 0$ consists of trivial $\mathcal{I}_\lambda$-modules, we can find an $\mathcal{I}_\lambda$-submodule W of V^{et} such that $V^{et} = j(Z) + W$ is a direct sum, with $W \simeq X^{et}$. It is easy to check that $V = j^{-1}(W) + Z$ is a direct sum, and this shows that the first sequence is $\mathbb{F}[\mathcal{I}_\lambda]$-split. □

The extension problem (4.3.3) has a Selmer interpretation. For a Galois extension $K/\mathbb{Q}$ with $\Lambda_E(S) \supseteq K \supseteq F = \mathbb{Q}(E)$, we define

$$H^1_{\mathcal{L}}(\mathrm{Gal}(K/\mathbb{Q}), \widehat{E}) = \ker : H^1(\mathrm{Gal}(K/\mathbb{Q}), \widehat{E}) \xrightarrow{\mathrm{res}} \prod_{v \mid \ell N_E} \mathcal{L}_v, \tag{4.3.6}$$

where $\mathcal{L}_v = \begin{cases} H^1(\mathcal{I}_v(K/\mathbb{Q}), \widehat{M}_v) & \text{if } v \mid N_E, \\ H^1(\mathcal{I}_v(K/\mathbb{Q}), \widehat{E}) \times H^1(\mathcal{D}_v(K/\mathbb{Q}), \widehat{E^0}) & \text{if } v \mid \ell. \end{cases}$

Corollary 4.3.7. *In* (4.3.3), *there is a submodule Z' of Z such that the exact sequence $0 \to Z/Z' \to V/Z' \to E \to 0$ is $\mathbb{F}[G]$-split and* $\dim_{\mathbb{F}} Z' \le \dim_{\mathbb{F}} H^1_{\mathcal{L}}(G, \widehat{E})$.

Proof. Apply Corollary 3.5.3(ii) with $X = E$ and $Y = Z$, using Lemmas 4.3.4 and 4.3.5 for the local conditions over N_E and ℓ, respectively. □

Lemma 4.3.8. *Let* $s_E(S) = \dim_{\mathbb{F}} H^1_{\mathcal{L}}(\mathrm{Gal}(\Lambda_E(S), \widehat{E})$. *Then*

$$s_E(S) \le \dim_{\mathbb{F}} H^1_{\mathcal{L}}(\Delta, \widehat{E}) + r_E(S) \dim_{\mathbb{F}} \mathrm{End}_{\mathbb{F}[\Delta]} \widehat{E}.$$

If $\mathcal{I}_\lambda(F/\mathbb{Q})$ contains an ℓ-Sylow subgroup of Δ for $\lambda \mid \ell$, then $H^1_{\mathcal{L}}(\Delta, \widehat{E}) = 0$.

Proof. Let $\Lambda = \Lambda_E(S)$ and $\Gamma = \mathrm{Gal}(\Lambda/\mathbb{Q})$. By inflation-restriction, we have

$$0 \to H^1_{\mathcal{L}}(\Delta, \widehat{E}) \to H^1_{\mathcal{L}}(\Gamma, \widehat{E}) \to \mathrm{Hom}_{\mathbb{F}_\ell[\Delta]}(\mathrm{Gal}(\Lambda/F), \widehat{E}), \tag{4.3.9}$$

since $\mathrm{Gal}(\Lambda/F)$ acts trivially on $\widehat{E}$. Lemma 4.3.1 gives us $\mathbb{F}_\ell[\Delta]$-isomorphisms

$$\mathrm{Hom}_{\mathbb{F}_\ell[\Delta]}(\mathrm{Gal}(\Lambda/F), \widehat{E}) \simeq \mathrm{Hom}_{\mathbb{F}_\ell[\Delta]}(\widehat{X}^r, \widehat{X}^a) \simeq (\mathrm{End}_{\mathbb{F}_\ell[\Delta]} \widehat{X})^{ra},$$

where $r = r_E(S)$. Since $ab = [\mathbb{F} : \mathbb{F}_\ell]$, Lemma 4.3.1(ii) now shows that

$$\dim_{\mathbb{F}} \mathrm{Hom}_{\mathbb{F}_\ell[\Delta]}(\mathrm{Gal}(\Lambda/F), \widehat{E}) = r \dim_{\mathbb{F}} \mathrm{End}_{\mathbb{F}[\Delta]} \widehat{E}.$$

Suppose that $\mathcal{I}_\lambda(F/\mathbb{Q})$ contains an ℓ-Sylow subgroup P of Δ. Any element $[c]$ of $H^1_{\mathcal{L}}(\Delta, \widehat{E})$ restricts to 0 in $H^1(\mathcal{I}_\lambda(F/\mathbb{Q}), \widehat{E})$, and so vanishes on further restriction to $H^1(P, \widehat{E})$. But then $[c] = 0$ because $H^1(\Delta, \widehat{E}) \xrightarrow{\mathrm{res}} H^1(P, \widehat{E})$ is injective; cf. [55, Ch. IX, §2, Thm. 4]. □

We introduce two invariants to estimate the dimension of a non-prosaic nugget. Recall our standard assumption that A is an abelian variety of $\mathfrak{o}$-type and $\mathfrak{l}$ is a prime of $\mathfrak{o}$ above the prime ℓ of good reduction for A.

Definition 4.3.10. Let $\mathfrak{W}(\mathcal{E})$ be the set of nuggets $\mathcal{W}$ that are subquotients of $A[\mathfrak{l}^\infty]$, have the exceptional $\mathcal{E}$ as a constituent and satisfy $N_W = N_E$. Put

$$\delta_A(\mathcal{E}) = \max_{\mathcal{W} \text{ in } \mathfrak{W}(\mathcal{E})} (\dim_{\mathbb{F}} \mathcal{W} - \dim_{\mathbb{F}} \mathcal{E}).$$

For a fixed E in $\mathfrak{S}_{\mathfrak{l}}(A)$, the *deficiency* is given by $\delta_A(E) := \max \delta_A(\mathcal{E})$, where $\mathcal{E}$ has Galois module E. We omit A when it is clear from the context.

We say the exact sequence $0 \to \mathcal{U} \to \mathcal{V} \to \mathcal{W} \to 0$ is *generically split* if the associated exact sequence of Galois modules splits. In view of (4.1.5), for any $\mathcal{W}$ in $\mathfrak{W}(\mathcal{E})$, we have exact sequences

$$0 \to \mathcal{Z} \to \mathcal{V} \to \mathcal{E} \to 0 \quad \text{and} \quad 0 \to \mathcal{V}/\mathcal{Z} \to \mathcal{W}/\mathcal{Z} \to \mathcal{M} \to 0, \tag{4.3.11}$$

with $\mathcal{Z}$ and $\mathcal{M}^D$ constant by Corollary 4.1.10.

Definition 4.3.12. Let $\mathfrak{W}_{spl}(\mathcal{E})$ consist of those $\mathcal{W}$ in $\mathfrak{W}(\mathcal{E})$ for which both exact sequences in (4.3.11) are generically split. Define $\epsilon_{\mathfrak{l}}(\mathcal{E}) = \max \dim_{\mathbb{F}} W - \dim_{\mathbb{F}} E$ over $\mathcal{W}$ in $\mathfrak{W}_{spl}(\mathcal{E})$. For a fixed E in $\mathfrak{S}_{\mathfrak{l}}(A)$, let $\epsilon_{\mathfrak{l}}(E) = \max \epsilon_{\mathfrak{l}}(\mathcal{E})$, taken over $\mathcal{E}$ with E as a Galois module.

When ℓ is odd, generic splitting implies splitting as group schemes, so $\epsilon_{\mathfrak{l}}(\mathcal{E}) = 0$. See §4.4 for bounds on $\epsilon_{\mathfrak{l}}(\mathcal{E})$ when $\ell = 2$. With Notation 4.3.2, we have the following bound on the deficiency $\delta_A(E)$.

Proposition 4.3.13. *Let* $\Gamma_E = \mathrm{Gal}(\Lambda_E(T)/\mathbb{Q})$ *and* $s_E = \dim_{\mathbb{F}} H^1_{\mathcal{L}}(\Gamma_E, \widehat{E})$. *Then* $\delta_A(E) \le s_E + s_{E^*} + \epsilon_{\mathfrak{l}}(E)$.

Proof. For $\mathcal{W}$ in $\mathfrak{W}(\mathcal{E})$, consider the first exact sequence of (4.3.11). Let $L = \mathbb{Q}(V)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. Since inflation $H^1_{\mathcal{L}}(G, \widehat{E}) \to H^1_{\mathcal{L}}(\Gamma_E, \widehat{E})$ is injective, $\dim H^1_{\mathcal{L}}(G, \widehat{E}) \le s_E$. Then, by Corollary 4.3.7, there is a subspace Z' of Z such that $0 \to Z/Z' \to V/Z' \to E \to 0$ is $\mathbb{F}[G]$-split exact and $\dim_{\mathbb{F}} Z' \le s_E$. Write $\mathcal{Z}_1$ (resp. $\mathcal{V}_1$, $\mathcal{W}_1$) for the quotient of $\mathcal{Z}$ (resp. $\mathcal{V}$, $\mathcal{W}$) that corresponds to Z/Z' (resp. V/Z', W/Z'). Then $\mathcal{W}_1$ is a nugget with special filtration $0 \subseteq \mathcal{Z}_1 \subset \mathcal{V}_1 \subseteq \mathcal{W}_1$ and $N_{W_1} = N_E$. Moreover, $0 \to \mathcal{Z}_1 \to \mathcal{V}_1 \to \mathcal{E} \to 0$ is generically split.

Passing to Cartier duals on $0 \to \mathcal{V}_1/\mathcal{Z}_1 \to \mathcal{W}_1/\mathcal{Z}_1 \to \mathcal{M} \to 0$, we find $\mathbb{F}$-module subschemes $\mathcal{M}' \subseteq \mathcal{M}$ and $\mathcal{V}_1 \subseteq \mathcal{W}' \subseteq \mathcal{W}_1$, with $\dim_{\mathbb{F}} M/M' \le s_{E^*}$, such that $0 \to \mathcal{V}_1/\mathcal{Z}_1 \to \mathcal{W}'/\mathcal{Z}_1 \to \mathcal{M}' \to 0$ is generically split. It follows that $\mathcal{W}'$ is in $\mathcal{W}_{spl}(\mathcal{E})$, so $\dim \mathcal{W}' - \dim E \le \epsilon_{\mathfrak{l}}(E)$ by Definition 4.3.12. The claim now ensues from $\dim \mathcal{W} \le \dim \mathcal{W}' + s_E + s_{E^*}$. ☐

Remark 4.3.14.

i) If $\mathcal{V}$ is a "one-sided nugget" with $0 \to \mathcal{Z} \to \mathcal{V} \to \mathcal{E} \to 0$ and $N_V = N_E$, our proof gives $\dim Z \le s_E + \epsilon_{\mathfrak{l}}(E)$.

ii) Since $N_V = N_E$ in the proof above, Lemma 4.3.4 implies the stronger local condition $\mathcal{L}_v = H^1(\mathcal{D}_v, \widehat{M_v})$ at places v over N_E.

Lemma 4.3.15. *Let* $\mathcal{W}$ *be a nugget and* $\mathfrak{f}(W) = \sum_p \mathfrak{f}_p(W)$. *If* W *has an exceptional constituent* E, *then* $\dim_{\mathbb{F}} W - \mathfrak{f}(W) \le \dim_{\mathbb{F}} E - \mathfrak{f}(E) + \delta(E)$. *If* W *is prosaic, then* $\dim_{\mathbb{F}} W \le \mathfrak{f}(W) + 1$, *with equality only if some core has conductor* $p \equiv \pm 1\,(\tilde{\ell})$.

Proof. Suppose the lemma is false and choose a counterexample $\mathcal{W}$ of minimal dimension. We have exact sequences as in (4.1.5).

By definition, $\mathcal{Z}$ is filtered by copies of $\mathcal{Z}_{\mathfrak{l}}$, so $G = \mathrm{Gal}(\mathbb{Q}(Z)/\mathbb{Q})$ is an ℓ-group. Let $\mathfrak{a}_G$ be the augmentation ideal in $\mathbb{F}[G]$ and r the least integer such that $\mathfrak{a}_G^r Z = 0$. If $r \ge 2$, some prime p occurs in the conductor of $\mathfrak{a}_G^{r-2} Z$ by Corollary 4.1.10. Let σ_v generate inertia at a place v above p. There is an element z_2 in $\mathfrak{a}_G^{r-2} Z$ such that $z_1 = (\sigma_v - 1) z_2 \ne 0$. Since z_1 is in $\mathfrak{a}_G^{r-1} Z$, it generates a trivial Galois module. Let $\mathcal{Z}_1$ denote the corresponding $\mathbb{F}$-module subscheme of $\mathcal{Z}$ and let $\mathcal{W}' = \mathcal{W}/\mathcal{Z}_1$. Then $\dim_{\mathbb{F}} \mathcal{W}' = \dim_{\mathbb{F}} \mathcal{W} - 1$ and $\mathfrak{f}(W') \le \mathfrak{f}(W) - 1$, so

$$\dim_{\mathbb{F}} W' - \mathfrak{f}(W') \ge \dim_{\mathbb{F}} W - \mathfrak{f}(W), \tag{4.3.16}$$

and $\mathcal{W}'$ would be a smaller counterexample. Thus Z has trivial action so that $\mathcal{Z} \simeq \mathcal{Z}_{\mathfrak{l}}^a$ is constant of exponent ℓ. Upon passing to Cartier duals, we find similarly that $\mathcal{M}^D$ is constant and $\mathcal{M} \simeq \boldsymbol{\mu}_{\mathfrak{l}}^b$.

Assume E is non-zero and set $\overline{\mathcal{W}} = \mathcal{W}/\mathcal{Z}$. We claim that $N_W = N_{\overline{W}}$. Otherwise, the conductor exponents of W and $\overline{W}$ differ at some place v. Since Galois acts trivially on Z, there is a non-zero element z in $(\sigma_v - 1)(W) \cap Z$. Let $\mathcal{W}'$ be the $\mathbb{F}$-module scheme quotient of $\mathcal{W}$ corresponding to the Galois module $W/\langle z\rangle$. Then (4.3.16) holds for $\mathcal{W}'$ violating minimality of $\mathcal{W}$. A similar argument with the Cartier dual of the sequence $0 \to \mathcal{E} \to \overline{\mathcal{W}} \to \mathcal{M} \to 0$ implies that $N_{\overline{W}} = N_E$. So $N_W = N_E$ and $\mathcal{W}$ is not a counterexample by Definition 4.3.10.

If $\mathcal{W}$ is prosaic, i.e. $E = 0$, we use the argument above, the nugget property and minimality to show that $\dim_{\mathbb{F}} Z = \dim_{\mathbb{F}} M = 1$. Then $\mathcal{W}$ is a core, for which the claim was established in Corollary 4.2.3. ☐

4.4. **Better bounds for $\delta(E)$.** Keep Notation 4.3.2 and (4.3.3), with $\ell = 2$. For each λ over 2 and group scheme $\mathcal{E}$, we have the associated connected, biconnected and étale $\mathcal{D}_\lambda$-modules E^0, E^b and E^{et}. Since λ is unramified in the elementary 2-extension L/F, we have $\mathcal{D}_\lambda(L/F) = \langle h\rangle$, with $h^2 = 1$.

Lemma 4.4.1. *Let $\mathfrak{b}_\lambda$ be the augmentation ideal in $\mathbb{F}[\mathcal{I}_\lambda]$. For $\mathfrak{l}\,|\,2$ in $\mathfrak{o}$, we have*

$$\epsilon_{\mathfrak{l}}(E) \le \min\{\dim_{\mathbb{F}} E^{\mathcal{D}_\lambda}, \dim_{\mathbb{F}} E^{\mathcal{I}_\lambda} - \dim_{\mathbb{F}}(\mathfrak{b}_\lambda E)^{\mathcal{I}_\lambda}\}.$$

If $\mathcal{I}_\lambda$ acts on E via a non-trivial 2-group, then $\epsilon_{\mathfrak{l}}(E) \le \dim_{\mathbb{F}} E - 2$.

Proof. If $\mathcal{W}$ is in $\mathfrak{W}_{spl}(\mathcal{E})$, then the second sequence in (4.3.11) is generically split, so there is a Galois submodule X of W with $E_1 = W/X \simeq E$ and the sequence $0 \to \mathcal{X} \to \mathcal{W} \to \mathcal{E}_1 \to 0$ is exact. Thus $\mathcal{X}$ is a constant group scheme by Corollary 4.1.10. Taking multiplicative subschemes at λ, we find that $\mathcal{W}^m \simeq \mathcal{E}_1^m$.

Similarly, we have $0 \to \mathcal{E}_2 \to \mathcal{W} \to \mathcal{Y} \to 0$, with $\mathcal{Y}^D$ constant and $E_2 \simeq E$. Taking multiplicative subschemes at λ gives

$$0 \to \mathcal{E}_2^m \to \mathcal{W}^m \to \mathcal{Y} \to 0. \tag{4.4.2}$$

Hence $\dim W - \dim E = \dim Y = \dim W^m - \dim E_2^m = \dim E_1^m - \dim E_2^m$.

We have $\dim E_1^m \le \dim E^{\mathcal{I}_\lambda}$ and $\mathfrak{b}_\lambda E \subseteq E_2^0$ because $\mathcal{I}_\lambda$ acts trivially on E_1^m and E_2^{et}. Moreover, by [41], the tame ramification group acts non-trivially on the simple constituents of E_2^b over the strict Henselization, so $(E_2^0)^{\mathcal{I}_\lambda} \subseteq E_2^m$. The inequality $\dim E_2^m \ge \dim(\mathfrak{b}_\lambda E)^{\mathcal{I}_\lambda}$ gives $\epsilon_{\mathfrak{l}}(E) \le \dim E^{\mathcal{I}_\lambda} - \dim(\mathfrak{b}_\lambda E)^{\mathcal{I}_\lambda}$. In particular, when $\mathcal{I}_\lambda$ acts on E through a non-trivial 2-group, we have $\epsilon_{\mathfrak{l}}(E) \le \dim E - 2$.

The isomorphism $\mathcal{E}_1^m \xrightarrow{\sim} \mathcal{W}^m$ and the surjection $\mathcal{W}^m \twoheadrightarrow \mathcal{Y}$ in (4.4.2) yield a surjection of $\mathcal{D}_\lambda$-modules $\mathcal{E}_1^m \twoheadrightarrow Y$. Since Y is a trivial Galois module, this map induces a surjection $E_1^m/\mathfrak{a}_\lambda E_1^m \twoheadrightarrow Y$, where $\mathfrak{a}_\lambda$ is the augmentation ideal in $\mathbb{F}[\mathcal{D}_\lambda]$. But $\mathcal{I}_\lambda$ acts trivially on E_1^m, and so $\mathcal{D}_\lambda$ acts via the group generated by a Frobenius Φ. Hence

$$\begin{aligned} \dim_{\mathbb{F}} W - \dim_{\mathbb{F}} E = \dim_{\mathbb{F}} Y &\le \dim_{\mathbb{F}} E_1^m/\mathfrak{a}_\lambda E_1^m \\ &= \dim_{\mathbb{F}} (E_1^m)^{\langle\Phi\rangle} = \dim_{\mathbb{F}} (E_1^m)^{\mathcal{D}_\lambda} \le \dim_{\mathbb{F}} E^{\mathcal{D}_\lambda}. \end{aligned}$$ ☐

Corollary 4.4.3. *If $\Delta \subseteq \mathrm{SL}_{\mathbb{F}}(E)$, then* $\epsilon_{\mathfrak{l}}(E) \le \begin{cases} \dim_{\mathbb{F}} E & \text{if } \mathcal{D}_\lambda = 1, \\ \dim_{\mathbb{F}} E - 1 & \text{if } |\mathcal{D}_\lambda| = 2, \mathcal{I}_\lambda = 1, \\ \dim_{\mathbb{F}} E - 2 & \text{otherwise.} \end{cases}$

Proof. If the claim is false, the lemma implies that $\dim_{\mathbb{F}} E^{\mathcal{D}_\lambda} = \dim_{\mathbb{F}} E - 1$. Then $\mathcal{D}_\lambda$ is an elementary 2-group, since $\Delta \subseteq \mathrm{SL}_{\mathbb{F}}(E)$. By the lemma, we now find that $\mathcal{I}_\lambda = 1$. Thus $\mathcal{D}_\lambda$ is cyclic and so has order 2. □

Definition 4.4.4. We say $\mathcal{E}$ is $(S\backslash T)$-*transparent* if $\mathrm{Ext}^1_{\mathbb{Z}_S}(\mathcal{E}, \mathcal{Z}_{\mathfrak{l}}) = 0$, where $S \supseteq T$ and $T = T_E$ is the set of bad primes of E. When $S = T$, we simply say transparent.

Lemma 4.4.5. *Let E be a self-dual exceptional $\mathbb{F}[G_{\mathbb{Q}}]$-module and $S \supseteq T_E$. If $\dim_{\mathbb{F}} E = 2$, $H^1_{\mathcal{L}}(\Delta, E) = 0$ and $r_E(S) = 0$, then*

i) *$\delta(E) = 0$ and E is (S/T_E)-transparent if either $|\mathcal{D}_\lambda(F/\mathbb{Q})| = |\mathcal{I}_\lambda(F/\mathbb{Q})| = 2$ or $|\mathcal{D}_\lambda(F/\mathbb{Q})| \geq 3$.*
ii) *$\delta(E) \leq 1$ if $|\mathcal{D}_\lambda(F/\mathbb{Q})| = 2$ and $\mathcal{I}_\lambda(F/\mathbb{Q}) = 1$.*
iii) *$\delta(E) \leq 2$ in all other cases.*

Proof. Since E is self-dual, it affords a representation whose determinant is the mod 2 cyclotomic character [45], and so Δ is contained in $\mathrm{SL}_2(\mathbb{F})$. Now use Lemma 4.3.8, Corollary 4.4.3 and Proposition 4.3.13. □

The restriction $\tilde{c} = \mathrm{res}[c] : \mathrm{Gal}(L/F) \to \mathrm{Hom}(E, Z)$ is an $\mathbb{F}[\Delta]$-homomorphism and $\tilde{c}_h : E \to Z$ is $\mathbb{F}$-linear; cf. Remark 3.5.4.

Lemma 4.4.6. *Let $\mathfrak{a}_\lambda$ be the augmentation ideal in $\mathbb{F}[\mathcal{D}_\lambda(F/\mathbb{Q})]$. Then $\tilde{c}_h$ vanishes on $E^0 + \mathfrak{a}_\lambda E$ and $\dim_{\mathbb{F}} \tilde{c}_h(E) \leq \dim_{\mathbb{F}} (E^{et})^{\mathcal{D}_\lambda(F/\mathbb{Q})}$.*

Proof. Since $\tilde{c}_h(E^0) = 0$ by Lemma 4.3.5, $\tilde{c}_h$ factors through E^{et}. Also, $\mathcal{I}_\lambda$ acts trivially on E^{et}, so $\mathfrak{a}_\lambda E^{et} = (\Phi - 1)(E^{et})$, for any Frobenius Φ in $\mathcal{D}_\lambda(F/\mathbb{Q})$. We know that Φ acts trivially on Z and h is a power of Φ. It follows that

$$\tilde{c}_h(\Phi\bar{e}) = \Phi^{-1}(\tilde{c}_h(\Phi\bar{e})) = (\Phi^{-1}(\tilde{c}_h))(\bar{e}) = \tilde{c}_{\Phi^{-1}(h)}(\bar{e}) = \tilde{c}_h(\bar{e})$$

for all $\bar{e}$ in E^{et}. Hence $\tilde{c}_h$ vanishes on $\mathfrak{a}_\lambda E^{et}$ and so it factors through $E^{et}/\mathfrak{a}_\lambda E^{et}$. This last space has the same dimension as $(E^{et})^{\Phi}$. □

Lemma 4.4.7. *If the residue degree $f_\lambda(F/\mathbb{Q})$ is even and $\mathcal{D}_\lambda(F/\mathbb{Q})$ acts on E^{et} through a quotient of odd order, then the primes over 2 split completely in L/F.*

Proof. If $f_\lambda(F/\mathbb{Q})$ is even, then h is a square in $\mathcal{D}_\lambda(L/\mathbb{Q})$, say $h = g^2$, with g chosen to have order a power of 2. Hence g acts trivially on E^{et} and $(1+g)(E) \subseteq E^0$. By Lemma 4.3.5, we may arrange for the cocycle $c\colon G \to \mathrm{Hom}(E, Z)$ to satisfy $c_g(E^0) = 0$. Then, by the cocycle identity, we have

$$\tilde{c}_h(e) = c_{g^2}(e) = ((1+g)c_g)(e) = c_g((1+g^{-1})(e)) \in c_g(E^0) = 0$$

for all e in E. But $\tilde{c}$ is injective, so $h = 1$. □

We now impose the following hypotheses, with notation from §4.3.

D **1**. E is two-dimensional over $\mathbb{F}$, irreducible and self-dual as an $\mathbb{F}[G_{\mathbb{Q}}]$-module.
2. The generalized Selmer group $H^1_{\mathcal{L}}(\Delta, \widehat{E})$ is trivial.
3. There is an $\mathbb{F}_2[\Delta]$-isomorphism $\mathrm{Gal}(\Lambda/F) \simeq \widehat{X}$, that is, $r_E = 1$.
4. The primes over 2 do not split completely in Λ/F, so $\mathcal{E}$ is not biconnected.

Remark 4.4.8. Under **D2**, the cohomological restriction map $[c] \mapsto \tilde{c}$ is injective, so in (4.3.3), V splits if and only if $\tilde{c} = 0$. By **D3**, $L = \mathbb{Q}(V)$ is equal to F or Λ. If $L = F$, then $\tilde{c} = 0$ and (4.3.3) splits, while if $L = \Lambda$, $\tilde{c}$ induces the isomorphism in **D3** and $\mathcal{D}_\lambda(L/F) = \langle h \rangle$ has order 2 by **D4**. By irreducibility of X, h generates $\mathrm{Gal}(L/F)$ as an $\mathbb{F}_2[\Delta]$-module. Let $\mathcal{Z}'$ be the $\mathbb{F}$-module subscheme of $\mathcal{Z}$ corresponding to $Z' = \sum\{\, c_\gamma(E) \,|\, \gamma \in \mathrm{Gal}(L/F) \,\} = \tilde{c}_h(E)$. Remark 3.5.4 shows that the following sequence is generically split:

$$0 \to \mathcal{Z}/\mathcal{Z}' \to \mathcal{V}/\mathcal{Z}' \to \mathcal{E} \to 0. \tag{4.4.9}$$

Lemma 4.4.10. *Assume* **D** *and residue degree* $f_\lambda(F/\mathbb{Q}) = 2$. *Then* $\delta(\mathcal{E}) \le 1$, *unless there is a nugget* $\mathcal{W}$ *with* $\mathbf{gr}\,\mathcal{W} = [\mathcal{Z}_\mathfrak{l}\,\mathcal{E}\boldsymbol{\mu}_\mathfrak{l}]$ *and* $\dim \mathcal{E}^{et} \ne 1$, *in which case,* $\delta(E) \le 2$. *The latter can only happen if* $\dim_\mathbb{F} A[\mathfrak{l}] \ge 6$.

Proof. Let $\mathcal{V}$, $\mathcal{W}$ be nuggets as in (4.3.11) and $L = \mathbb{Q}(V)$. If $\dim \mathcal{E}^{et} \le 1$, then $\mathcal{D}_\lambda$ acts on E^{et} via a subgroup of $\mathbb{F}^\times$ and so the primes over 2 split in L/F by Lemma 4.4.7. By **D4**, $L = F$ and (4.3.3) splits. By Lemma 4.4.1, we have

$$\dim Z = \dim V - \dim E \le \epsilon_2(E) \le \dim E^{\mathcal{D}_\lambda} \le 1.$$

If $\dim \mathcal{E}^{et} = 2$, Lemma 4.4.6 shows $\dim Z' \le 1$ in the generically split sequence (4.4.9), which must split as an exact sequence of schemes by Lemma 3.1.4. Since $\mathcal{V}$ is a nugget, we have $Z/Z' = 0$, so $\dim_\mathbb{F} \mathcal{Z} \le 1$ in all cases. By Cartier duality, $\dim_\mathbb{F} \mathcal{M} \le 1$. Hence $\delta(E) \le 2$, with equality only if $\mathbf{gr}\,\mathcal{W} = [\mathcal{Z}_\mathfrak{l}\,\mathcal{E}\boldsymbol{\mu}_\mathfrak{l}]$ for some nugget $\mathcal{W}$.

When $\dim \mathcal{E}^{et} = \dim \mathcal{E}^0 = 1$, we have seen that (4.3.3) is generically split and so is $0 \to \mathcal{V} \to \mathcal{W} \to \mathcal{M} \to 0$, by a dual argument. We have $\delta(\mathcal{E}) \le 1$, since Lemma 4.4.1 gives $\dim \mathcal{W} - \dim \mathcal{E} \le \epsilon_2(E) \le \dim E^{\mathcal{D}_\lambda} \le 1$.

If $\dim A[\mathfrak{l}] = 4$, $\dim \mathcal{E}^{et} = \dim \mathcal{E}^0 = 1$ since $\mathcal{W} = A[\mathfrak{l}]$ has as many $\boldsymbol{\mu}_\mathfrak{l}$ as $\mathcal{Z}_\mathfrak{l}$. ☐

For the final result of this section, we need some facts about representations that respect a flag of $\mathbb{F}_2[G_\mathbb{Q}]$-modules $0 \subset Z \subset V \subset W$, with $\mathbf{gr}\,W = [\mathbb{F}_2 E\,\mathbb{F}_2]$. We assume $\dim_{\mathbb{F}_2} E = 2$ and $\Delta = \mathrm{Gal}(\mathbb{Q}(E)/\mathbb{Q}) \simeq \mathrm{SL}_2(\mathbb{F}_2)$.

For $x = (a,b)^t$ a column vector in E, consider the Δ-invariant quadratic form $Q(x) = a^2 + ab + b^2$ and define $x^\dagger = (b,a)$. Then $(x,y) \mapsto x^\dagger y = \det(x,y)$ is the symplectic form on E associated to Q by $Q(x+y) = Q(x) + Q(y) + x^\dagger y$. Setting

$$\iota(x,\delta,c) = \left[\begin{smallmatrix} 1 & x^\dagger\delta & c \\ 0 & \delta & x \\ 0 & 0 & 1 \end{smallmatrix}\right],$$

we have $\iota(x,\delta_1,c_1)\,\iota(y,\delta_2,c_2) = \iota(x+\delta_1 y,\ \delta_1\delta_2,\ c_1 + x^\dagger\delta_1 y + c_2)$.

Let $\mathcal{P} = \{\iota(x,\delta,c) \,|\, \delta \in \Delta,\ c \in \mathbb{F}_2\}$ and $\mathcal{P}_1 = \{\,\iota(x,\delta,Q(x)) \,|\, x \in E,\ \delta \in \Delta\}$. Then $\mathcal{P} \simeq \mathcal{P}_1 \times \langle \xi \rangle$, where $\xi = \iota(0, I_2, 1)$ is the central involution in $\mathcal{P}$. The normal subgroup $H = \{\iota(x, I_2, Q(x)) \,|\, x \in E\}$ of $\mathcal{P}_1$ is Δ-isomorphic to E under the action of $\tilde{\delta} = \iota(0,\delta,0)$ by conjugation. The relation $(\delta x)^\dagger = x\delta^{-1}$, implied by the Δ-invariance of Q, gives $\tilde{\delta}\,\iota(x,1,Q(x))\,\tilde{\delta}^{-1} = \iota(\delta x, 1, Q(\delta x))$.

Let $\tilde{\Delta} = \iota(0,\Delta,0)$. Then $\mathcal{P}_1 = H\tilde{\Delta} \simeq \mathcal{S}_4$ is a Coxeter group, generated by

$$\tau_1 = \iota\left(0, \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right], 0\right), \quad \tau_2 = \iota\left(0, \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right], 0\right), \quad \tau_3 = \iota\left(\left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right], 1\right),$$

three involutions whose pairwise products have order 3.

Lemma 4.4.11. *If* E *satisfies* **D**, *with* $\mathbb{F} = \mathbb{F}_2$ *and* $|\mathcal{I}_\lambda(F/\mathbb{Q})| = 2$, *then* $\delta(E) \le 1$.

Proof. Note that **D1** and **D2** follow from the other two. In fact, $r_E = 1$ implies $s_E \le 1$ by Lemma 4.3.8. Let $\mathcal{W}$ be a nugget with $N_W = N_E$ as in Definition 4.3.10. Lemma 4.4.1 implies that $\epsilon_2(E) = 0$. It follows from Remark 4.3.14 that the étale subscheme Z in (4.1.5) satisfies $\dim Z \le 1$, with equality only if $\mathbb{Q}(V) = \Lambda$. By a dual argument, we have $\dim M \le 1$, with equality only if $\mathbb{Q}(W/Z) = \Lambda$.

Assume $\dim Z = \dim M = 1$. We build a basis for W reflecting the local structure of $\mathcal{W}$ at λ. Because $|\mathcal{I}_\lambda(F/\mathbb{Q})| = 2$, we have $\dim E^0 = 1$, and so $\dim V^0 = 1$. Let b_1 generate Z and b_2 generate V^0. Extend to bases b_1, b_2, b_3 for V and b_2, b_4 for W^0. Write ρ_W for the matrix representation of $\Gamma = \mathrm{Gal}(\mathbb{Q}(W)/\mathbb{Q})$ afforded by the basis b_1, b_2, b_3, b_4. The images of the induced representations ρ_V on V and $\rho_{W/Z}$ on W/Z are both isomorphic to $G = \mathrm{Gal}(\Lambda/\mathbb{Q})$. Also, $\rho_V(g_1) = \rho_V(g_2)$ if and only if $\rho_{W/Z}(g_1) = \rho_{W/Z}(g_2)$.

The inertia group $\mathcal{I}_\lambda(\mathbb{Q}(W)/\mathbb{Q}) = \langle \sigma_\lambda \rangle$ is cyclic of order 2. Both W^0 and W^{et} are unramified $\mathcal{D}_\lambda$-modules. The Frobenius $\Phi = \Phi_\lambda$ in $\mathrm{Gal}(\Lambda/F)$ is non-trivial on Λ and we have

$$\rho_W(\Phi) = \iota(\left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], I_2, 0) \quad \text{and} \quad \rho_W(\sigma_\lambda) = \tau_1.$$

For each place v over a prime p dividing $N_W = N_E$, let σ_v generate $\mathcal{I}_v(\mathbb{Q}(W)/\mathbb{Q})$. Since the conductor exponent $\mathfrak{f}_p(E) = 1$, $\rho_W(\sigma_v)$ is a transvection in $\mathrm{SL}_4(\mathbb{F}_2)$ and $\rho_V(\sigma_v)$ becomes a transposition under the isomorphism Image $\rho_V \simeq \mathcal{S}_4$. By conjugation, we may produce any transvection in the upper left 3×3 corner by a suitable choice of v and so assume that

$$\rho_W(\sigma_v) = \left[\begin{smallmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&1&1&s_v\\ 0&0&0&1 \end{smallmatrix}\right].$$

Over each bad q, there is a w with $\rho_W(\sigma_w)$ of the same shape for some s_w. Since $\rho_V(\sigma_v) = \rho_V(\sigma_w)$, we have $\rho_{W/Z}(\sigma_v) = \rho_{W/Z}(\sigma_w)$, and so $s_v = s$ is independent of p. Replacing b_4 by $b_4' = b_4 + sb_2$ preserves $\rho_W(\Phi)$ and $\rho_W(\sigma_\lambda)$, but makes $\rho_W(\sigma_v) = \tau_2$. Thus the group $\tilde{\Delta}$, generated by τ_1 and τ_2, is contained in Γ.

We claim that $\Gamma \subseteq \mathcal{P}_1$. But Γ is generated by its inertia groups, and so by Γ-conjugates of $\tilde{\Delta}$. Since $\tilde{\Delta} \subseteq \mathcal{P}_1$, it suffices to show $\Gamma \subseteq \mathcal{P}$. Let g in Γ fix F, say

$$\rho_W(g) = \left[\begin{smallmatrix} 1&x^t&c\\ 0&I_2&y\\ 0&0&1 \end{smallmatrix}\right],$$

with c in $\mathbb{F}_2$, and x^t and y in E. Choose δ in Δ so that $\delta(1,0)^t = y$ and let $h = \tilde{\delta}\Phi\tilde{\delta}^{-1}$. Then $\rho_{W/Z}(g) = \rho_{W/Z}(h)$ and so $\rho_V(g) = \rho_V(h)$. Thus, $\rho_W(g)$ and $\rho_W(h)$ agree up to an element of $\langle \xi \rangle$. Since $\rho_W(h) = \iota(y, I_2, 0)$ is in $\mathcal{P}$, we have $\Gamma \subseteq \mathcal{P}$. But $\rho_W(\Phi)$ is not in $\mathcal{P}_1$, a contradiction. □

5. General bound

Let A be a semistable abelian variety of $\mathfrak{o}$-type. Our aim here is to bound $\epsilon_0(A[\mathfrak{l}])$, the number of one-dimensional constituents in a composition series for $A[\mathfrak{l}]$ as an $\mathbb{F}[G_\mathbb{Q}]$-module.

Definition 5.1. The *semisimple conductor* of $A[\mathfrak{l}]$ is $N_A^{ss}(\mathfrak{l}) = \prod N_E$, where E runs over the multiset $\mathfrak{S}_\mathfrak{l}(A)$. The *prosaic conductor* is $N_A^u(\mathfrak{l}) = N/N_A^{ss}(\mathfrak{l})$, where $N = N_A^0$ is the reduced conductor of A. When $\mathfrak{l}$ is clear from the context, it may be omitted. Write Π_A^u for the set of prime factors of N_A^u.

The prosaic conductor depends only on $\mathfrak{l}$ and the $\mathfrak{o}$-isogeny class of A, since this is true of $N_A^{ss}(\mathfrak{l})$ by Proposition 3.2.10, but it is not the conductor of a Galois module naturally associated to A.

Lemma 5.2. *Let A have good reduction at a prime $q \neq \ell$ and let s_0 be the greatest integer in $2\dim A \cdot \log(1+\sqrt{q})/\log|\mathbb{F}_\mathfrak{l}|$. Let $\mathcal{Z}$ (resp. $\mathcal{M}$) be an $\mathfrak{o}$-module scheme* *subquotient of* $A[\mathfrak{l}^n]$ *filtered by copies of* $\mathcal{Z}_\mathfrak{l}$ *(resp.* $\boldsymbol{\mu}_\mathfrak{l}$*). Then*

$$\operatorname{length}_\mathfrak{o} Z \le \mathfrak{f}(Z) + s_0 \qquad \textit{and} \qquad \operatorname{length}_\mathfrak{o} M \le \mathfrak{f}(M) + s_0.$$

If $\operatorname{End} A = \mathfrak{o}$, *then* $\max\{\operatorname{length} Z, \operatorname{length} M\} \le s_1$, *where* s_1 *is the number of isomorphism classes in the* $\mathbb{Q}$*-isogeny class of* A.

Proof. By duality, we only prove the assertions about Z. Replacing A by a quotient, suppose $\mathcal{Z} \subseteq A[\mathfrak{l}^n]$. The result holds when Z has trivial Galois action because $A(\mathbb{Q})[\ell^\infty]$ injects into $\tilde{A}(\mathbb{F}_q)$ by specialization and s_0 is the Weil bound for the $\mathfrak{o}$-length of the $\mathfrak{l}$-primary component of the reduction $\tilde{A}(\mathbb{F}_q)$ of A modulo q.

Parallel to the proof of Lemma 4.3.15, let $\mathcal{Z}$ be a counterexample of minimal length, G the ℓ-group $\operatorname{Gal}(\mathbb{Q}(Z)/\mathbb{Q})$, I_G the augmentation ideal of $\mathfrak{o}_\mathfrak{l}[G]$ and $r \ge 2$ the least integer such that $I_G^r Z = 0$. There is a prime $p = p_v$ ramified in $I_G^{r-2} Z$ and an element z_2 in $I_G^{r-2} Z$, such that $z_1 = (\sigma_v - 1) z_2 \ne 0$ is killed by $\mathfrak{l}$. Let $\mathcal{Z}_1 \subseteq \mathcal{Z}$ correspond to the trivial $\mathfrak{o}_\mathfrak{l}[G]$-module $Z_1 = \langle z_1 \rangle$ and let $\overline{\mathcal{Z}} = \mathcal{Z}/\mathcal{Z}_1$. Then $\operatorname{length} \overline{Z} - \mathfrak{f}(\overline{Z}) \ge \operatorname{length} Z - \mathfrak{f}(Z)$ and $\overline{\mathcal{Z}}$ is a smaller counterexample.

The stronger bound uses Faltings's theorem. Let $\{\mathcal{Z}_i\}$ be an increasing filtration of subschemes of $\mathcal{Z}$. Then the abelian varieties $A_i = A/\mathcal{Z}_i$ are non-isomorphic, since the kernel of an isomorphism $A_i \xrightarrow{\sim} A_j$ would equal $A_i[\mathfrak{l}^r]$ and so is not étale. □

Theorem 5.3. *Let* $A_{/\mathbb{Q}}$ *be an* $\mathfrak{o}$*-type semistable abelian variety, good at* ℓ*, and* $\mathfrak{l} \mid \ell$ *in* $\mathfrak{o}$*. Then*

$$\epsilon_0(A[\mathfrak{l}]) \le \Omega(N_A^u(\mathfrak{l})) + \Omega_\ell(N_A^u(\mathfrak{l})) + \sum_{E \textit{ in } \mathfrak{S}_\mathfrak{l}(A)} \delta_A(E).$$

Proof. Put $\mathfrak{S} = \mathfrak{S}_\mathfrak{l}(A)$ and $\mathbb{F} = \mathbb{F}_\mathfrak{l}$. Let $\mathcal{F}$ be a nugget filtration of $A[\mathfrak{l}^n]$, with $\mathbf{gr}\,\mathcal{F} = [\mathcal{M}, \mathcal{V}_1, \dots, \mathcal{V}_m, \mathcal{Z}]$, and each $\mathcal{V}_i$ a nugget. Set $\eta_i = 1$ if $\mathcal{V}_i$ is a prosaic nugget with a core of prime conductor $p \equiv \pm 1 \mod \tilde{\ell}$, and $\eta_i = 0$ otherwise. If $\mathcal{V}_i$ is not prosaic, V_i has a unique exceptional $\mathbb{F}[G_\mathbb{Q}]$-module E_i as its constituent. Take the $\mathfrak{o}$-length of $A[\mathfrak{l}^n]$ and apply Lemmas 4.3.15 and 5.2 to obtain

$$\begin{aligned}
n \dim_\mathbb{F} A[\mathfrak{l}] &= \operatorname{length}_\mathfrak{o} Z + \operatorname{length}_\mathfrak{o} M + \sum_i \dim_\mathbb{F} V_i \\
&\le 2s_0 + \mathfrak{f}(Z) + \mathfrak{f}(M) + \sum_{V_i \text{ prosaic}} (\mathfrak{f}(V_i) + \eta_i) \\
&\qquad + \sum_{V_i \text{ not prosaic}} (\mathfrak{f}(V_i) + \dim_\mathbb{F} E_i - \mathfrak{f}(E_i) + \delta_A(E_i)) \\
&\le 2s_0 + \mathfrak{f}(Z) + \mathfrak{f}(M) + \sum_i \mathfrak{f}(V_i) + \sum_{V_i \text{ prosaic}} \eta_i \\
&\qquad + n \left[\sum_{E \text{ in } \mathfrak{S}} (\dim_\mathbb{F} E - \mathfrak{f}(E) + \delta_A(E)) \right],
\end{aligned}$$

since any E appears n times as often in $A[\mathfrak{l}^n]$ as in $A[\mathfrak{l}]$. By Lemma 3.2.5(ii) and the bound (3.2.8) on the conductor of $A[\mathfrak{l}^n]$, we have

$$\begin{aligned} \mathfrak{f}(Z)+\mathfrak{f}(M)+\sum_i \mathfrak{f}(V_i) &\leq \mathfrak{f}(A[\mathfrak{l}^n]) \leq n\,\Omega(N_A^0) \\ &\leq n\left[\Omega(N_A^u(\mathfrak{l}))+\sum_{E\in\mathfrak{S}}\mathfrak{f}(E)\right]. \end{aligned}$$

Clearly $\epsilon_0(A[\mathfrak{l}])=\dim_{\mathbb{F}} A[\mathfrak{l}]-\sum_{E\in\mathfrak{S}}\dim_{\mathbb{F}} E$ and $\sum_{\text{prosaic}}\eta_i \leq n\,\Omega_\ell(N_A^u(\mathfrak{l}))$. Substitute, divide by n and let n go to infinity to finish. ☐

Corollary 5.4. *If N_A is the conductor of A and $\mathbb{Q}(A[\mathfrak{l}])$ is an ℓ-extension of $\mathbb{Q}(\boldsymbol{\mu}_\ell)$, then $\mathfrak{S}_\mathfrak{l}(A)$ is empty and* $2\dim A \leq \Omega(N_A)+\Omega_\ell(N_A)$.

Corollary 5.5. *Assume that A is good outside S and each exceptional constituent E in $\mathfrak{S}_\mathfrak{l}(A)$ is $(S\backslash T_E)$-transparent, as in* Definition 4.4.4.

i) *We have $\epsilon_0(A[\mathfrak{l}])=0$ under one of the following:*
   a. *$\ell\geq 5$ and no prime dividing $N_A^u(\mathfrak{l})$ satisfies $p\equiv\pm1\,(\ell)$;*
   b. *$\ell=3$ and $N_A^u(\mathfrak{l})=q^a$ with $q\not\equiv\pm1\,(9)$;*
   c. *$\ell=2$ and $N_A^u(\mathfrak{l})=q^a$ with $q^*\equiv5\,(8)$.*

ii) *We have $\epsilon_0(A[\mathfrak{l}])\leq 2a$ under one of the following:*
   a. *$\ell=3$ and $N_A^u(\mathfrak{l})=p^aq^b$ with either $q \bmod 9$ in $\{2,5\}$, or with $q \bmod 9$ in $\{4,7\}$ and $p^{\frac{q-1}{3}}\not\equiv 1\,(q)$;*
   b. *$\ell=2$ and $N_A^u(\mathfrak{l})=p^aq^b$ with $p^*\equiv1\,(8)$, $q^*\equiv5\,(8)$ and some Hilbert symbol $(p^*,q^*)_\pi=-1$.*

Proof. By $(S\backslash T)$-transparency, each non-prosaic nugget is just an exceptional constituent. Then, as in the proof of the last theorem,

$$n\,\epsilon_0(A[\mathfrak{l}])\leq 2s_0+\sum_{V_i\text{ prosaic}}\dim V_i.$$

By Corollary 4.2.3, there is no prosaic nugget in (i). In (ii), all are two-dimensional, of conductor p by Lemma 4.2.6, so there are at most na prosaic nuggets. ☐

6. Mirages

6.1. **Introducing mirages.** Let $A_{/\mathbb{Q}}$ be a semistable abelian variety of $\mathfrak{o}$-type with good reduction at ℓ. Let $\mathfrak{l}$ be a prime of $\mathfrak{o}$ above ℓ and $\mathbb{F}=\mathbb{F}_\mathfrak{l}$. Recall that B is an object of $\mathfrak{I}_A^\mathfrak{l}$ if there is an $\mathfrak{o}$-isogeny from A to B with an $\mathfrak{l}$-primary kernel. In this section, all isogenies are $\mathfrak{o}$-linear, with $\mathfrak{l}$-primary kernels.

Definition 6.1.1. A *mirage* $\mathfrak{C}$ associates to each B in $\mathfrak{I}_A^\mathfrak{l}$ a set of $\mathbb{F}$-module subschemes of $B[\mathfrak{l}]$ such that $\varphi(\mathfrak{C}(B_1))\subseteq\mathfrak{C}(B_2)$ for each isogeny $\varphi\colon B_1\to B_2$. Call B *obstructed* if $\mathfrak{C}(B)=\{0\}$ and $\mathfrak{C}$ *unobstructed* if no B in $\mathfrak{I}_A^\mathfrak{l}$ is obstructed.

Proposition 6.1.2. *If $\mathfrak{C}$ is unobstructed on $\mathfrak{I}_A^\mathfrak{l}$, then there is a B in $\mathfrak{I}_A^\mathfrak{l}$ and a filtration $0\subset\mathcal{W}_1\subset\cdots\subset\mathcal{W}_s=B[\mathfrak{l}^r]$, with $\mathcal{W}_{i+1}/\mathcal{W}_i$ in $\mathfrak{C}(B/\mathcal{W}_i)$ for all i.*

Proof. Set $A_0=A$ and construct inductively the abelian variety $A_n=A_{n-1}/\kappa_n$ with κ_n chosen in $\mathfrak{C}(A_{n-1})$. Write $\mathcal{K}_n$ for the kernel of the induced isogeny from A to A_n. By Faltings [13], we may find an isomorphic pair $B=A_m$ and $B'=A_n$ with $m<n$. This produces an endomorphism α of B, whose kernel $\mathcal{W}=\mathcal{K}_n/\mathcal{K}_m$

admits a filtration as above. Since α is in $\operatorname{End} B = \mathfrak{o}$ and $\mathcal{W}$ is killed by a power of $\mathfrak{l}$, we have $\mathcal{W} = B[\alpha] = B[\mathfrak{l}^r]$, with $\alpha\mathfrak{o} = \mathfrak{l}^r$. □

Here is a particularly simple illustration of the use of mirages.

Corollary 6.1.3. *If $E, E_1, ..., E_r$ are the distinct irreducible Galois constituents of $A[\mathfrak{l}]$, then a subquotient of $A[\mathfrak{l}^\infty]$ is a non-split extension of E_i by E for some $i \geq 1$.*

Proof. For any B in $\mathfrak{I}_A^{\mathfrak{l}}$, consider the mirage $\mathfrak{C}(B)$ consisting of the $\mathbb{F}$-module subschemes of $B[\mathfrak{l}]$ whose Galois submodules have *no* constituent isomorphic to E. Thanks to Propositions 3.2.10 and 6.1.2, we may assume that A is obstructed. Choose a subscheme $\mathcal{V} \subseteq A[\mathfrak{l}]$ with $\mathbf{gr}\, V = [E \ldots E E_i]$ having the smallest number of E's. If the quotient W corresponding to the last two terms were split, $\mathcal{W}$ would contain an $\mathbb{F}$-submodule scheme $\mathcal{E}'$ with $E' \simeq E_i$. This violates the minimality and thereby the obstruction. □

Let C be a covariant functor from $\mathfrak{I}_B^{\mathfrak{l}}$ to the category of $\mathfrak{o}_{\mathfrak{l}}$-modules, such that $C(A)$ is a pure $\mathfrak{o}_{\mathfrak{l}}$-submodule of $\mathbb{T}_{\mathfrak{l}}(A)$ for all A in $\mathfrak{I}_B^{\mathfrak{l}}$. Let $\varphi_* = C(\varphi)$ be the map induced by an $\mathfrak{o}$-isogeny $\varphi : A \to A'$. Denote the image of $C(A)$ in $A[\mathfrak{l}^n]$ by

$$C^{(n)}(A) = (C(A) + \mathfrak{l}^n \mathbb{T}_{\mathfrak{l}}(A))/\mathfrak{l}^n \mathbb{T}_{\mathfrak{l}}(A) \tag{6.1.4}$$

and set $\overline{C}(A) = C^{(1)}(A) \subseteq A[\mathfrak{l}]$. We create a mirage by letting $\mathfrak{C}(A)$ be the set of all simple $\mathbb{F}$-module subschemes of $A[\mathfrak{l}]$ whose Galois module is contained in $\overline{C}(A)$. We say that C is obstructed if $\mathfrak{C}$ is obstructed.

Lemma 6.1.5. *If C is unobstructed, then $C(A) = \mathbb{T}_{\mathfrak{l}}(A)$ for all $A \in \mathfrak{I}_B^{\mathfrak{l}}$.*

Proof. We first show that if $A_1 \xrightarrow{\varphi} A_2 \xrightarrow{\psi} A_3$ is a chain of $\mathfrak{o}$-isogenies such that $\ker \varphi_* \subseteq C^{(n_1)}(A_1)$ and $\ker \psi_* \subseteq C^{(n_2)}(A_2)$, then $\ker(\psi\varphi)_* \subseteq C^{(n_1+n_2)}(A_1)$. The kernel of φ is annihilated by $\mathfrak{l}^k$ for some $k \leq n_1$. There is a quasi-inverse $\mathfrak{o}$-isogeny $\varphi' : A_2 \to A_1$, such that the induced maps $(\varphi\varphi')_*$ and $(\varphi'\varphi)_*$ are multiplication by $\mathfrak{l}^k$ on $\mathbb{T}_{\mathfrak{l}}(A_2)$ and on $\mathbb{T}_{\mathfrak{l}}(A_1)$, respectively. Hence,

$$C^{(n_2)}(A_2) = \mathfrak{l}^k C^{(n_2+k)}(A_2) = \varphi_* \varphi'_*(C^{(n_2+k)}(A_2)) \subseteq \varphi_*(C^{(n_2+k)}(A_1)).$$

If x lies in $\ker(\psi\varphi)_*$, then $\varphi_*(x)$ is in $\ker \psi_* \subseteq C^{(n_2)}(A_2)$, so we can find y in $C^{(n_2+k)}(A_1)$ satisfying $\varphi_*(x) = \varphi_*(y)$. Hence x is in $y + \ker \varphi_* \subseteq C^{(n)}(A_1)$ for all $n \geq \max\{n_2 + k, n_1\}$.

Next, as in the proof of Proposition 6.1.2, we may find an endomorphism of some A in $\mathfrak{I}_B^{\mathfrak{l}}$ whose kernel $\mathcal{W} = A[\mathfrak{l}^r]$ is the kernel of the composition of a suitably long chain of isogenies as above. Hence $\mathcal{W} \subseteq C^{(n)}(A)$ for n sufficiently large. Thus $\operatorname{rank}_{\mathfrak{o}_{\mathfrak{l}}} C(A) = \operatorname{rank}_{\mathfrak{o}_{\mathfrak{l}}} \mathbb{T}_{\mathfrak{l}}(A)$. The ranks on both sides are $\mathfrak{o}$-isogeny invariants. Therefore, by purity, $C(A') = \mathbb{T}_{\mathfrak{l}}(A')$ for all A' in $\mathfrak{I}_B^{\mathfrak{l}}$. □

The toric space $M_t(A, v, \mathfrak{l})$ and finite space $M_f(A, v, \mathfrak{l})$ described in §3 will be used to build mirages. Let $\mathcal{P}$ be a set of places of $\overline{\mathbb{Q}}$ with exactly one v over each bad prime p of A. For any subset $\mathcal{P}'$ of $\mathcal{P}$, let

$$M_t(A, \mathcal{P}', \mathfrak{l}) = \langle M_t(A, v, \mathfrak{l}) \,|\, v \in \mathcal{P}' \rangle^{sat},$$

where the *saturation* of an $\mathfrak{o}_{\mathfrak{l}}$-submodule X of $\mathbb{T}_{\mathfrak{l}}(A)$ is the pure submodule

$$X^{sat} = (k_{\mathfrak{l}} \otimes X) \cap \mathbb{T}_{\mathfrak{l}}(A),$$

with $k_{\mathfrak{l}}$ the field of fractions of $\mathfrak{o}_{\mathfrak{l}}$. For $\mathfrak{o}$-isogenies $\varphi\colon A \to A'$, we have the desired functoriality $\varphi_*(M_t(A,v,\mathfrak{l})) \subseteq M_t(A',v,\mathfrak{l})$. If $C(A)$ contains $M_t(A,\mathcal{P}',\mathfrak{l})$, then the same holds for all B in $\mathcal{I}_A^{\mathfrak{l}}$ by purity. In view of (3.2.3), we have

$$\max_{v\in\mathcal{P}'} \tau_{p_v} \le \operatorname{rank}_{\mathfrak{o}_{\mathfrak{l}}} M_t(A,\mathcal{P}',\mathfrak{l}) \le \sum_{v\in\mathcal{P}'} \tau_{p_v}. \tag{6.1.6}$$

The following lemma can provide a better lower bound when $\mathcal{P}$ is suitably chosen.

Lemma 6.1.7. *Let X be a proper pure $\mathfrak{o}_{\mathfrak{l}}$-submodule of $\mathbb{T}_{\mathfrak{l}}(A)$ and p a prime of bad reduction for A. Then we can find a place v above p in $L_\infty = \mathbb{Q}(A[\mathfrak{l}^\infty])$ such that $X + M_t(A,v,\mathfrak{l})$ contains X properly.*

Proof. Let $G = \mathrm{Gal}(L_\infty/\mathbb{Q})$ and pick some place w over p. If the claim is false, we have $\sigma(M_t(A,w,\mathfrak{l})) = M_t(A,\sigma(w),\mathfrak{l}) \subseteq X$ for all σ in G, so X contains the $\mathfrak{o}_{\mathfrak{l}}[G]$-submodule Y of $\mathbb{T}_{\mathfrak{l}}(A)$ generated by $M_t(A,w,\mathfrak{l})$. But Tate's conjecture, proved by Faltings, asserts that $\mathrm{End}_{\mathbb{Z}_\ell[G]}(\mathbb{T}_\ell(A)) = \mathrm{End}\,A \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Thus $\mathrm{End}_{\mathfrak{o}_{\mathfrak{l}}[G]}(\mathbb{T}_{\mathfrak{l}}(A)) = \mathfrak{o}_{\mathfrak{l}}$ and the semisimplicity of $\mathbb{T}_{\mathfrak{l}}(A)$ implies that $X = Y = \mathbb{T}_{\mathfrak{l}}(A)$. □

6.2. **Mirages in the prosaic case.** Let G be a 2-group, $\mathbb{F}$ a finite field of characteristic 2 and W an $\mathbb{F}[G]$-module. For any subgroup H of G, let $\mathfrak{a}_H$ be the augmentation ideal in $\mathbb{F}[H]$, with $\mathfrak{a} = \mathfrak{a}_G$. If $H = \langle g_j \,|\, 1 \le j \le n\rangle$, the identity

$$g_1g_2 - 1 = (g_1-1) + (g_2-1) + (g_1-1)(g_2-1)$$

shows that $\mathfrak{a}_H = \langle g_j - 1 \,|\, 1 \le j \le n\rangle$. For $k \ge 0$, we consider the filtration

$$W_k = \{x \in W \,|\, \mathfrak{a}^k x = 0\} = \{x \in W \,|\, \mathfrak{a}x \in W_{k-1}\}. \tag{6.2.1}$$

Then $0 = W_0 \subset \cdots \subset W_j \subset \cdots \subset W_m = W$ for some $m \ge 0$, with proper inclusions along the way. Within the appropriate ranges of k and k', we have

$$\mathfrak{a}^k\, W_{k'+k} \subseteq W_{k'}. \tag{6.2.2}$$

Thus G acts trivially on W_{k+1}/W_k, has exponent two on W_{k+2}/W_k and exponent dividing four on W_{k+4}/W_k. In particular, $W_1 = W^G$.

Lemma 6.2.3. *Let $H = \{h \in G \,|\, (h-1)(W_{k+2}) \subseteq W_k\}$. Then $\overline{G} = G/H$ is elementary abelian, say of rank r, and* $\dim W_{k+2}/W_{k+1} \le r \dim W_{k+1}/W_k$.

Proof. We have an injective $\mathbb{F}$-linear map $\psi : W_{k+2}/W_{k+1} \to \mathrm{Hom}_{\mathbb{F}_2}(\overline{G}, W_{k+1}/W_k)$ induced by $\psi(x)(g) = (g-1)(x)$ for x in W_{k+2} and g in G. □

Lemma 6.2.4. *Assume that the maximal quotient $\mathfrak{G}$ of G acting faithfully on W_3 is abelian. If either* (i) $W_2^{\langle g\rangle} = W_1$ *for some involution g in $\mathfrak{G}$, or* (ii) *$\mathfrak{G}$ is elementary abelian and* $\dim W_2/W_1 = 1$, *then $W_3 = W_2$.*

Proof. (i) If x is in $W_3 - W_2$, we can find h in $\mathfrak{G}$ such that $y = (h-1)(x)$ is not in W_1 and so $z = (g-1)(y) \ne 0$. But $(g-1)(x)$ is in $W_2^{\langle g\rangle} = W_1$ and so is fixed by h. Hence, $0 = (h-1)(g-1)(x) = (g-1)(h-1)(x) = (g-1)(y) = z$.

(ii) For some g in $\mathfrak{G}$, $g-1$ has rank one on W_2 and $\dim W_2^{\langle g\rangle} = \dim W_1$. Now (i) applies because $W_1 \subseteq W_2^{\langle g\rangle}$. □

Lemma 6.2.5. *If $g^2 = 1$ on W_3 and $W_2^{\langle g\rangle} = W_1$, then g acts trivially on W_3/W_1.*

Proof. We have $(g-1)(W_3) \subseteq W_2^{\langle g\rangle} = W_1$, so g is trivial on W_3/W_1. □

Lemma 6.2.6. *If* $g = \left[\begin{smallmatrix} 1 & x & a & b \\ 0 & 1 & c & d \\ 0 & 0 & 1 & y \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right]$ *has order two, then* $cx = 0, cy = 0$ *and* $dx + ay = 0$.

For the rest of this subsection, we assume:

M1 W is a Galois submodule of $A[\mathfrak{l}]$ with $G = \mathrm{Gal}(\mathbb{Q}(W)/\mathbb{Q})$ a 2-group generated by involutions and W_k is given by (6.2.1).

Let χ_d denote the quadratic character of $\mathbb{Q}(\sqrt{d})$.

Lemma 6.2.7. *Suppose* $C(A)$ *contains* $M_t(A, v, \mathfrak{l})$ *and* A *is obstructed for* C. *Then* $\overline{M}_t(A, v, \mathfrak{l}) \cap W_1 = 0$ *and* p_v *does not ramify in* $\mathbb{Q}(W_2)$. *Assume further that* $\mathbb{Q}(W_2) = \mathbb{Q}(\sqrt{d_1})$ *is a quadratic field.*

i) *Then* W_2 *contains all submodules* U *of* W *such that* $\mathbb{Q}(U) \subseteq \mathbb{Q}(\sqrt{d_1})$.
ii) *If* $\chi_{d_1}(p_v) = -1$, *then* $\overline{M}_t(A, v, \mathfrak{l}) \cap W_2 = 0$ *and* p_v *does not ramify in* $\mathbb{Q}(W_3)$.
iii) *If* 2 *ramifies in* $\mathbb{Q}(\sqrt{d_1})$, *then* $\mathcal{W}_2/\mathcal{W}_1 \simeq \mathcal{Z}_{\mathfrak{l}}^r$ *as group schemes.*

Proof. By definition, G is trivial on W_1. Thus $X = \overline{M}_t(A, v, \mathfrak{l}) \cap W_1$ is a Galois module and then $X = 0$ because A is obstructed. Since $(\sigma_v - 1)(W_2)$ is contained in X, we see that p_v does not ramify in $\mathbb{Q}(W_2)$.

(i) G acts on $\mathbb{Q}(\sqrt{d_1})$ via $\langle g \rangle$ for some involution g in G. Hence G acts trivially on $(g-1)(U)$. We deduce that $(g-1)(U) \subseteq W_1$, and so $U \subseteq W_2$.
(ii) Any Frobenius Φ_v in G restricts to a generator of $\overline{G} = \mathrm{Gal}(\mathbb{Q}(\sqrt{d_1})/\mathbb{Q})$. But $\overline{M}_t(A, v, \mathfrak{l})$ is a $\mathcal{D}_v$-module, so $Y = \overline{M}_t(A, v, \mathfrak{l}) \cap W_2$ is a $G_{\mathbb{Q}}$-module and then $Y = 0$ because A is obstructed. Since $(\sigma_v - 1)(W_3)$ is contained in Y, we see that p_v does not ramify in $\mathbb{Q}(W_3)$.
(iii) The involution σ_λ (see Remark 3.3.12) restricts to a generator of $\overline{G}$ and σ_λ acts trivially on the multiplicative component W_2^m at λ. Hence W_2^m is contained in W_1. It follows that $\mathcal{W}_2/\mathcal{W}_1$ is étale at 2. Since $G_{\mathbb{Q}}$ acts trivially, $\mathcal{W}_2/\mathcal{W}_1$ is isomorphic to a direct sum of copies of $\mathcal{Z}_{\mathfrak{l}}$ globally. ☐

Let $\mathcal{P}^u = \{v \in \mathcal{P} \mid p_v \in \Pi_A^u\}$, where Π_A^u is the set of prime divisors of the prosaic $\mathfrak{l}$-conductor $N_A^u(\mathfrak{l})$ as in Definition 5.1. Note that N_W divides $N_A^u(\mathfrak{l})$.

Proposition 6.2.8. *If* $C(A) \supseteq M_t(A, \mathcal{P}^u, \mathfrak{l})$, A *is obstructed for* C *and* $W_1 \subsetneq W_2$, *then* $\mathbb{Q}(W_2) = \mathbb{Q}(i)$. *Moreover:*

i) *the odd primes ramified in* $\mathbb{Q}(W_3)$ *are* $1 \bmod 4$;
ii) $K = \mathbb{Q}(W_3/W_1)$ *is a totally real elementary* 2*-extension unramified at* 2;
iii) $\mathbb{Q}(W_3)/K$ *is unramified at odd places.*

Proof. Lemma 6.2.7 implies $\mathbb{Q}(W_2)$ is unramified at odd places, so $\mathbb{Q}(W_2) = \mathbb{Q}(i)$. By Lemma 6.2.5, we find that $g = \sigma_\infty$ and $g = \sigma_\lambda$ act trivially on W_3/W_1. Hence K is totally real and unramified over 2. If p_v ramifies in $\mathbb{Q}(W_3)$, then $p_v \equiv 1\,(4)$ by Lemma 6.2.7(ii). Furthermore, p_v already ramifies in K. Otherwise, σ_v acts trivially on W_3/W_1, so $(\sigma_v - 1)(W_3) \subseteq \overline{M}_t(A, v, \mathfrak{l}) \cap W_1 = 0$ by Lemma 6.2.7, making σ_v trivial on $\mathbb{Q}(W_3)$. The necessarily odd primes that ramify in $K/\mathbb{Q}$ cannot ramify further in $\mathbb{Q}(W_3)/K$ by Lemma 3.3.10. ☐

Corollary 6.2.9. *Assume that* K *is a quadratic field* $\mathbb{Q}(\sqrt{d_2})$. *Then* $\mathbb{Q}(W_3)$ *is in* $D_4(-1, d_2)$. *Let* n *be maximal such that* $W_{n-1} \neq W_n$ *and* $\mathrm{Gal}(\mathbb{Q}(W_n)/\mathbb{Q})$ *is generated by two elements. If* $q_w \equiv 3\,(4)$ *and* $\chi_{d_2}(q_w) = -1$ *for some* w *in* $\mathcal{P}^u$, *then* $\overline{M}_t(A, w, \mathfrak{l}) \cap W_n = 0$, $W_n \subsetneq W_{n+1}$ *and* q_w *does not ramify in* W_{n+1}.

Proof. Fix v in $\mathcal{P}$ such that p_v divides d_2. The group $\mathrm{Gal}(\mathbb{Q}(W_3)/\mathbb{Q})$ is generated by σ_∞ and involutions $\sigma_{v'}$ with v' in $\mathcal{P}^u$. If $\sigma_{v'}$ is not trivial on W_3, we show that $\sigma_{v'} = \sigma_v$ on W_3. Indeed, σ_v and $\sigma_{v'}$ agree on K. For x in W_3, it follows that $y = \sigma_v(x) - \sigma_{v'}(x)$ becomes trivial in W_3/W_1, so y is in W_1. Now

$$y = (\sigma_v - 1)(x) - (\sigma_{v'} - 1)(x) \in \overline{C}(A) \cap W_1 = 0$$

because A is obstructed. Hence $\mathrm{Gal}(\mathbb{Q}(W_3)/\mathbb{Q}) = \langle \sigma_\infty, \sigma_v \rangle$. From matrix representations for σ_∞ and σ_v with respect to the filtration on W_3, one easily sees that $\mathbb{Q}(W_3)$ is in $D_4(-1, d_2)$.

By Burnside's theorem, $\mathrm{Gal}(\mathbb{Q}(W_n)/\mathbb{Q}) = \langle \sigma_\infty, \sigma_v \rangle$. Thus $\mathrm{Gal}(\mathbb{Q}(W_n)/\mathbb{Q})$ is dihedral and $\tau = \sigma_\infty \sigma_v$ generates the cyclic subgroup of index 2. The fixed field of τ is $\mathbb{Q}(\sqrt{-d_2})$.

Suppose the hypotheses on q_w hold. Then the restriction of a Frobenius Φ_w to $\mathbb{Q}(W_n)$ generates the same subgroup of $\mathrm{Gal}(\mathbb{Q}(W_n)/\mathbb{Q})$ as τ. Since $M_t(A, w, \mathfrak{l})$ is a $\mathcal{D}_w$-module, τ preserves $Y = \overline{M}_t(A, w, \mathfrak{l}) \cap W_n$. If $Y \neq 0$, then τ has a non-zero fixed point y in Y. It follows that $\sigma_\infty(y) = \sigma_v(y)$, and so

$$z = (\sigma_\infty - 1)(y) = (\sigma_v - 1)(y)$$

is fixed by σ_∞ and σ_v. Hence z is a rational point in $\overline{M}_t(A, w, \mathfrak{l})$. But then $z = 0$ because A is obstructed. From this, it follows that both σ_v and σ_∞ fix y. Hence y is a rational point in Y. Since A is obstructed, we conclude that $Y = 0$, so $W_n \subsetneq W_{n+1}$ and q_w is unramified in W_n. □

Theorem 6.2.10. *Let A be a semistable $\mathfrak{o}$-type abelian variety with odd conductor N. Then $2 \dim A \leq \Omega(N)$ if $\mathrm{Gal}(\mathbb{Q}(A[\mathfrak{l}])/\mathbb{Q})$ is a 2-group for some $\mathfrak{l} | 2$ in $\mathfrak{o}$ and either:* i) *all prime factors of N are $3 \bmod 4$, or*
ii) *at least two primes divide N, one $p \equiv 1\,(4)$, and for all other $q \mid N$, we have $q \equiv 3\,(4)$ and $\chi_p(q) = -1$.*

Proof. Let $C(B) = M_t(B, \mathcal{P}, \mathfrak{l})$ for all B in $\mathfrak{I}^{\mathfrak{l}}_A$. If A is obstructed for the associated mirage, Lemma 6.1.5 implies that $C(A) = \mathbb{T}_{\mathfrak{l}}(A)$, and so (6.1.6) gives

$$2 \dim A = d \operatorname{rank}_{\mathfrak{o}_{\mathfrak{l}}} \mathbb{T}_{\mathfrak{l}}(A) = d \operatorname{rank}_{\mathfrak{o}_{\mathfrak{l}}} C(A) \leq \Omega(N_A).$$

Suppose A is obstructed and consider the filtration (6.2.1) of $W = A[\mathfrak{l}]$. Since $\mathcal{P}$ is not empty, Lemma 6.2.7 shows that $W_2 \supsetneq W_1$, so $\mathbb{Q}(W_2) = \mathbb{Q}(i)$ by Proposition 6.2.8(i). Since at least one prime $q \equiv 3\,(4)$ divides N_A, Lemma 6.2.7(ii) shows that $W_3 \supsetneq W_2$ and the odd primes ramifying in $\mathbb{Q}(W_3)$ are 1 mod 4. In case (i), we now have $\mathbb{Q}(W_3) = \mathbb{Q}(i)$. But then $W_3 = W_2$ by Lemma 6.2.7(i).

Assume (ii) holds and $\mathbb{Q}(W_3) \supsetneq \mathbb{Q}(i)$. By Proposition 6.2.8, $K = \mathbb{Q}(W_3/W_1) = \mathbb{Q}(\sqrt{p})$. With n as in Corollary 6.2.9, $\mathbb{Q}(W_3)$ is in $D_4(-1, p)$ and $W \supsetneq W_n$. By Burnside, there is a quadratic field $\mathbb{Q}(\sqrt{d_3})$ in $\mathbb{Q}(W_{n+1})$ but not in $\mathbb{Q}(i, \sqrt{p})$. Thus some q ramifies in $\mathbb{Q}(W_{n+1})$ and contradicts Corollary 6.2.9. □

For the rest of this subsection, we assume:

M2 A is $(\mathfrak{o}, N)$-paramodular, $W = A[\mathfrak{l}]$, $L = \mathbb{Q}(W)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$ is a 2-group. In particular, A has good ordinary reduction at 2. Recall that $N_A^0 = N$ is the reduced conductor of A.

Proposition 6.2.11. *Assume $N_A^0 = pqr$ for primes p, q, r with $p \equiv -q \equiv 5\,(8)$ and $r \equiv 7\,(8)$. Then $\chi_p(r) = 1$. Moreover, $\chi_q(p) = 1$ or $\chi_q(r) = 1$.*

Proof. By Lemma 6.1.7, we choose $\mathcal{P}$ so that $C(A) = \mathbf{M}_t(A, \mathcal{P}, \mathfrak{l})^{\mathrm{sat}}$ has $\mathfrak{o}_\mathfrak{l}$-rank three. Suppose A is obstructed for the associated mirage and let $W = A[\mathfrak{l}]$. Since $\overline{C}(A) \cap W_1 = 0$, we have $\dim_\mathbb{F} W_1 = 1$.

Proposition 6.2.8 and its corollary show that $\mathbb{Q}(W_2) = \mathbb{Q}(i)$, $\mathbb{Q}(W_3/W_1) = \mathbb{Q}(\sqrt{p})$ and $\mathbb{Q}(W_3)$ is in $D_4(-1, p)$. We have $\dim W_k = k$ for $k = 1, 2, 3$ by Lemma 6.2.3, and so $W = W_4$. Because 2 ramifies in $\mathbb{Q}(W_2)$ and is inert in $\mathbb{Q}(W_3/W_1)$, we find that $\mathbf{gr}\, W_3 = [\boldsymbol{\mu}_\mathfrak{l} \mathcal{Z}_\mathfrak{l} \mathcal{Z}_\mathfrak{l}]$. Hence $\mathbf{gr}\, W = [\boldsymbol{\mu}_\mathfrak{l} \mathcal{Z}_\mathfrak{l} \mathcal{Z}_\mathfrak{l} \boldsymbol{\mu}_\mathfrak{l}]$, forcing 2 to split in $\mathbb{Q}(W_4/W_2)$. But the conductor of W_4/W_2 divides qr, and so $\mathbb{Q}(W_4/W_2) = \mathbb{Q}(\sqrt{-r})$. By Corollary 6.2.9, we have $\chi_p(r) = 1$.

Let $\Phi_q = \mathrm{Frob}_w$ at the place w in $\mathcal{P}$ over q. Suppose, contrary to our claim, that $\chi_q(p) = \chi_q(r) = -1$. Then Φ_w admits a matrix representation as in (6.2.6) with c, x, y all non-zero, so $\ker(\Phi_w - 1) = W_1$. Since the Φ_w-module $\overline{M}_t(A, w, \mathfrak{l})$ is one-dimensional over $\mathbb{F}$, $W_1 = \overline{M}_t(A, w, \mathfrak{l})$, and so A is not obstructed. ☐

Proposition 6.2.12. *If $q \equiv 3\,(4)$ and $N_A^0 = pq^a$, then $a = 2$, $p \equiv 1\,(4)$ and $\chi_p(q) = 1$.*

Proof. If v is a place over p, then $M_f(A, v, \mathfrak{l}) = \mathbb{T}_\mathfrak{l}(A)^{\mathcal{I}_v}$ is a pure $\mathfrak{o}_\mathfrak{l}$-submodule of $\mathbb{T}_\mathfrak{l}(A)$ of rank 3. Suppose A is obstructed for the mirage associated to $C(A) = M_f(A, v, \mathfrak{l})$. Then $\overline{C}(A) \cap W_1 = 0$, so $\dim_\mathbb{F} W_1 = 1$; thus $W = W_1 \oplus \overline{M}_f(A, v, \mathfrak{l})$. Now $\mathcal{I}_v$ acts trivially on W, so $L/\mathbb{Q}$ is unramified at p. It follows that the maximal elementary 2-extension of $\mathbb{Q}$ inside L is contained in $\mathbb{Q}(i, \sqrt{q})$. Hence $G = \langle \sigma_\infty, \sigma_w \rangle$, where w is a place over q.

Since the Hilbert symbol $(-1, q)_q = -1$, there is no $D_4(-1, q)$ field, and so G is abelian. Lemmas 6.2.3 and 6.2.4 now imply that $\dim W_2 = 3$, and $\mathbb{Q}(W_2) = \mathbb{Q}(i, \sqrt{q})$. In particular, σ_w is not trivial on W_2, and so $(\sigma_w - 1)(W_2) = W_1$.

If $a = 1$, then $\dim(\sigma_w - 1)(W) = 1$, so $(\sigma_w - 1)(W) = W_1$ and we find that $(\sigma_\infty - 1)(\sigma_w - 1)(W) = 0$. Because σ_w and σ_∞ are commuting involutions, it follows that $\mathfrak{a}_G^2 W = 0$. But then $W = W_2$, a contradiction. Hence $a = 2$. Finally, by Theorem 6.2.10, we have $p \equiv 1\,(4)$ and $\chi_p(q) = 1$. ☐

Proposition 6.2.13. *If $q \equiv 5\,(8)$ and $N_A^0 = pq^2$, then $p^* \equiv 1\,(8)$ and $\chi_p(q) = 1$.*

Proof. We have $p^* \equiv 1\,(8)$ by Theorem 5.3. Fix a place λ over 2 to define the multiplicative component $\mathbb{T}_\mathfrak{l}(A)^m$, which has $\mathfrak{o}_\mathfrak{l}$-rank 2 because A is ordinary at 2. By Lemma 6.1.7, we can choose v over p to guarantee that the $\mathfrak{o}_\mathfrak{l}$-rank of

$$C(A) = \{M_t(A, v, \mathfrak{l}) + \mathbb{T}_\mathfrak{l}(A)^m\}^{sat}$$

is 3. Assume that A is obstructed for C and let $W = A[\mathfrak{l}]$. Then $\overline{C}(A) \cap W_1 = 0$, so $\dim W_1 = 1$. Moreover, the $\mathbb{F}$-module scheme associated to W_1 is $\mathcal{W}_1 \simeq \mathcal{Z}_\mathfrak{l}$ and $\mathbb{Q}(W_2)$ is unramified at p. Choose σ_λ as in Remark 3.3.12. Then $(\sigma_\lambda - 1)(W_2)$ is contained in $W_1^m = 0$. Thus σ_λ fixes W_2 pointwise and $\mathbb{Q}(W_2)$ is unramified at 2.

It follows that $\mathbb{Q}(W_2) = \mathbb{Q}(\sqrt{q})$, and so $\dim W_2 = 2$ by Lemma 6.2.3. Moreover, $\mathbf{gr}\, \mathcal{W}_2 = [\mathcal{Z}_\mathfrak{l}\, \mathcal{Z}_\mathfrak{l}]$ because 2 is inert in $\mathbb{Q}(W_2)$. Let V be any Galois submodule of W containing W_2 with $\dim_\mathbb{F} V = 3$. Then $\mathrm{Gal}(\mathbb{Q}(V)/\mathbb{Q}) \simeq D_4$ and $\mathbf{gr}\, \mathcal{V} = [\mathcal{Z}_\mathfrak{l}\, \mathcal{Z}_\mathfrak{l}\, \boldsymbol{\mu}_\mathfrak{l}]$. Since 2 splits in $\mathbb{Q}(V/W_1)/\mathbb{Q}$, we have $\mathbb{Q}(V/W_1) = \mathbb{Q}(\sqrt{p^*})$, whence $\chi_p(q) = 1$ by Proposition 4.2.9. ☐

Proposition 6.2.14. *Let $N_A^0 = pqr^a$ with p, q, r prime and $q^* \equiv r^* \equiv 5\,(8)$. Assume $K = \mathbb{Q}(\sqrt{p^*}, \sqrt{q^*}, \sqrt{r^*})$ has no quadratic extension unramified outside ∞ and split over 2.*

i) *If $p^* \equiv 1\,(8)$ and $1 \le a \le 2$, then $(p, q, r) \equiv (1, 5, 5) \bmod 8$.*
ii) *If $p^* \equiv 5\,(8)$ and $a = 2$, then $p \equiv q \equiv r \equiv 5\,(8)$.*

Proof. We refer to the filtration (6.2.1) of $\mathcal{W} = A[\mathfrak{l}]$. Let A be obstructed for the mirage $C(A) = \{M_t(A, v, \mathfrak{l}) + \mathbb{T}_\mathfrak{l}(A)^m\}^{sat}$ of $\mathfrak{o}_\mathfrak{l}$-rank three, as in the proof of Proposition 6.2.13, so $\mathcal{W}_1 \simeq \mathcal{Z}_\mathfrak{l}$ and $\mathbb{Q}(W_2) \subseteq \mathbb{Q}(\sqrt{q^*}, \sqrt{r^*})$. By Lemma 6.2.3, $\dim W_2 \le 3$ with equality only if $[\mathbb{Q}(W_2) : \mathbb{Q}] = 4$. A nugget filtration of $\mathcal{W}$ must have one of the following gradings:

$$\alpha : [\mathcal{Z}_\mathfrak{l}\mathcal{Z}_\mathfrak{l}\boldsymbol{\mu}_\mathfrak{l}\boldsymbol{\mu}_\mathfrak{l}], \qquad \beta : [\mathcal{Z}_\mathfrak{l}\boldsymbol{\mu}_\mathfrak{l}\boldsymbol{\mu}_\mathfrak{l}\mathcal{Z}_\mathfrak{l}], \qquad \gamma : [\mathcal{Z}_\mathfrak{l}\boldsymbol{\mu}_\mathfrak{l}\mathcal{Z}_\mathfrak{l}\boldsymbol{\mu}_\mathfrak{l}].$$

If $0 \subsetneq \mathcal{V}_1 \subsetneq \mathcal{V}_2 \subsetneq \mathcal{V}_3 \subsetneq \mathcal{W}$ is the corresponding flag, then $\mathcal{V}_1 = \mathcal{W}_1$ and $\mathcal{V}_2 \subseteq \mathcal{W}_2$.

Let $X \subseteq W$ be a Galois submodule with $\mathbb{Q}(X)/\mathbb{Q}$ abelian. If p ramifies in $\mathbb{Q}(X)$, then $(\sigma_v - 1)(X)$ is a Galois submodule of W, violating the obstruction.

Suppose α or β holds. Then $\mathcal{V}_3$ is a nugget and by Corollary 4.2.10 (or its dual), we find that $K(V_3)/K$ is an elementary 2-extension, unramified at finite places and split over 2. Our assumption now implies that $K(V_3) = K$, so $\mathbb{Q}(V_3)/\mathbb{Q}$ is abelian. But p ramifies in $\mathbb{Q}(V_3)$ by Lemma 4.3.15, a contradiction.

Assume γ holds. Then $\mathbb{Q}(V_2) = \mathbb{Q}(\sqrt{q^*r^*})$ because p is unramified and 2 splits. Since $\mathcal{W}/\mathcal{V}_2$ is a nugget, we have $\mathbb{Q}(W/V_2) = \mathbb{Q}(\sqrt{d_3})$, with $d_3 = p^*$ in case (i) and $d_3 = p^*r^*$ in case (ii). Let g in Lemma 6.2.6 generate the relevant inertia group, to conclude that $\mathbb{Q}(V_3/V_1)$ is unramified at p, q, r and so $\mathbb{Q}(V_3/V_1) \subseteq \mathbb{Q}(i)$.

If $\mathbb{Q}(V_3/V_1) = \mathbb{Q}$, then $V_3 = W_2$ and $\mathbb{Q}(W_2) = \mathbb{Q}(\sqrt{q^*}, \sqrt{r^*})$. Because W^m and W^{et} are unramified $\mathcal{D}_\lambda$-modules, 2 is unramified in $\mathbb{Q}(W)$ and $f_\lambda(\mathbb{Q}(W)/\mathbb{Q}) = 2$. But then $K(W) = K$ leads to a contradiction as above.

If $\mathbb{Q}(V_3/V_1) = \mathbb{Q}(i)$, Proposition 4.2.9 shows that $(-1, q^*r^*)_\pi = (-1, d_3)_\pi = 1$ for all π in $\{p, q, r\}$. Hence $p \equiv q \equiv r \equiv 1\,(4)$ and the claim ensues. □

We sketch a more easily tested version of the previous proposition.

Proposition 6.2.15. *Let $N_A^0 = pqr^a$ with p, q, r prime and $q^* \equiv r^* \equiv 5\,(8)$.*

i) *If $p^* \equiv 1\,(8)$, $1 \le a \le 2$ and none of $D_4^{nr}(p^*, q^*)$, $D_4^{nr}(p^*, r^*)$, $D_4^{sp}(p^*, q^*r^*)$ exists, then $(p, q, r) \equiv (1, 5, 5) \bmod 8$.*
ii) *If $p^* \equiv 5\,(8)$, $a = 2$ and none of $D_4^{nr}(p^*q^*, r^*)$, $D_4^{nr}(p^*r^*, q^*)$, $D_4^{nr}(q^*r^*, p^*)$ exists, then $p \equiv q \equiv r \equiv 5\,(8)$.*

Proof. In case α or β of the previous proof, Corollary 4.2.10 implies that the current conditions suffice. Case γ leads to a quadratic extension L/K, unramified outside infinity and split over 2, such that $L/\mathbb{Q}$ is Galois, with group $D_4 \times C_2$. This descends to a D_4-extension $M/\mathbb{Q}$, such that M/k is cyclic of order 4, unramified outside infinity and split over 2, with $k = \mathbb{Q}(\sqrt{p^*q^*})$ or $k = \mathbb{Q}(\sqrt{p^*r^*})$ in (i) and $k = \mathbb{Q}(\sqrt{p^*q^*r^*})$ in (ii). □

6.3. **Mirages with exceptionals.** In this subsection, A is a semistable abelian variety of $\mathfrak{o}$-type with good reduction at $\ell = 2$, $\mathfrak{l}$ is a prime over 2 in $\mathfrak{o}$ and $\mathbb{F} = \mathbb{F}_\mathfrak{l}$. Let E be an exceptional constituent of $A[\mathfrak{l}]$ and $T = T_E$ the set of bad primes of E. We need a variant of Notation 4.3.2.

Notation 6.3.1. Let X be an irreducible component of E as an $\mathbb{F}_2[\Delta]$-module. For $S \supseteq T$, let $\Lambda_E^{cr}(S)$ be the maximal elementary 2-extension Λ of F such that

i) Λ/F is unramified outside $\{2, \infty\} \cup (S \backslash T)$,
ii) for $\lambda \,|\, 2$, the ramification groups $\mathcal{I}_\lambda(\Lambda/\mathbb{Q})^\alpha = 0$ when $\alpha > 1$ and
iii) $\mathrm{Gal}(\Lambda/F) \simeq X^{*\,r}$ as an $\mathbb{F}_2[\Delta]$-module.

Let $r_E^{cr}(S)$ be the multiplicity of X^* in $\mathrm{Gal}(\Lambda_E^{cr}(S)/F)$ and $\Gamma_E^{cr}(S) = \mathrm{Gal}(\Lambda_E^{cr}(S)/\mathbb{Q})$. Note that $X^* \simeq \widehat{X}$, so $\Lambda_E^{cr}(S)$ contains $\Lambda_E(S)$.

Remark 6.3.2. Assume V is a semistable $\mathbb{F}[G_\mathbb{Q}]$-module, $T_E \subseteq T_V \subseteq S$ and

$$0 \to \mathbb{F}^n \to V \overset{\pi}{\to} E \to 0 \tag{6.3.3}$$

is exact. Then $\mathbb{Q}(V) \subseteq \Lambda_E^{cr}(S)$ by Remark 3.5.4 and Lemma 3.3.10.

Suppose $F \subseteq K \subseteq \Lambda_E^{cr}(S)$, with K Galois over $\mathbb{Q}$. At bad places v of E, let $M_v = (\sigma_v - 1)(E)$ and $\mathcal{L}_v^{cr} = H^1(\mathcal{I}_v(K/\mathbb{Q}), M_v^*)$. Set

$$H^1_{\mathcal{L}^{cr}}(\mathrm{Gal}(K/\mathbb{Q}), E^*) = \ker\colon H^1(\mathrm{Gal}(K/\mathbb{Q}), E^*) \xrightarrow{\text{res}} \prod_{v | N_E} \mathcal{L}_v^{cr}.$$

Lemma 6.3.4. *If* $G = \mathrm{Gal}(\mathbb{Q}(V)/\mathbb{Q})$ *and* $H^1_{\mathcal{L}^{cr}}(G, E^*) = 0$, *then* (6.3.3) *splits.*

Proof. Let $M = \ker \pi \simeq \mathbb{F}^n$ in (6.3.3) and let v lie over a bad prime of E. Since V is semistable, σ_v acts trivially on $\pi^{-1}(M_v) = (\sigma_v - 1)(V) + M$. Hence the sequence $0 \to M \to \pi^{-1}(M_v) \to M_v \to 0$ is $\mathbb{F}[\mathcal{I}_v]$-split. Corollary 3.5.3(i), with $X = M^*$, $Y = E^*$, $\overline{Y}_i = M_v^*$ and $\overline{V}_i = \pi^{-1}(M_v)^*$, now implies that $X' = X^G = M^*$. We conclude by duality from Lemma 3.5.2(i). □

The following hypothesis will be used to create mirages of the form (6.1.4).

M3 There is an odd order subgroup H of $G_\infty = \mathrm{Gal}(\mathbb{Q}(A[\mathfrak{l}^\infty])/\mathbb{Q})$ such that $E^H = 0$ for all E in $\mathfrak{S}_\mathfrak{l}(A)$.

Lemma 6.3.5. *If* $\mathrm{Gal}(\mathbb{Q}(E)/\mathbb{Q})$ *is solvable for all* E *in* $\mathfrak{S}_\mathfrak{l}(A)$, *then* **M3** *holds.*

Proof. Since $\mathbb{Q}(A[\mathfrak{l}^\infty])$ is a pro-2 extension of the field $\mathbb{Q}(A[\mathfrak{l}]^{ss})$ generated by the points of all the exceptional Galois $\mathfrak{o}_\mathfrak{l}$-modules E in $\mathfrak{S}_\mathfrak{l}(A)$, G_∞ is solvable. The profinite version of Hall's theorem provides a subgroup H of maximal odd order in G_∞. Fix E and let $\overline{H}$ be the projection of H to $\Delta_E = \mathrm{Gal}(\mathbb{Q}(E)/\mathbb{Q})$. Then $\overline{H}$ has maximal odd order in Δ_E. A minimal normal subgroup N of Δ_E is a p-group. Since E is irreducible and Δ_E acts faithfully, we have $E^N = 0$, and so p is odd. Hence $\overline{H}$ contains a conjugate of N. It follows that $E^H = E^{\overline{H}} = 0$. □

Since H has odd order, the central idempotent $e_H = \frac{1}{|H|} \sum_{h \in H} h$ gives a natural H-splitting $M = M^H \oplus (1 - e_H)M$ for any $\mathfrak{o}_\mathfrak{l}[H]$-module M. Define

$$D_H = D_H(A) = (1 - e_H)\mathbb{T}_\mathfrak{l}(A) = \ker\colon \mathbb{T}_\mathfrak{l}(A) \xrightarrow{e_H} \mathbb{T}_\mathfrak{l}(A).$$

Then D_H is a pure $\mathfrak{o}_\mathfrak{l}$-submodule of $\mathbb{T}_\mathfrak{l}(A)$. For $\mathfrak{o}_\mathfrak{l}$-linear isogenies $\varphi : A \to A'$, the functorial property $\varphi(D_H(A)) \subseteq D_H(A')$ holds. By projection to $A[\mathfrak{l}]$, we obtain an $\mathbb{F}[H]$-module $\overline{D}_H = (1 - e_H)A[\mathfrak{l}]$, such that

$$\dim_\mathbb{F} \overline{D}_H = \dim_\mathbb{F} A[\mathfrak{l}] - \epsilon_0(A[\mathfrak{l}]), \tag{6.3.6}$$

where $\epsilon_0(A[\mathfrak{l}])$ is the number of one-dimensional constituents of $A[\mathfrak{l}]$. Under **M3**, $\dim A[\mathfrak{l}]^H = \epsilon_0(A[\mathfrak{l}])$, and any E in $\mathfrak{S}_\mathfrak{l}(A)$ which is a submodule of $A[\mathfrak{l}]$ lies in $\overline{D}_H$.

Definition 6.3.7. We say E is $(S\backslash T_E)$-*fissile* if, for every semistable $\mathbb{F}[G_{\mathbb{Q}}]$-module Y such that $T_Y \subseteq S$, the exact sequence $0 \to \mathbb{F} \to Y \to E \to 0$ splits. We say *fissile* if $S = T_E$.

Recall that $N_A^u = N_A^u(\mathfrak{l})$ is the prosaic $\mathfrak{l}$-conductor of A and Π_A^u is the set of primes dividing N_A^u, as in Definition 5.1. See Definition 4.4.4 for p-transparency.

Theorem 6.3.8. *Assume that* **M3** *applies and that all E in $\mathfrak{S}_{\mathfrak{l}}(A)$ are fissile. Then $\epsilon_0(A[\mathfrak{l}]) \leq \Omega(N_A^u)$, if one of the following holds:*

i) *all primes in Π_A^u are $3 \bmod 4$, or*
ii) *exactly one p in Π_A^u is $1 \bmod 4$, every subquotient $\mathcal{E}$ of $A[\mathfrak{l}]$ with Galois module E is p-transparent and $\chi_p(q) = -1$ for all other q in Π_A^u.*

Proof. Recall that $\mathcal{P}^u$ contains one place of $\mathbb{Q}(A[\mathfrak{l}^\infty])$ for each prime of Π_A^u. Let $C(A) = (M_t(A, \mathcal{P}^u, \mathfrak{l}) + D_H)^{sat}$. If the associated mirage is unobstructed, then Lemma 6.1.5 and (6.1.6) imply that

$$\dim_{\mathbb{F}} A[\mathfrak{l}] = \dim_{\mathbb{F}} \overline{C}(A) \leq \dim_{\mathbb{F}} \overline{D}_H + \dim_{\mathbb{F}} \overline{M}_t(A, \mathcal{P}^u, \mathfrak{l}) \leq \dim_{\mathbb{F}} \overline{D}_H + \Omega(N_A^u),$$

and our claim follows from (6.3.6). We therefore assume that A is obstructed.

Let X be an $\mathbb{F}[G_{\mathbb{Q}}]$-submodule of $A[\mathfrak{l}]$ of minimal length with exactly one exceptional constituent. Then we have a filtration $0 \subseteq W \subset X$, with $X/W \simeq E$ in $\mathfrak{S}_{\mathfrak{l}}(A)$ and $\mathbb{Q}(W)/\mathbb{Q}$ a 2-extension. Moreover, $W \neq 0$ or else E is a Galois submodule of $\overline{D}_H$ and A is unobstructed.

The corresponding $\mathbb{F}$-module scheme $\mathcal{W}$ admits a filtration with quotients isomorphic to $\mathcal{Z}_{\mathfrak{l}}$ or $\boldsymbol{\mu}_{\mathfrak{l}}$ and conductor N_W dividing N_A^u. Because X is minimal and E is fissile, there is a place w in $\mathcal{P}^u$ ramified in $\mathbb{Q}(X)$ and unramified in $\mathbb{Q}(E)$. For all such w, the action of σ_w on E is trivial, so

$$0 \neq (\sigma_w - 1)(X) \subseteq \overline{M}_t(A, \mathcal{P}^u, \mathfrak{l}) \cap W. \tag{6.3.9}$$

Consider the filtration (6.2.1) on W. If $W = W_1$, then $(\sigma_w - 1)(X)$ is a Galois module, violating the obstruction. Hence $W_1 \subsetneq W_2$ and Proposition 6.2.8 gives $\mathbb{Q}(W_2) = \mathbb{Q}(i)$. Assuming (i), we have $W = W_2$ by Proposition 6.2.8(ii). But then (6.3.9) violates Lemma 6.2.7(ii) and we are done. From now on, we therefore assume that (ii) holds.

For each k, we have the exact sequence of $\mathbb{F}$-module schemes

$$0 \to \mathcal{W}/\mathcal{W}_k \to \mathcal{X}/\mathcal{W}_k \to \mathcal{E} \to 0. \tag{6.3.10}$$

Suppose $W = W_2$. Then $\mathcal{W}/\mathcal{W}_1 \simeq \mathcal{Z}_{\mathfrak{l}}^a$ by Lemma 6.2.7(iii). By (6.3.9) and Lemma 6.2.7(ii), any odd prime ramified in $\mathbb{Q}(X)$ but not in $\mathbb{Q}(E)$ is $1 \bmod 4$. Thus $T_X \subseteq \{p\} \cup T_E$. Depending on whether or not p divides N_E, we may use fissility or p-transparency on (6.3.10) with $k = 1$ to contradict minimality of X. Hence W_3 contains W_2 properly. By Proposition 6.2.8(i), p is the only odd prime that may ramify in $\mathbb{Q}(W_3)$, and so $\mathbb{Q}(W_3)$ is in $D_4(-1, p)$.

Let W_n be as defined in Corollary 6.2.9. Since that corollary and (ii) preclude the existence of a prime ramified in $\mathbb{Q}(W_{n+1})$ but unramified in $\mathbb{Q}(W_n)$, we have $W = W_n$. Now (ii), Corollary 6.2.9 and (6.3.9) imply that $T_X \subseteq \{p\} \cup T_E$. In fact, $p \notin T_E$ and p must ramify in $\mathbb{Q}(X/W_{n-1})$. Otherwise, we contradict the minimality of X by using fissility on (6.3.10) with $k = n - 1$.

Let v be the place over p in $\mathcal{P}^u$. Because $G_{\mathbb{Q}}$ acts trivially on W/W_{n-1}, we know that $Y = (\sigma_v - 1)(X) + W_{n-1}$ is a $G_{\mathbb{Q}}$-module. We claim $Y = W$. If not, let $W' \supseteq Y$ be a Galois submodule of codimension 1 in W. Since σ_v acts trivially on

X/W', the bad primes of X/W' are in T_E. Then we contradict the minimality of X, thanks to the splitting of $0 \to W/W' \to X/W' \to E \to 0$ implied by fissility. Hence $Y = W$, and so $(\sigma_v - 1)(W) = (\sigma_v - 1)(W_{n-1}) \subseteq W_{n-2}$. It follows that $\mathbb{Q}(W/W_{n-2}) = \mathbb{Q}(i)$. The argument used to prove Lemma 6.2.7(iii) shows that $\mathcal{W}/\mathcal{W}_{n-1}$ is a direct sum of copies of $\mathcal{Z}_\mathfrak{l}$. Minimality of X is now contradicted by applying p-transparency to (6.3.10) with $k = n - 1$. □

We impose the following assumption for the rest of this subsection.

M4 A is $\mathfrak{o}$-paramodular, $\mathfrak{S}_\mathfrak{l}^{all}(A) = \{\mathbb{F}, \mathbb{F}, E\}$, $\dim_{\mathbb{F}_\mathfrak{l}} E = 2$ and $H^1(\Delta, E) = 0$. Let T be the set of bad primes of E and S that of A.

By Corollary 3.4.5, $E^* \simeq E$.

Proposition 6.3.11. *Assume* **M4**, *E absolutely irreducible and $r_E^{cr}(T) = 1$. If one of the following holds, then $N_A^u(\mathfrak{l}) > 1$:*

i) *$F = \mathbb{Q}(E)$ is the maximal real subfield of $\Lambda_E^{cr}(T)$; or*
ii) *λ does not ramify in F, $|\mathcal{D}_\lambda(F/\mathbb{Q})| \leq 2$ and λ ramifies in $\Lambda_E^{cr}(T)$.*

Proof. For B in $\mathcal{I}_A^0$, let $\mathfrak{C}(B)$ consist of the $\mathbb{F}$-module subschemes of $B[\mathfrak{l}]$ isomorphic to $\boldsymbol{\mu}_\mathfrak{l}$ or $\mathcal{Z}_\mathfrak{l}$ and let A be obstructed for this mirage. Then there is a filtration $0 \subset \mathcal{E} \subset \mathcal{V} \subset A[\mathfrak{l}]$ whose Galois modules have the grading $[E\,\mathbb{F}\,\mathbb{F}]$. Moreover V does not split, and so $L = \mathbb{Q}(V)$ contains F properly, since $H^1(\Delta, E) = 0$.

If $N_A^u(\mathfrak{l}) = 1$, we have $L = \Lambda_E^{cr}(T)$, since Remark 6.3.2 gives the inclusion and then the argument in Remark 4.4.8 gives equality because $r_E^{cr}(T) = 1$. Set $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/F)$. As in the proof of Lemma 4.3.8, inflation-restriction, the vanishing of $H^1(\Delta, E)$ and Lemma 4.3.1(iii) imply that

$$\dim_\mathbb{F} H^1(G, E) = \dim_\mathbb{F} \mathrm{Hom}_{\mathbb{F}_2[\Delta]}(H, E) = r_E^{cr}(T) \dim_\mathbb{F} \mathrm{End}_{\mathbb{F}[\Delta]} E = 1.$$

Define W by the exact sequence $0 \to E \to A[\mathfrak{l}] \to W \to 0$, so $\mathbf{gr}\, W = [\mathbb{F}\,\mathbb{F}]$. If $\mathbb{Q}(W) = \mathbb{Q}$, then $\mathbb{Q}(A[\mathfrak{l}])$ is contained in L by Remark 6.3.2, whence $\mathbb{Q}(A[\mathfrak{l}]) = L$. By Lemma 3.5.2(i), there is a submodule W' of W whose preimage V' in $A[\mathfrak{l}]$ fits into a *split* exact sequence of Galois modules $0 \to E \to V' \to W' \to 0$ wherein $\dim_\mathbb{F} W/W' \leq 1$. But then $W' \neq 0$, and so the splitting of this last sequence contradicts the obstruction. Hence $\mathbb{Q}(W)$ is a *quadratic* field.

But $N_W = 1$, and so $\mathbb{Q}(W) = \mathbb{Q}(i)$. If (i) holds, let τ be a complex conjugation in G. If (ii), let $\tau = \sigma_\lambda$ as in Remark 3.3.12, since $\mathcal{D}_\lambda(L/\mathbb{Q})$ is a 2-group. Thus τ is an involution, trivial on F, but not on V or W. This contradicts Lemma 6.2.6. □

We defined r_E in Notation 4.3.2 and fissile in Definition 6.3.7.

Proposition 6.3.12. *Assume* **M4**, *2 ramifies in $F = \mathbb{Q}(E)$ and $r_E(S) = 0$, where S is the set of bad places for A and T that for E. If $p^* \equiv 1\,(8)$ and all $q_i^* \equiv 5\,(8)$, then* none *of the following occurs:*

i) *E is fissile and $N_A^u = p^a$ or $q_1^a q_2^b$,*
ii) *E is q_3-fissile and $N_A^u = p^a q_3^b$,*
iii) *$r_E^{cr}(T) = 1$, $N_A^u = p^a$ (resp. $N_A^u = q_1^a q_2^b$) and the primes $v \,|\, p$ (resp. $v \,|\, q_1$ or $v \,|\, q_2$) do not split completely in $\Lambda_E^{cr}(T)/F$.*
iv) *$N_A^u = p^a q_3^b$, $r_E^{cr}(T \cup \{q_3\}) = 1$ and the primes $v \,|\, p$ do not split completely in $\Lambda_E^{cr}(T \cup \{q_3\})/F$.*
v) *F is the maximal totally real subfield of $\Lambda_E^{cr}(T)$ and $N_A^u = p^a$ with $p \equiv 7\,(8)$.*

Proof. For each B in $\mathfrak{I}_A^{\mathfrak{l}}$, let $\mathfrak{C}(B)$ consist of all subschemes of $B[\mathfrak{l}]$ isomorphic to $\boldsymbol{\mu}_{\mathfrak{l}}$ or an $\mathcal{E}$. Since 2 ramifies in $\mathbb{F}$, $\mathcal{E}_{|\mathbb{Z}_2}$ is biconnected or $\mathbf{gr}\,\mathcal{E}_{|\mathbb{Z}_2} = [\boldsymbol{\mu}_{\mathfrak{l}}\, \mathcal{Z}_{\mathfrak{l}}]$. Hence $B[\mathfrak{l}^s]$ also has as many $\mathcal{Z}_{\mathfrak{l}}$'s as $\boldsymbol{\mu}_{\mathfrak{l}}$'s globally. By Proposition 6.1.2, if $\mathfrak{C}$ is not obstructed, then for some B, no subquotient of $B[\mathfrak{l}^r]$ is isomorphic to $\mathcal{Z}_{\mathfrak{l}}$, a contradiction. Thus, assume that A is obtructed.

By Lemma 4.4.5(i), A is Π_A^u-transparent because $r_E(S) = 0$ and 2 ramifies in F. This leads to a filtration $0 \subset \mathcal{V}_1 \subset \mathcal{V} \subset \mathcal{W} = A[\mathfrak{l}]$ with grading $[\mathcal{Z}_{\mathfrak{l}}\, \boldsymbol{\mu}_{\mathfrak{l}}\, \mathcal{E}]$ and $\mathcal{V}$ not split. Corollary 4.2.3 gives $N_V = p$ or $q_1 q_2$. Write $\mathcal{X} = \mathcal{W}/\mathcal{V}_1$ and $L = \mathbb{Q}(X)$. By Lemma 3.2.7, N_X is squarefree and so $\gcd(N_E, N_X/N_E) = 1$.

If an involution τ is trivial on E but not on V, Lemma 6.2.6 shows that τ is trivial on X. By choosing $\tau = \sigma_w$ at places w that divide N_V but not N_E, we deduce that $N_X = N_E$ in (i), (iii) and (iv), while N_X divides $q_3 N_E$ in (ii).

In cases (i) and (ii), fissility provides a Galois submodule E' of X isomorphic to E. Such an E' is also available in cases (iii) and (iv). Otherwise, we have $L = \Lambda_E^{cr}(T)$ in (iii), while $L = \Lambda_E^{cr}(T \cup \{q_3\})$ in (iv). Any Frobenius Φ_v in $\mathcal{D}_v(\mathbb{Q}(W)/F)$ centralizes the generator σ_v of inertia in $\mathcal{D}_v(\mathbb{Q}(W)/F)$. They are represented by matrices the form

$$\sigma_v = \begin{bmatrix} 1 & 1 & * & * \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \Phi_v = \begin{bmatrix} 1 & * & * & * \\ 0 & 1 & \alpha & \beta \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

with $(\alpha, \beta) \neq (0, 0)$ by our assumption that v does not split in L/F. But then the matrices do not commute.

Such an E' also is available in (v), where we have $\mathbb{Q}(V) = \mathbb{Q}(\sqrt{-p})$, and we may use $\tau = \sigma_\infty$ to see that $K = \mathbb{Q}(X)$ is totally real. But $T_X = T_E = T$, so $K \subseteq \Lambda_E^{cr}(T)$ and therefore $K = F$.

In all cases, we now have a filtration $\mathbf{gr}\,\mathcal{W} = [\mathcal{Z}_{\mathfrak{l}}\, \mathcal{E}'\, \boldsymbol{\mu}_{\mathfrak{l}}]$. Thanks to the Π_A^u-transparency of $\mathcal{E}'$, there is an exceptional $\mathbb{F}$-module subscheme $\mathcal{E}''$ of $A[\mathfrak{l}]$, violating the obstruction. □

Lemma 6.3.13. *Suppose* **M3**, **M4** *and* $N_A^u = p^a q$ *with* p, q *primes not dividing* N_E. *If* E *is* p*-fissile and all* $\mathcal{E}$ *are* $\{p, q\}$*-transparent, then* $p^* \equiv 1\,(8)$ *and* $\chi_{p^*}(q) = 1$.

Proof. Fix w over q, write $M_t = M_t(A, w, \mathfrak{l})$ and let A be obstructed for the mirage associated to $C(A) = (M_t + D_H)^{sat}$. Then E is not a Galois submodule of $A[\mathfrak{l}]$. Let V be a Galois submodule of $A[\mathfrak{l}]$ with $\mathbf{gr}\, V = [\mathbb{F}\, E]$. If q ramifies in $\mathbb{Q}(V)$, then $\overline{M}_t = (\sigma_w - 1)(V)$ is the one-dimensional Galois submodule of V and A is unobstructed. Hence N_V divides pN_E. But then V is split by p-fissility, a contradiction.

We thus have a filtration $0 \subset \mathcal{W}_1 \subset \mathcal{W}_2 \subset \mathcal{W} = A[\mathfrak{l}]$, in which $\mathbf{gr}\, W = [\mathbb{F}\, \mathbb{F}\, E]$ and E cannot move to the left. The $\{p, q\}$-transparency implies that $\mathcal{W}_2$ is a nugget with $\mathbf{gr}\, \mathcal{W}_2 = [\mathcal{Z}_{\mathfrak{l}}\, \boldsymbol{\mu}_{\mathfrak{l}}]$. Since E is p-fissile, q ramifies in $\mathbb{Q}(W/W_1)$, and so q is unramified in $\mathbb{Q}(W_2)$. Hence $\mathbb{Q}(W_2) = \mathbb{Q}(\sqrt{p^*})$, with $p^* \equiv 1\,(8)$. Now $(\sigma_w - 1)(W/W_1) = W_2/W_1$, and so $W_2 = W_1 + \overline{M}_t$ is a trivial $\mathcal{D}_w$-module. Therefore $\chi_{p*}(q) = 1$. □

Proposition 6.3.14. *Suppose* **M4**, $N_A^u = p$ *and* $\mathcal{D}_v$ *acts irreducibly on* E *for* $v \,|\, p$ *in* $\mathbb{Q}(A[\mathfrak{l}^\infty])$. *Unless* $\mathcal{W} \simeq \boldsymbol{\mu}_{\mathfrak{l}}$ *and* $\mathcal{E}_{|\mathbb{Z}_2}$ *is étale, assume that all exact sequences*

$$0 \to \mathcal{W} \to \mathcal{V} \to \mathcal{E} \to 0 \tag{6.3.15}$$

of $\mathbb{F}$*-module schemes over* $\mathbb{Z}_T$ *with* $W \simeq \mathbb{F}$ *are generically split. Then* $p \equiv 1\,(4)$.

Proof. The irreducibility of E as a $\mathcal{D}_v$-module and normality of the cyclic 2-group $\mathcal{I}_v$ imply that $E^{\mathcal{I}_v} = E$, and so p is unramified in $\mathbb{Q}(E)$. Let H be a cyclic odd Hall subgroup of $\mathcal{D}_v(\mathbb{Q}(A[\mathfrak{l}^\infty])$. Then **M3** holds because $E^H = E^{\mathcal{D}_v} = 0$. Since $M_t = M_t(A, v, \mathfrak{l})$ is a pure $\mathcal{D}_v$-module of $\mathfrak{o}$-rank one, $\overline{M_t} \cap \overline{D}_H = 0$ and $C(A) = M_t + D_H$ is a pure $\mathfrak{o}_\mathfrak{l}$-submodule of $\mathbb{T}_\mathfrak{l}(A)$ of rank 3. Assume A is obstructed for the associated mirage.

Suppose $A[\mathfrak{l}] \supset \mathcal{V}$ for an $\mathbb{F}$-module subscheme as in (6.3.15), defined over $\mathbb{Z}_S$ with $S = T \cup \{p\}$. In Lemma 3.2.5, we have $\overline{\delta} = 0$, so $f_p(V) = f_p(E) = 0$. Hence $\mathcal{V}$ extends to an $\mathbb{F}$-module scheme over $\mathbb{Z}_T$. By obstruction, the generic splitting assumption implies that $\mathcal{W} \simeq \boldsymbol{\mu}_\mathfrak{l}$ and $\mathcal{E}_{|\mathbb{Z}_2}$ is étale. Hence $\mathbf{gr}\, A[\mathfrak{l}] = [\boldsymbol{\mu}_\mathfrak{l}\, \mathcal{E}\, \boldsymbol{\mu}_\mathfrak{l}]$. Since $E^* \simeq E$, the splitting assumption allows us to move E to the right, creating Galois submodules $X \supset X_1$ with $\mathbf{gr}\, X = [\mathbb{F}\,\mathbb{F}]$. Since $\overline{M}_t \subseteq X \cap \overline{C}(A)$ and A is obstructed, $X = X_1 + \overline{M}_t$ is not a trivial Galois module and p is unramified in $\mathbb{Q}(X)$. Thus $\mathbb{Q}(X) = \mathbb{Q}(i)$ and $\mathcal{D}_v$ acts on X as an odd order group. This implies our conclusion by Lemma 6.2.7(ii). □

7. Small irreducibles and their extensions

The goal of this section is to make the criteria obtained earlier testable, by reducing the study of large Galois extensions to that of more tractable cyclic extensions of smaller fields with precisely controlled conductors. The Bordeaux tables, Maple and Magma then help with the numerical verifications.

7.1. **Extensions of E by $\mathbb{F}$.** Let $\mathcal{E}$ be a simple $\mathbb{F}$-module scheme whose Galois module E is semistable, self-dual and two-dimensional over $\mathbb{F}$. Let $F = \mathbb{Q}(E)$, $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ and $\ell = \mathrm{char}(\mathbb{F}) \notin T$, where T is the set of bad places of E. Assume also that E remains irreducible as an $\mathbb{F}_\ell[\Delta]$-module (cf. Lemma 4.3.1). As in [45], $\boldsymbol{\mu}_\ell \subseteq F$, since $\det(\rho_E) = \omega$ is the mod-ℓ cyclotomic character, and $\Delta \simeq \rho_E(G_\mathbb{Q})$ is conjugate to a subgroup of

$$\mathrm{R}_2(\mathbb{F}) := \{M \in \mathrm{GL}_2(\mathbb{F}) \mid \det M \in \mathbb{F}_\ell^\times\}.$$

There are *transvections* in Δ, i.e. elements g such that $\mathrm{rank}_\mathbb{F}(g-1) = 1$.

Lemma 7.1.1 ([45], [60]). *We have* $\Delta = \mathrm{R}_2(\mathbb{F})$ *unless:*

i) $\ell = 2$ *and* $\Delta = D_m \subseteq \mathrm{SL}_2(\mathbb{F})$, *with* $\mathbb{F}$ *minimal such that* $|\mathbb{F}| \equiv \pm 1 \bmod m$, *or*

ii) $\ell = 3$, $\Delta = \langle \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ i & 1 \end{smallmatrix}\right] \rangle$ *with* $i \in \mathbb{F}_9$ *and* $i^2 = -1$. *Then* $\Delta \cap \mathrm{SL}_2(\mathbb{F}_9)$ *is isomorphic to* $\mathrm{SL}_2(\mathbb{F}_5)$.

Lemma 7.1.2. *We have* $H^j(\Delta, E) = 0$ *for all* $j \geq 0$, *unless* $\ell = 2$ *and* $|\mathbb{F}| \geq 4$.

Proof. Each Δ contains a non-trivial normal subgroup Γ of order prime to ℓ. Since E is irreducible, $E^\Gamma = E^\Delta = 0$. We have $H^k(\Gamma, E) = 0$ for $k \geq 1$ and conclude thanks to the inflation-restriction sequence for $j \geq 1$ that

$$0 = H^j(\Delta/\Gamma, E^\Gamma) \to H^j(\Delta, E) \to H^j(\Gamma, E)^{\Delta/\Gamma} = 0. \qquad \square$$

In this subsection, assume $H^1(\Delta, \widehat{E}) = 0$. For $S \supseteq T$, suppose $\mathcal{V}$ is an $\mathbb{F}$-module scheme over $\mathbb{Z}_S$ such that the following sequence is *not* generically split:

$$0 \to \mathcal{V}_1 \to \mathcal{V} \to \mathcal{E} \to 0, \tag{7.1.3}$$

where $\mathcal{V}_1 = \mathcal{Z}_{\mathfrak{l}}$ or $\mathbb{F} = \mathbb{F}_2$ and $\mathcal{V}_1 = \boldsymbol{\mu}_2$. Set $L = \mathbb{Q}(V)$ and $G = \mathrm{Gal}(L/\mathbb{Q})$. Then V affords a matrix representation:

$$\rho_V(g) = \begin{bmatrix} 1 & x_g \; y_g \\ 0 & \rho_E(g) \end{bmatrix} \in \mathrm{GL}_3(\mathbb{F}), \tag{7.1.4}$$

where (x_g, y_g) is viewed as an element of $\widehat{E} = \mathrm{Hom}_{\mathbb{F}}(E, \mathbb{F}) \simeq \mathbb{F} \oplus \mathbb{F}$. The class $[c]$ in $H^1(G, \widehat{E})$ associated to (7.1.3) does not vanish, even when restricted to

$$H^1(\mathrm{Gal}(L/F), \widehat{E})^{\Delta} = \mathrm{Hom}_{\mathbb{F}_\ell[\Delta]}(\mathrm{Gal}(L/F), \widehat{E}).$$

By irreducibility of E over $\mathbb{F}_\ell$, $\mathrm{res}[c] : \mathrm{Gal}(L/F) \to \widehat{E}$ is an isomorphism of $\mathbb{F}_\ell[\Delta]$-modules and so G is a semidirect product

$$G \simeq \mathrm{Gal}(L/F) \rtimes \mathrm{Gal}(F/\mathbb{Q}) \simeq \left[\begin{smallmatrix} 1 & \widehat{E} \\ 0 & I \end{smallmatrix}\right] \rtimes \left[\begin{smallmatrix} 1 & 0 \\ 0 & \Delta \end{smallmatrix}\right].$$

We describe a subfield F_1 of F and an extension L_1/F_1, such that L is the Galois closure of $L_1/\mathbb{Q}$. Since any ℓ-Sylow subgroup P of Δ fixes a line in E pointwise, assume P is contained in $\Delta_1 = \Delta \cap \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. Let

$$F_1 = F^{\Delta_1}, \; G_1 = \mathrm{Gal}(L/F_1) = G \cap \left[\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & * \end{smallmatrix}\right], \; N_1 = G \cap \left[\begin{smallmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & * \end{smallmatrix}\right] \text{ and } L_1 = L^{N_1}.$$

Then $\det\colon \Delta_1/P \simeq \mathbb{F}_\ell^\times$, N_1 is normal in G_1 and $G_1/N_1 \simeq \mathbb{F}$. If $F_1 \subset L_2 \subseteq L_1$, the Galois closure of $L_2/\mathbb{Q}$ is L by irreducibility of E as an $\mathbb{F}_\ell[\Delta]$-module.

Lemma 3.2.5 shows that $\mathcal{V}$ extends to a finite flat group scheme over $\mathbb{Z}_{S'}$, where

$$S' = T \cup \{p_v \in S \backslash T \mid E \text{ is not irreducible as an } \mathbb{F}[\mathcal{D}_v(F/\mathbb{Q})]\text{-module}\},$$

and so we tacitly assume $S = S'$. Write $\mathfrak{c}_\infty$, $\mathfrak{c}_\ell$ and $\mathfrak{c}_p$ for the semilocal components of the ray class conductor of L_1/F_1 at the places over ∞, ℓ and $p \neq \ell$ respectively.

Lemma 7.1.5. *We have the following bounds on the conductor* $\mathfrak{c}(L_1/F_1)$*:*

i) $\mathfrak{c}_p$ *divides* p *if* p *is in* $S\backslash T$ *and* $\mathfrak{c}_p = 1$ *for other* $p \neq \ell$.
ii) $\mathfrak{c}_\infty = 1$ *unless* F_1 *is totally real, when* $\mathfrak{c}_\infty$ *is the product of its infinite places.*
iii) $\mathfrak{c}_{\mathfrak{l}} = 1$ *when* $\mathcal{V}_1 = \mathcal{Z}_{\mathfrak{l}}$.

Proof. Let v be a prime of L ramifying in L_1/F_1. If $p_v \neq \ell$ is in $S\backslash T$, then v is tame, with conductor exponent one. If v lies over $T \cup \{\ell\}$, Lemma 3.3.10 implies that $\mathcal{I}_v(L/F) = 0$. Thus $\mathcal{I}_v(L/F_1)$ contains an element σ_v of order ℓ, not trivial on L_1, such that $\rho_E(\sigma_v) \neq 1$. It follows that $\rho_V(\sigma_v) = \left[\begin{smallmatrix} 1 & x & y \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right]$ with $xa \neq 0$, and so $(\sigma_v - 1)^2(V) \neq 0$.

If v lies over T, this contradicts semistability. If v lies over ℓ, then σ_v acts wildly on E, ruling out the possibility that $\mathcal{E}_{|\mathbb{Z}_\ell}$ is biconnected. Hence $\mathbf{gr}\,\mathcal{E}_{|\mathbb{Z}_\ell} = [\boldsymbol{\mu}_{\mathfrak{l}}\, \mathcal{Z}_{\mathfrak{l}}]$ in the filtration induced by our fixed basis for V and $\mathbf{gr}\,\mathcal{V}_{|\mathbb{Z}_\ell} = [\mathcal{Z}_{\mathfrak{l}}\, \boldsymbol{\mu}_{\mathfrak{l}}\, \mathcal{Z}_{\mathfrak{l}}]$. But inertia acts tamely on $\boldsymbol{\mu}_{\mathfrak{l}}$, contradicting $x \neq 0$.

Suppose $\ell = 2$ and F_1 has a complex place, whence F is totally complex. If σ_v is complex conjugation for v lying over a real place of F_1, then $\rho_E(\sigma_v) \neq 1$. But σ_v fixes F_1, and so $\rho_V(\sigma)$ is upper triangular. If v were ramified in L_1/F_1, we would have the same contradiction as for v over T, since $\sigma_v^2 = 1$. $\square$

For the rest of this section, assume $\mathbb{F} = \mathbb{F}_2$, so $\ell = 2$, $\Delta \simeq \mathrm{SL}_2(\mathbb{F}_2)$ and F_1 is a cubic field. Moreover, $E \simeq \widehat{E}$ as Galois modules, $H^1(\Delta, E) = 0$ and $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathcal{S}_4$.

Define the prime $\lambda_1 \,|\, 2$ in F_1 according to the factorization of $(2)\mathcal{O}_{F_1}$:

$$(2)\mathcal{O}_{F_1} = \begin{cases} \lambda_1^3 & \text{if } e_{\lambda_1}(F_1/\mathbb{Q}) = 3, \\ \lambda_1^2\lambda_1' & \text{if } e_{\lambda_1}(F_1/\mathbb{Q}) = 2, \\ \lambda_1\lambda_1' & \text{if } f_{\lambda_1}(F_1/\mathbb{Q}) = 2. \end{cases} \tag{7.1.6}$$

Lemma 7.1.7. *If $\mathcal{V}_1 = \boldsymbol{\mu}_2$ in (7.1.3), then $\mathfrak{c}_2(L_1/F_1)$ divides 4. It even divides λ_1^2 if: (i) 2 ramifies in $F/\mathbb{Q}$ or (ii) $f_\lambda(F/\mathbb{Q}) = 2$ and $\mathcal{E}^m \neq 0$ over $\mathbb{Z}_2$.*

Proof. Conductors of small extensions of $\mathbb{Q}_2$ may be found by direct calculation or in the Tables of [26], where the last entry of the *Galois Slope Content* is at most 2 exactly when the higher ramification bound in Lemma 3.3.2 holds.

Assume λ ramifies in L/F. If $\mathcal{E}_{|\mathbb{Z}_2}$ is biconnected, $\mathcal{D}_\lambda(L/\mathbb{Q}) \simeq \mathcal{S}_4$ and $\mathcal{I}_\lambda(L/\mathbb{Q}) \simeq \mathcal{A}_4$. By [26] for sextics over $\mathbb{Q}_2$, we have $\mathrm{ord}_2(d_{L_1/\mathbb{Q}}) = 6$, whence $\mathfrak{c}_2(L_1/F_1) = \lambda_1^2$ by the conductor-discriminant formula. The end of the proof of Lemma 7.2.3 gives an explicit description of the completion L_λ.

When $\mathcal{I}_\lambda(L/\mathbb{Q})$ is a 2-group, Lemma 3.3.2 implies that $\mathcal{I}_\lambda(L/\mathbb{Q})_2 = 1$. Passing between lower numbering for subgroups and upper numbering for quotients, we find that $\mathcal{I}_\lambda(L_1/F_1)_2 = 1$, and so the conductor exponent of L_1/F_1 at λ is 2 by [55, Ch. XV, §2, Cor. 2].

Now assume (i) with $e_\lambda(F/\mathbb{Q}) = 2$, or (ii). Fix the primes λ and λ' of L over λ_1 and λ_1'. Since λ_1' splits in $F_1/\mathbb{Q}$, $\mathcal{D}_{\lambda'}(L/\mathbb{Q})$ is contained in G_1. The non-trivial action of $\mathcal{D}_{\lambda'}(F/\mathbb{Q})$ on our basis for V implies that $\mathbf{gr}\, V = [\boldsymbol{\mu}_2\, \boldsymbol{\mu}_2\, \mathcal{Z}_2]$ at λ'. But then $\mathcal{I}_{\lambda'}(L/\mathbb{Q}) \subset N_1$, so is trivial on L_1. Thus λ_1' is unramified in L_1/F_1 and $\mathfrak{c}_2(L_1/F_1)$ divides λ_1^2. □

Lemma 7.1.8. *Let L_1 be a sextic field whose Galois closure L is an $\mathcal{S}_4$-field with F as its $\mathcal{S}_3$-subfield. If L/F is unramified over 2 and one of the following holds for $\lambda \,|\, 2$, then $|\mathcal{D}_\lambda(L/F)| = 2$:*

i) *$e_\lambda(F/\mathbb{Q}) = 2$ and there are exactly 3 primes over 2 in L_1, or*
ii) *$e_\lambda(F/\mathbb{Q}) = 1$, $f_\lambda(F/\mathbb{Q}) = 2$ and there are exactly 2 primes over 2 in L_1.*

Proof. A 2-Sylow subgroup G_1 of $G = \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathcal{S}_4$ cuts out the cubic subfield F_1, and the subgroup N_1 generated by the two transpositions in G_1 cuts out L_1. The subgroup κ of G generated by the even involutions cuts out F. Write λ, λ' for primes of L over λ_1, λ_1' respectively. Then $\mathcal{D}_{\lambda'}(L/\mathbb{Q})$ is contained in G_1 because λ_1' is split in $F_1/\mathbb{Q}$.

If $\mathcal{D}_\lambda(L/F) = 1$, then $\mathcal{D}_\lambda(L/\mathbb{Q})$ has order 2 and is not trivial on F, so it is generated by a transposition. Thus $\mathcal{D}_\lambda(L/F_1) = \mathcal{D}_\lambda(L/L_1)$ and the two primes above 2 in F_1 split into 4 in L_1.

Suppose there is a residue extension over 2 in L/F, so $\mathcal{D}_{\lambda'}(L/\mathbb{Q})$ has order 4.

i) If $e_{\lambda'}(F/\mathbb{Q}) = 2$, then $\mathcal{I}_{\lambda'}(L/\mathbb{Q})$ is generated by a transposition $\sigma_{\lambda'}$. Hence $\mathcal{D}_{\lambda'} = N_1$ and λ_1' splits in L_1/F_1. Let $\lambda = \gamma(\lambda')$, with $\gamma \in G$ of order 3. Then $\mathcal{D}_\lambda(L/F) \cap N_1 = 1$, and so λ_1 is inert in L_1/F_1.
ii) If $f_{\lambda'}(F/\mathbb{Q}) = 2$, then $\mathcal{D}_{\lambda'}(L/\mathbb{Q})$ is cyclic, generated by a Frobenius and so $\mathcal{D}_{\lambda'}(L/\mathbb{Q}) \cap N_1$ is generated by the unique even involution in N_1. It follows that λ_1' is inert in L_1/F_1. Conjugating by γ, we find that $\mathcal{D}_\lambda(L/\mathbb{Q}) \cap N_1 = 1$. Hence λ_1 also is inert in L_1/F_1. □

Remark 7.1.9. Let A be a hypothetical $(\mathfrak{o}, N)$-paramodular variety with $|\mathbb{F}_\mathfrak{l}| = 2$ and $\mathfrak{S}_\mathfrak{l}(A) = \{E\}$, where $\dim_{\mathbb{F}_2} E = 2$. Then N_E is a squarefree divisor of N and the $\mathcal{S}_3$-field $F = \mathbb{Q}(E)$ can be constructed by class field theory or Magma, as a cyclic cubic over $\mathbb{Q}(\sqrt{\pm N_E})$, ramified only over 2∞, with $F_1/\mathbb{Q}$ as a cubic subfield.

Let S contain the set T of primes dividing N_E. If no quadratic L_1/F_1 satisfies the bounds in Lemma 7.1.5, then $r_E(S) = 0$ and extensions (7.1.3) over $\mathbb{Z}_S$ with $\mathcal{V}_1 \simeq \mathcal{Z}_2$ are generically split. Lemma 4.4.5 controls the deficiency $\delta_A(E)$ in Theorem 5.3. When $r_E(S) = 0$ and 2 ramifies in F, E is $(S\backslash T)$-transparent. When $r_E(S) = 0$ and 2 is unramified in F, with residue degree 2, we get only $\delta_A(E) \leq 1$, due to the fickle nature of group schemes $\mathcal{E}$ corresponding to E. If only one quadratic extension L_1/F_1 satisfies the conductor bound, then $r_E(T) = 1$, as required by **D**3 in §4.4. Lemma 7.1.8 serves for testing **D**4.

Now retain the bounds in Lemma 7.1.5(i),(ii) at odd places, but invoke the weaker bounds on $\mathfrak{c}_2(L_1/F_1)$ in Lemma 7.1.7. When no quadratic L_1/F_1 exists, $r_E^{cr}(S) = 0$ and E is $(S\backslash T)$-fissile. Further, under 7.1.7(ii), the splitting required in Proposition 6.3.14 holds. Finally, $r_E^{cr}(S) = 1$ if exactly one quadratic L_1/F_1 exists.

7.2. **Extensions of E_2 by E_1.** Here $|\mathbb{F}_\mathfrak{l}| = 2$ and $\mathfrak{S}_\mathfrak{l}^{all}(A) = \{E_1, E_2\}$ with E_i two-dimensional non-isomorphic Galois modules and $\operatorname{cond}(E_i) = N_i$. By Corollary 6.1.3, we may assume that $W = A[\mathfrak{l}]$ is a non-split extension:

$$0 \to E_1 \to W \to E_2 \to 0. \tag{7.2.1}$$

For $i = 1, 2$, set $F_i = \mathbb{Q}(E_i)$, $F = \mathbb{Q}(E_1, E_2) = F_1F_2$ and $\Delta_i = \operatorname{Gal}(F/F_{3-i}) \simeq \operatorname{Gal}(F_i/\mathbb{Q}) \simeq \operatorname{SL}_2(\mathbb{F}_2)$, so $\operatorname{Gal}(F/\mathbb{Q}) = \Delta_1 \times \Delta_2$. Let $L = \mathbb{Q}(W)$ and $G = \operatorname{Gal}(L/\mathbb{Q})$.

Lemma 7.2.2. *L contains F properly.*

Proof. As Δ_1-modules, $E_2 \simeq \mathbb{F}_2^2$ and $\mathcal{H} = \operatorname{Hom}_{\mathbb{F}_2}(E_2, E_1) \simeq E_1^2$. Assume $L = F$ and use inflation-restriction for exactness of the sequence

$$H^1(\operatorname{Gal}(F_2/\mathbb{Q}), \mathcal{H}^{\Delta_1}) \to H^1(\operatorname{Gal}(F/\mathbb{Q}), \mathcal{H}) \to H^1(\Delta_1, \mathcal{H}).$$

The first term vanishes since $\mathcal{H}^{\Delta_1} \simeq \operatorname{Hom}_{\mathbb{F}_2[\Delta_1]}(E_2, E_1) = 0$ and the last because $H^1(\Delta_1, E_1) = 0$. Thus the middle term is trivial and (7.2.1) splits. □

Let ρ_i be the Galois representation afforded by E_i, fix a basis w_1, w_2 for E_1 and extend by w_3, w_4 to a basis for W. Then G admits a representation of the form

$$\rho : g \mapsto \begin{bmatrix} \rho_1(g) & B(g) \\ 0 & \rho_2(g) \end{bmatrix}.$$

Conjugation by $\left[\begin{smallmatrix} X & Z \\ 0 & Y \end{smallmatrix}\right]$ on $\left[\begin{smallmatrix} I & B \\ 0 & I \end{smallmatrix}\right]$ in $\operatorname{Gal}(L/F)$ yields $\left[\begin{smallmatrix} I & XBY^{-1} \\ 0 & I \end{smallmatrix}\right]$. Since $M_{2\times 2}(\mathbb{F}_2)$ is $\mathbb{F}_2[\Delta_1 \times \Delta_2]$-irreducible, ρ maps onto the parabolic subgroup indicated above.

Let H be the 2-Sylow subgroup of G whose image under ρ is the group of all unipotent upper triangular matrices. Its fixed field $K = L^H$ is the compositum of the cubic fields $K_i = K \cap F_i$. Let J be the subgroup of H with $B(g)$ upper triangular. Then $L_0 = L^J$ is a quadratic extension whose Galois closure over $\mathbb{Q}$ is L. Let $\mathfrak{c}_2$ be the 2-part of the ray class conductor of L_0/K. Write N_1N_2Q for the Artin conductor of W and let Q_0 be the part of Q prime to N_1N_2.

Lemma 7.2.3. *The extension L_0/K is unramified outside $2\infty Q_0$ and ramifies at ∞ only if F is totally real. Assume that $\mathcal{E}_2$ is biconnected at 2.*

i) *If $\mathcal{E}_1$ is biconnected at 2, then $2\mathcal{O}_K = (\lambda_K\lambda_K')^3$ and $\mathfrak{c}_2$ divides $(\lambda_K\lambda_K')^2$.*
ii) *If $\mathcal{E}_1$ at 2 is a non-split extension of $\mathcal{Z}_2$ by $\boldsymbol{\mu}_2$, then $\mathfrak{c}_2$ divides λ_K^2, where λ_K is the unique prime of K with $[K_{\lambda_K} : \mathbb{Q}_2] = 6$. The other prime over 2 splits.*

Proof. At an archimedean or odd place v of L ramified in L/K, the inertia group $\mathcal{I}_v(L/K)$ inside $\mathrm{Gal}(L/K)$ is generated by an involution σ, as in Lemma 6.2.6. If v ramifies in L_0/K, then σ does not fix L_0, so $c = 1$ and thus $x = y = 0$. Hence v does not ramify in $F/\mathbb{Q}$. It follows that either v lies over Q_0 or v is archimedean and F is totally real.

Let π be a root of $x^3 - 2$ in $\overline{\mathbb{Q}}_2$. In (i), we have $2\mathcal{O}_K = (\lambda_K \lambda_K')^3$, since $F_i \otimes \mathbb{Q}_2 \simeq \mathbb{Q}_2(\boldsymbol{\mu}_3, \pi)$. The bound on $\mathfrak{c}_2$ is in [51, Prop. 6.4].

For (ii), let λ' be a prime of L with $K_{\lambda'} = \mathbb{Q}_2(\pi)$. Then the completion of K_1 at λ' is $\mathbb{Q}_2$ and $\mathcal{D}_{\lambda'}(F_1/K_1) = \mathrm{Gal}(F_1/K_1)$ has order 2. Hence the connected component E_1^0 at λ' is the subspace $\langle w_1 \rangle$. For any σ in $H = \mathrm{Gal}(L/K)$, we have $(\sigma - 1)(w_3) \in E_1$. If, in addition, σ is in $\mathcal{D}_\lambda(L/K)$, then $(\sigma - 1)(W) \subseteq W^0$ because W^{et} is one-dimensional. Hence $(\sigma - 1)(w_3)$ is in $W^0 \cap E_1 = E_1^0 = \langle w_1 \rangle$, so σ is in J and λ' splits in L_0/K.

Suppose λ over 2 in L ramifies in L_0/K and let W^0 be the connected component at λ. Then $K_\lambda = \mathbb{Q}_2(\pi, \sqrt{d})$ with $d \in \{-1, 3, -3\}$ and $\mathbb{Q}_2(W^0)$ is the unique $\mathcal{S}_4$-field M over $\mathbb{Q}_2$ satisfying Fontaine's bound (cf. [26]). Explicitly,

$$M = \mathbb{Q}_2(\zeta, \pi, \sqrt{1 + 2\pi^2}, \sqrt{1 + 2\zeta\pi^2}),$$

with ζ a primitive cube root of unity. Further, $\mathcal{D}_\lambda \simeq \mathcal{S}_4 \times \mathcal{S}_2$ if 2 ramifies in F_1 and $\mathcal{D}_\lambda \simeq \mathcal{S}_4$ otherwise.

We use tildes for the completion of various fields at λ. If $d \equiv 3 \bmod 4$, then $\tilde{F} = \tilde{K}(\zeta) = \mathbb{Q}_2(\pi, \zeta, i)$ and $\tilde{L} = M(i)$. The abelian conductor exponents of $\tilde{L}_0/\tilde{K}$ and $\tilde{L}_0\tilde{F}/\tilde{F}$ are equal since $\tilde{F}/\tilde{K}$ is unramified. Local class field theory or the conductor-discriminant formula implies that every quadratic extension of $\tilde{F}$ inside $\tilde{L} = \tilde{F}(\sqrt{1 + 2\pi^2}, \sqrt{1 + 2\zeta\pi^2})$ has conductor exponent 2. Hence $\mathfrak{c}_2$ divides λ_K^2, where λ_K lies below λ in K.

If $d = -3$, then $\tilde{L} = M$, $\tilde{K} = \mathbb{Q}_2(\zeta, \pi)$ and the same method applies. □

7.3. **Wherein $A[\mathfrak{l}]$ is irreducible and $|\mathbb{F}_\mathfrak{l}| = 2$.** Let A be a semistable $(\mathfrak{o}, N)$-paramodular abelian variety with odd N and S the set of primes dividing N. Suppose $\mathfrak{l}$ has a totally positive generator and $E = A[\mathfrak{l}]$ is irreducible. We may assume A is minimally $\mathfrak{o}$-polarized. Then $\mathcal{E}$ is Cartier self-dual by Lemma 3.4.7(ii) and E is symplectic.

Let $F = \mathbb{Q}(E)$ and $G = \mathrm{Gal}(F/\mathbb{Q}) \subseteq \mathcal{S}_6$, via the induced action on the set Θ^- of six odd theta characteristics [8, §2, §4]. When N is not a perfect square, G can only be $\mathcal{S}_5$, $\mathcal{S}_6$ or the wreath product $\mathcal{S}_3 \wr \mathcal{S}_2$. The last is a group of order 72, isomorphic to the orthogonal group $\mathrm{O}_4^+(\mathbb{F}_2)$, as in [38, p. 409]. The field F is the Galois closure of a subfield K of degree 5 or 6 fixed by the stabilizer of an odd theta. Let d_K be the absolute discriminant of K. See [8, Prop. 4.1] for $\mathrm{ord}_2(d_K)$. For odd p, [8, Prop. 3.11] gives $\mathrm{ord}_p(d_K)$ in terms of the toroidal dimensional of the special fiber; cf. Notation 3.2.2.

Proposition 7.3.1. *We have* $\mathrm{ord}_p(d_K) = t_p$, *unless* $t_p = 2$ *and* $[K:\mathbb{Q}] = 6$, *when* $2 \le \mathrm{ord}_p(d_K) \le 3$. *In addition,* $\mathrm{ord}_2(d_K) \le 6$ *if* $[K:\mathbb{Q}] = 6$ *and* $\mathrm{ord}_2(d_K) \le 4$ *if* $[K:\mathbb{Q}] = 5$.

Lemma 7.3.2. *No prime over* 2 *in* K *has residue degree* 5. *If* $[K:\mathbb{Q}] = 5$, *then no prime over* 2 *in* K *has residue degree* 3.

Proof. If the residue degree $f_\lambda(K) = 5$, then 2 is unramified in K and so in F. Hence $\mathcal{E}_{|\mathbb{Z}_2}$ is ordinary and the connected-étale sequence implies that the order of $\mathcal{D}_\lambda(F/\mathbb{Q})$ divides 48, a contradiction.

If $f_\lambda(K) = 3$, then $e_\lambda(K) \le 2$ and again $\mathcal{E}_{|\mathbb{Z}_2}$ is ordinary. Any element Φ of order 3 in $\mathcal{D}_\lambda(F/\mathbb{Q})$ is fixed point free on E^0 and on E^{et}, so also on E. But if $[K:\mathbb{Q}] = 5$, then Φ fixes three odd thetas pointwise and the difference of any two corresponds to a fixed point for the action of Φ on E. □

Remark 7.3.3. Let N be the conductor of E and let K be a sextic field, as above. Write $N = N_1 N_2^2 N_3^2$, where the involutions generating inertia above $p \,|\, N_i$ are the product of i transpositions in $\mathcal{S}_6$. Then the discriminant of K divides $2^6 N_1 N_2^2 N_3^3$. The discriminant of its *twin field* [49], whose representation is twisted by the outer automorphism of $\mathcal{S}_6$, divides $2^8 N_1^3 N_2^2 N_3$, because one has weaker control at primes over 2, while products of 1 and 3 transpositions are switched. When both discriminants exceed 200,000, a totally complex field K *might* exist and lie beyond the tables in [10]. The conductors $N < 1000$ for which this issue arises are $5^2 \cdot N_1$ with $29 \le N_1 \le 39$, $7^2 \cdot N_1$ with $11 \le N_1 \le 19$ and $11^2 \cdot 7$, all with $N_2 = 1$. The solvable case $\mathcal{S}_3 \wr \mathcal{S}_2$ does not occur by class field theoretic calculation. John Jones kindly verified, with his targeted searches, that no such $\mathcal{S}_6$ field exists either.

Appendix A. How conductors are ruled out

Assume $\mathfrak{o}$ has a prime $\mathfrak{l} \,|\, 2$ of degree one. For each odd integer $N < 1000$, we considered all Galois structures available for $A[\mathfrak{l}]$ when A is a semistable $(\mathfrak{o}, N)$-paramodular abelian variety of reduced conductor N. We examine in detail the various possibilities for $\mathfrak{S}_\mathfrak{l}(A)$, the multiset of irreducible constituents of $A[\mathfrak{l}]$ of dimension at least 2 over $\mathbb{F}_2$. We say that a given multiset is ruled out for N if no such A exists.

I. $\mathfrak{S}_\mathfrak{l}(A)$ is empty. Then $\mathrm{Gal}(\mathbb{Q}(A[2])/\mathbb{Q})$ is a 2-group. All odd $N < 1000$, except those marked **u** in Table 1, are ruled out by Corollaries 5.4, 5.5(ii)b and the criteria in §6.2. The Jacobian of $y^2 = (x^2 + 2x + 5)(x^4 + 2x^3 + 3x^2 - 2x + 1)$ is of type **u** with the least conductor $N = 1649 = 17 \cdot 97$ known to us.

II. $\mathfrak{S}_\mathfrak{l}(A) = \{E\}$, with $\dim E = 2$. Set $F = \mathbb{Q}(E)$ and denote residue and ramification degree at $\lambda \,|\, 2$ by f_λ and e_λ respectively. See Remark 7.1.9 regarding the relevant invariants.
   A. 2 ramifies in F. We have $\delta(E) = 0$ for 92 cases with $e_\lambda(F/\mathbb{Q}) = 3$ and 64 cases with $e_\lambda(F/\mathbb{Q}) = 2$. Then Theorem 5.3 rules out N_E and qN_E when $q \equiv \pm 3 \bmod 8$ is prime. Corollary 5.5(i)c rules out $q^2 N_E$ when $r_E(T \cup \{q\}) = 0$. Nine more cases with $e_\lambda(F/\mathbb{Q}) = 3$ are ruled out by Proposition 6.3.11(i). We also use Lemma 4.4.11 and Theorem 5.3 to eliminate N_E when $e_\lambda(F/\mathbb{Q}) = 2$
   B. 2 is unramified in F. Lemma 3.1.5 precludes existence if $f_\lambda(F/\mathbb{Q}) = 3$. Proposition 6.3.11(ii) rules out 431 and 503, the only conductors available for E if $f_\lambda(F/\mathbb{Q}) = 1$. Finally, consider $f_\lambda(F/\mathbb{Q}) = 2$. Rule out N_E by Lemma 4.4.5(ii) and Theorem 5.3 for the 24 cases with $r_E(T) = 0$ and by Lemma 4.4.10 for the 7 cases with $r_E(T) = 1$. Use Proposition 6.3.14 for some pN_E.

III. $\mathfrak{S}_{\mathfrak{l}}(A) = \{E_1, E_2\}$ with $\dim E_i = 2$ and $F_i = \mathbb{Q}(E_i)$.
   A. Suppose at least one of the F_i is ramified at 2. When $N = N_{E_1} N_{E_2}$, we use Lemma 7.2.3 and Corollary 6.1.3 to eliminate all but three cases. For those, we know examples labeled "Prym" in Table 2. One rules out $N = pN_{E_1}N_{E_2}$, with p inert in F_1 and F_2, by Remark 3.2.4, even when $E_1 \simeq E_2$. This happens for $N = 3{\cdot}11^2$, $5{\cdot}11^2$ and $3{\cdot}11{\cdot}19$.
   B. Suppose F_1 and F_2 are unramified at 2. Locally at 2, the associated group schemes must be étale or multiplicative and so are Cartier duals. The only case available is $N = 713 = 23 \cdot 31$, for which we know two isogeny classes of Jacobians in Table 2.

IV. $\mathfrak{S}_{\mathfrak{l}}(A) = \{E\}$ with $\dim E = 4$. The criteria in §7.3 are given in terms of a *stem field*, i.e. a subfield K of $\mathbb{Q}(E)$ whose Galois closure is $\mathbb{Q}(E)$.
   A. Thirteen quintic fields are candidates for K. Each has Galois group $\mathcal{S}_5$ and is determined by its conductor N_E. The single case of the form $qN_E \leq 1000$ is $3{\cdot}277$ and is ruled out by Remark 3.2.4.
   B. The only candidates for a sextic K are three $\mathcal{S}_3 \wr \mathcal{S}_2$-fields and four $\mathcal{S}_6$-fields.

Table 1 lists all odd integers N which were not eliminated by our criteria and are *not* conductors of known semistable surfaces.

Notation A.1.

i) **u** means $A[\mathfrak{l}]$ is prosaic; that is, $\mathfrak{S}_{\mathfrak{l}}^{all}(A) = \{\mathbb{F}, \mathbb{F}, \mathbb{F}, \mathbb{F}\}$, with $\mathbb{F} = \mathbb{F}_2$.
ii) Boldface integers are the Artin conductors of any two-dimensional constituents.
iii) **q** means $\mathfrak{S}_{\mathfrak{l}}^{all}(A) = \{E\}$ for an irreducible, symplectic E with $\mathrm{Gal}(\mathbb{Q}(E)/\mathbb{Q})$ isomorphic to $\mathcal{S}_5$ and quintic stem field for $\mathbb{Q}(E)$.
iv) **wr72** or $\boldsymbol{\mathcal{S}_6}$ means $\mathfrak{S}_{\mathfrak{l}}^{all}(A) = \{E\}$ for an irreducible symplectic E, with sextic stem field for $\mathbb{Q}(E)$ and $\mathrm{Gal}(\mathbb{Q}(E)/\mathbb{Q}) \simeq \mathcal{S}_3 \wr \mathcal{S}_2$ or $\boldsymbol{\mathcal{S}_6}$ respectively.

Table 1. Hypothetical semistable odd conductors not eliminated.

N	WHY	N	WHY	N	WHY	N	WHY	N	WHY
415	**83**	613	**q**	687	**229**	847	**11, 11**	921	**307**
417	**139**	615	**u**	695	**139**	849	**283**	927	**wr72**
531	**59**	629	**37**	697	**u**	853	**q**	957	**11**
535	**107**	637	**91**	735	**u**	859	**859**	961	**31,31**
547	**q**	645	**43**	747	**83**	873	**u**	963	**107**
571	**571**	649	**59**	749	**107**	885	**59**	969	**u**
581	**83**	657	**u**	767	**59**	897	**u**	985	**197**
591	**197**	663	**u**	775	**u**	903	**43**	989	**43**
595	**u**	669	**223**	777	**u, 37**	913	**83**	991	**q**
599	**q**	677	**q**	841	**29, 29**	917	**131**	993	**331**

We could not eliminate semistable W's of Artin conductor $N = 657$, 775 and 847 because $W \simeq B[2]$ for a *non*-semistable surface B of that conductor in Table 2. For most other conductors N in Table 1, there are semistable abelian surfaces B whose conductor is a proper multiple of N with $W \simeq B[2]$.

Only 903 and 969 in Table 1 should be conductors of surfaces under our conjectures and data in [40]. There should also exist four-dimensional abelian varieties with $\mathfrak{o} = \mathbb{Z}[\sqrt{2}]$ and reduced conductors 637, 645 and 927 and a six-dimensional abelian variety of reduced conductor 991 with $\mathfrak{o}$ the maximal order of the cubic field of discriminant 148. Taking $\mathfrak{l}$ as the prime of degree one over 2 in those cases is consistent with the corresponding entries in Table 1.

Odd square conductors $N < 841$ do not appear in Table 1, thanks to Schoof:

Theorem A.2 ([52–54])**.** *Any $\mathbb{Q}$-simple semistable abelian variety with good reduction outside the odd square-free integer $n \leq 23$ is isogenous to $J_0(n)$.*

This should hold for $n = 29$ and 31. His proof for 23 probably applies to 31.

Appendix B. Abelian surfaces of odd conductor < 1000

Table 2 gives one member of each isogeny class of paramodular abelian *surfaces* of odd conductors below 1000 known to us and found by purely *ad hoc* methods. The "INFO" column uses Notation A.1. In general, our methods rule out all other possibilities for $\mathfrak{S}_{\mathfrak{l}}^{\mathrm{all}}(A)$. Most examples are semistable, except for those labeled "notSS". If a polynomial $f(x)$ is given, then the surface is the Jacobian of the curve $y^2 = f(x)$. Analogous tables for even conductors will appear in [40].

Let $C_{/\mathbb{Q}}$ be a curve and $\mathcal{C}$ a global integral model over $\mathbb{Z}$. We have *mild* reduction at p if $\mathcal{C}$ is bad at p, but the Néron model of $J(C)$ is not. Assume that C is given by the *non*-minimal model

$$C\colon\ y^2 + (ma_1 s + m^2 a_3)y = ma_0 s^3 + m^2 a_2 s^2 + m^3 a_4 s + m^4 a_6,$$

where m is an integer, s is a quadratic polynomial in $\mathbb{Z}[x]$, étale mod m, a_0 is an integer prime to m and all other a_i are linear in $\mathbb{Z}[x]$. If the discriminant of C is $m^{22}n$ with n prime to m, then the prime divisors of m are of mild reduction. The converse can be deduced by strong approximation from [28]. In Table 2, such a curve is indicated by the symbol "mild@m" and the conductor of its Jacobian is in the first column.

If X is a curve of genus three with a degree two cover of a genus one curve C, then the kernel $\mathrm{Prym}(X/C)$ of the natural projection $\pi\colon J(X) \to J(C)$ is an abelian surface with (1,2)-polarization. Its conductor is the quotient of that of $J(X)$ by that of $J(C)$. The surfaces of conductors 561, 665, 737 are such Pryms. They are *not* $\mathbb{Q}$-isogenous to Jacobians and will be described in a note [9] on abelian surfaces of polarization (1,2).

Let E be an elliptic curve, defined over $k = \mathbb{Q}(\sqrt{d})$, of conductor $\mathfrak{c}$ and not isogenous to its conjugate. Then the Weil restriction $S = R_{k/\mathbb{Q}}E$ is a surface of paramodular type with conductor $d^2 N_{k/\mathbb{Q}}(\mathfrak{c})$ (see [31]). The surfaces of conductors $657 = 3^2 \cdot 73$ and $775 = 5^2 \cdot 31$ are Weil restrictions of curves defined over $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{5})$, respectively. It is expected that elliptic curves over real fields should correspond to parallel weight 2 Hilbert modular forms. In [25], such Hilbert modular eigenforms over real quadratic fields are lifted to paramodular forms when Remark 1.3(iii) applies. This supports our conjecture, with expected level, for Weil restrictions of "Hilbert modular elliptic curves". For imaginary quadratic fields, work of Cremona and his students combined with [63] suggests modularity there as well.

TABLE 2. Paramodular abelian surfaces of ODD conductor < 1000.

N	EQUATION	INFO
249	$x^6 + 4x^5 + 4x^4 + 2x^3 + 1$	**83**
277	$x^6 + 2x^5 + 3x^4 + 4x^3 - x^2 - 2x + 1$	**q**
295	$x^6 - 2x^3 - 4x^2 + 1$	**59**
349	$x^6 - 2x^5 + 3x^4 - x^2 - 2x + 1$	**q**
353	$x^6 + 2x^5 + 5x^4 + 2x^3 + 2x^2 + 1$	**wr72**
389	$x^6 + 2x^5 + 5x^4 + 8x^3 + 8x^2 + 4x$	**389**
427	$x^6 - 4x^5 - 4x^4 + 18x^3 + 16x^2 - 16x - 15$	**61**
461	$x^6 + 2x^5 - 5x^4 - 8x^3 + 11x^2 + 10x - 11$	**q**
523	$x^6 - 2x^5 + x^4 + 4x^3 - 4x^2 - 4x$	**523**
555	$x^6 + 6x^5 + 5x^4 - 16x^3 - 8x^2 + 12x$	**37**
561	PRYM	$\mathbf{11}, \mathbf{51}$
587a	$-3x^6 + 18x^4 + 6x^3 + 9x^2 - 54x + 57$	$\mathcal{S}_\mathbf{6}$, mild@3
587b	$x^6 + 2x^4 + 2x^3 - 3x^2 - 2x + 1$	$\mathcal{S}_\mathbf{6}$
597	$x^6 + 4x^5 + 8x^4 + 12x^3 + 8x^2 + 4x$	**q**
603	$x^6 - 4x^5 + 2x^4 + 4x^3 + x^2 - 4x$	**67**
623	$-224x^6 - 1504x^5 - 4448x^4 - 7200x^3 - 6080x^2 - 2048x$	**89**, mild@8
633	$24x^6 + 40x^5 + 28x^4 + 80x^3 + 52x^2 - 32x$	**211**, mild@2
657	WEIL RESTRICTION	**u**, notSS
665	PRYM	$\mathbf{19}, \mathbf{35}$
691	$x^6 + 2x^5 - 3x^4 - 4x^3 + 4x$	**691**
709	$-4x^5 - 7x^4 - 4x$	**709**
713a	$x^6 + 2x^5 + x^4 + 2x^3 - 2x^2 + 1$	$\mathbf{23}, \mathbf{31}$
713b	$x^6 - 2x^5 + x^4 + 2x^3 + 2x^2 - 4x + 1$	$\mathbf{23}, \mathbf{31}$
731	$x^6 - 6x^4 + 4x^3 + 9x^2 - 16x - 4$	**43**
737	PRYM	$\mathbf{11}, \mathbf{67}$
741	$x^6 - 6x^5 + 9x^4 - 4x^2 + 12x$	**19**
743	$x^6 - 2x^4 - 2x^3 + 5x^2 - 2x + 1$	$\mathcal{S}_\mathbf{6}$
745	$x^6 + 2x^4 - 2x^3 + x^2 + 2x + 1$	**wr72**
763	$4x^5 + 9x^4 - 6x^2 + 1$	**763**
775	WEIL RESTRICTION	**u**, notSS
797	$x^6 + 4x^3 - 4x^2 + 4x$	**q**
807	$x^6 - 4x^5 + 2x^4 + 8x^3 - 3x^2 - 8x - 4$	**269**
847	$x^6 - 2x^5 + 5x^4 - 4x^3 + 4x - 8$	$\mathbf{11}, \mathbf{11}$, notSS
893a	$5x^6 - 40x^5 + 30x^4 - 510x^3 - 195x^2 - 1690x - 1295$	$\mathcal{S}_\mathbf{6}$, mild@5
893b	$x^6 - 2x^4 - 2x^3 - 3x^2 - 2x + 1$	$\mathcal{S}_\mathbf{6}$
901	$-7x^6 - 140x^5 - 532x^4 - 966x^3 - 504x^2 + 1596x + 2065$	**53**, mild@7
909	$x^6 - 2x^4 + 5x^2 - 4x$	**101**
925	$4x^5 + 8x^4 + 4x^3 - 3x^2 - 2x + 1$	**37**
953	$x^6 - 2x^5 + 5x^4 - 6x^3 + 2x^2 + 1$	**wr72**
971	$x^6 + 4x^5 - 8x^3 + 4x$	**q**
975	$x^6 + 4x^5 - 6x^3 + 8x^2 - 4x - 3$	**u**, notSS
997a	$x^6 + 2x^5 + x^4 + 4x^2 + 4x$	**997**
997b	$x^6 - 4x^4 - 8x^3 - 8x^2 - 4x$	**q**

Acknowledgments

The authors are grateful for the opportunity to lecture on preliminary aspects of this work at Edinburgh, Essen, MSRI, Tokyo, Kyoto, Osaka, Irvine, Rome, Banff, Shanghai, Beijing and New York. The authors were inspired by René Schoof, who kindly provided them with preprints. His hospitality and support to the first author during a visit to Roma III in May 2005 helped this project along. The contributions of Brooks Roberts and Ralf Schmidt as well as those of Cris Poor and David S. Yuen were decisive to our main conjecture. The authors thank them heartily for that as well as for useful conversations and correspondence. The authors also wish to thank the referee for many useful suggestions to improve the exposition.

References

[1] V. A. Abrashkin, *Galois modules of group schemes of period p over the ring of Witt vectors*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 4, 691–736, 910 (Russian); English transl., Math. USSR-Izv. **31** (1988), no. 1, 1–46. MR914857 (89a:14062)

[2] Anatolij N. Andrianov, *Quadratic forms and Hecke operators*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 286, Springer-Verlag, Berlin, 1987. MR884891 (88g:11028)

[3] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 302, Springer-Verlag, Berlin, 2004. MR2062673 (2005c:14001)

[4] Michael Aschbacher, *Finite group theory*, Cambridge Studies in Advanced Mathematics, vol. 10, Cambridge University Press, Cambridge, 1986. MR895134 (89b:20001)

[5] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[6] Armand Brumer and Kenneth Kramer, *Non-existence of certain semistable abelian varieties*, Manuscripta Math. **106** (2001), no. 3, 291–304, DOI 10.1007/PL00005885. MR1869222 (2003b:14054)

[7] Armand Brumer and Kenneth Kramer, *Semistable abelian varieties with small division fields*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 13–37, DOI 10.1007/978-1-4613-0249-0_2. MR2059756 (2005m:11106)

[8] Armand Brumer and Kenneth Kramer, *Arithmetic of division fields*, Proc. Amer. Math. Soc. **140** (2012), no. 9, 2981–2995, DOI 10.1090/S0002-9939-2012-11500-X. MR2917071

[9] A. Brumer and K. Kramer, Pryms of Bielliptic Quartics (in preparation).

[10] H. Cohen et al: Tables of number fields. http://pari.math.u-bordeaux1.fr/pub/numberfields

[11] B. Conrad, Wild ramification and deformation rings, Unpublished Notes (1999).

[12] C. W. Curtis and I. Reiner, Representations of finite groups and associative algebras, John Wiley, 1962.

[13] Gerd Faltings, Gisbert Wüstholz, Fritz Grunewald, Norbert Schappacher, and Ulrich Stuhler, *Rational points*, 3rd ed., Aspects of Mathematics, E6, Friedr. Vieweg & Sohn, Braunschweig, 1992. Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984; With an appendix by Wüstholz. MR1175627 (93k:11060)

[14] Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 22, Springer-Verlag, Berlin, 1990. With an appendix by David Mumford. MR1083353 (92d:14036)

[15] Jean-Marc Fontaine, *Il n'y a pas de variété abélienne sur* **Z**, Invent. Math. **81** (1985), no. 3, 515–538, DOI 10.1007/BF01388584 (French). MR807070 (87g:11073)

[16] Valeri Gritsenko, *Arithmetical lifting and its applications*, Number theory (Paris, 1992), London Math. Soc. Lecture Note Ser., vol. 215, Cambridge Univ. Press, Cambridge, 1995, pp. 103–126, DOI 10.1017/CBO9780511661990.008. MR1345176 (96d:11049)

[17] Valeri Gritsenko, *Irrationality of the moduli spaces of polarized abelian surfaces*, Abelian varieties (Egloffstein, 1993), de Gruyter, Berlin, 1995, pp. 63–84. With an appendix by the author and K. Hulek. MR1336601 (96e:14022)

[18] Valeri Gritsenko and Klaus Hulek, *Minimal Siegel modular threefolds*, Math. Proc. Cambridge Philos. Soc. **123** (1998), no. 3, 461–485, DOI 10.1017/S0305004197002259. MR1607981 (99c:14048)

[19] B. Gross, Letter to J.-P. Serre, June 22, 2010. Private communication.

[20] A. Grothendieck, Modèles de Néron et monodromie. Sém. de Géom. 7, Exposé IX, Lecture Notes in Math. **288**, New York: Springer-Verlag 1973.

[21] Everett W. Howe, *Isogeny classes of abelian varieties with no principal polarizations*, Moduli of abelian varieties (Texel Island, 1999), Progr. Math., vol. 195, Birkhäuser, Basel, 2001, pp. 203–216. MR1827021 (2002g:11079)

[22] Bertram Huppert and Norman Blackburn, *Finite groups. II*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 242, Springer-Verlag, Berlin, 1982. AMD, 44. MR650245 (84i:20001a)

[23] Tomoyoshi Ibukiyama, *On symplectic Euler factors of genus two*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **30** (1984), no. 3, 587–614. MR731520 (85j:11053)

[24] Christian U. Jensen, Arne Ledet, and Noriko Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, Cambridge, 2002. Constructive aspects of the inverse Galois problem. MR1969648 (2004d:12007)

[25] Jennifer Johnson-Leung and Brooks Roberts, *Siegel modular forms of degree two attached to Hilbert modular forms*, J. Number Theory **132** (2012), no. 4, 543–564, DOI 10.1016/j.jnt.2011.08.004. MR2887605

[26] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97, DOI 10.1016/j.jsc.2005.09.003. MR2194887 (2006k:11230)

[27] C. Khare and J.-P. Wintenberger, Serre's modularity conjecture (I), (II), Inv. Math. **178(3)** (2009), 485–504, 505–586.

[28] Qing Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348** (1996), no. 11, 4577–4610, DOI 10.1090/S0002-9947-96-01684-4 (French, with English summary). MR1363944 (97h:11062)

[29] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287 (80c:14015)

[30] J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR861974

[31] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190. MR0330174 (48 #8512)

[32] Laurent Moret-Bailly, *Pinceaux de variétés abéliennes*, Astérisque **129** (1985), 266 (French, with English summary). MR797982 (87j:14069)

[33] V. V. Nikulin, Integral symmetric bilinear forms and some of their applications, Trans. Moscow Math. Soc. **38** (1980) 71–135.

[34] Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135. MR0241435 (39 #2775)

[35] A. M. Odlyzko, *Lower bounds for discriminants of number fields. II*, Tôhoku Math. J. **29** (1977), no. 2, 209–216. MR0441918 (56 #309)

[36] Takeo Okazaki, *Proof of R. Salvati Manni and J. Top's conjectures on Siegel modular forms and abelian surfaces*, Amer. J. Math. **128** (2006), no. 1, 139–165. MR2197070 (2007a:11062)

[37] Vincent Pilloni, *Modularité, formes de Siegel et surfaces abéliennes*, J. Reine Angew. Math. **666** (2012), 35–82, DOI 10.1515/CRELLE.2011.123 (French, with French summary). MR2920881

[38] Harriet Pollatsek, *First cohomology groups of some linear groups over fields of characteristic two*, Illinois J. Math. **15** (1971), 393–417. MR0280596 (43 #6316)

[39] C. Poor and D. S. Yuen, Paramodular Cusp Forms, arXiv:0912.0049v1 (2009).

[40] C. Poor and D. S. Yuen, in preparation. See http://math.lfc.edu/∼yuen/paramodular.

[41] Michel Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280 (French). MR0419467 (54 #7488)

[42] L. Rédei and H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratisschen Zahlkörpers, J. reine ang. Math. **170** (1933), 69–74.

[43] Kenneth A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Ann. Math. (2) **101** (1975), 555–562. MR0371903 (51 #8120)

[44] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804. MR0457455 (56 #15660)

[45] Kenneth A. Ribet, *Images of semistable Galois representations*, Pacific J. Math. **Special Issue** (1997), 277–297, DOI 10.2140/pjm.1997.181.277. Olga Taussky-Todd: in memoriam. MR1610883 (99a:11065)

[46] Kenneth A. Ribet, *Abelian varieties over* **Q** *and modular forms*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 241–261, DOI 10.1007/978-3-0348-7919-4_15. MR2058653 (2005k:11120)

[47] Brooks Roberts and Ralf Schmidt, *On modular forms for the paramodular groups*, Automorphic forms and zeta functions, World Sci. Publ., Hackensack, NJ, 2006, pp. 334–364, DOI 10.1142/9789812774415_0015. MR2208781 (2006m:11065)

[48] Brooks Roberts and Ralf Schmidt, *Local newforms for GSp(4)*, Lecture Notes in Mathematics, vol. 1918, Springer, Berlin, 2007. MR2344630 (2008g:11080)

[49] David P. Roberts, *Twin sextic algebras*, Rocky Mountain J. Math. **28** (1998), no. 1, 341–368, DOI 10.1216/rmjm/1181071838. MR1639810 (99j:12001)

[50] Riccardo Salvati Manni and Jaap Top, *Cusp forms of weight* 2 *for the group* $\Gamma_2(4,8)$, Amer. J. Math. **115** (1993), no. 2, 455–486, DOI 10.2307/2374865. MR1216438 (94e:11050)

[51] René Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Ann. **325** (2003), no. 3, 413–448, DOI 10.1007/s00208-002-0368-7. MR1968602 (2005b:11076)

[52] René Schoof, *Abelian varieties over* $\mathbb{Q}$ *with bad reduction in one prime only*, Compos. Math. **141** (2005), no. 4, 847–868, DOI 10.1112/S0010437X05001107. MR2148199 (2006c:11068)

[53] René Schoof, *Semistable abelian varieties with good reduction outside 15*, Manuscripta Math. **139** (2012), no. 1-2, 49–70, DOI 10.1007/s00229-011-0509-y. MR2959670

[54] R. Schoof, On the modular curve $X_0(23)$ in Faber, C. et al., Geom. and Arith., EMS Publishing House, Zürich (to appear).

[55] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016)

[56] J.-P. Serre, Facteurs locaux des fonctions zêta des variétés algébriques. Séminaire Delange-Pisot-Poitou. Théorie des nombres **11**, 1969-1970.

[57] Jean-Pierre Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230, DOI 10.1215/S0012-7094-87-05413-5 (French). MR885783 (88g:11022)

[58] Goro Shimura, *On analytic families of polarized abelian varieties and automorphic functions*, Ann. of Math. (2) **78** (1963), 149–192. MR0156001 (27 #5934)

[59] N. P. Smart, *S-unit equations, binary forms and curves of genus* 2, Proc. London Math. Soc. (3) **75** (1997), no. 2, 271–307, DOI 10.1112/S002461159700035X. MR1455857 (98d:11072)

[60] Michio Suzuki, *Group theory. I*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 247, Springer-Verlag, Berlin, 1982. Translated from the Japanese by the author. MR648772 (82k:20001c)

[61] John Tate, *Finite flat group schemes*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 121–154. MR1638478

[62] Richard Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991), no. 2, 281–332, DOI 10.1215/S0012-7094-91-06312-X. MR1115109 (92j:11044)

[63] Richard Taylor, *l-adic representations associated to modular forms over imaginary quadratic fields. II*, Invent. Math. **116** (1994), no. 1-3, 619–643, DOI 10.1007/BF01231575. MR1253207 (95h:11050a)

[64] J. Tilouine, *Nearly ordinary rank four Galois representations and p-adic Siegel modular forms*, Compos. Math. **142** (2006), no. 5, 1122–1156, DOI 10.1112/S0010437X06002119. With an appendix by Don Blasius. MR2264659 (2007j:11071)

[65] J. Tilouine, *Siegel varieties and p-adic Siegel modular forms*, Doc. Math. **Extra Vol.** (2006), 781–817. MR2290605 (2007k:11067)

[66] J. Top, Hecke L-series related with algebraic cycles or with Siegel modular forms, thesis, Utrecht, 1989.

[67] Lawrence C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1982. MR718674 (85g:11001)

[68] John Wilson, *Degrees of polarizations on an abelian surface with real multiplication*, Bull. London Math. Soc. **33** (2001), no. 3, 257–264, DOI 10.1017/S0024609301007974. MR1817763 (2002c:11062)

[69] André Weil, *Zum Beweis des Torellischen Satzes*, Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa. **1957** (1957), 33–53 (German). MR0089483 (19,683e)
[70] Hiroyuki Yoshida, *On Siegel modular forms obtained from theta series*, J. Reine Angew. Math. **352** (1984), 184–219, DOI 10.1515/crll.1984.352.184. MR758701 (86e:11036)

Department of Mathematics, Fordham University, Bronx, New York 10458
E-mail address: brumer@fordham.edu

Department of Mathematics, Queens College, Flushing, New York 11367 – and – The Graduate Center CUNY, New York, New York 10016
E-mail address: kkramer@gc.cuny.edu