PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 9, September 2012, Pages 2981–2995
S 0002-9939(2012)11500-X
Article electronically published on January 12, 2012

ARITHMETIC OF DIVISION FIELDS

ARMAND BRUMER AND KENNETH KRAMER

(Communicated by Matthew A. Papanikolas)

Abstract. We study the arithmetic of division fields of semistable abelian varieties $A_{/\mathbb{Q}}$. The Galois group of $\mathbb{Q}(A[2])/\mathbb{Q}$ is analyzed when the conductor of A is odd and squarefree. The irreducible semistable mod 2 representations of small conductor are determined under GRH. These results are used in our paper *Paramodular abelian varieties of odd conductor*.

1. Introduction

This paper contains results needed in [4] and of independent interest. We write S for a set of primes, N_S for their product and ℓ for a prime not in S. If $F/\mathbb{Q}$ is Galois, $\mathcal{I}_v(F/\mathbb{Q})$ denotes the inertia group at a place v of F.

Definition 1.1 ([3])**.** The Galois extension $F/\mathbb{Q}$ is (ℓ, N_S)-*controlled* if

i) $F/\mathbb{Q}$ is unramified outside $S \cup \{\ell, \infty\}$;
ii) $\mathcal{I}_v(F/\mathbb{Q}) = \langle \sigma_v \rangle$ is cyclic of order ℓ for all ramified v not over ℓ;
iii) $\mathcal{I}_\lambda(F/\mathbb{Q})^u = 1$ for all $u > 1/(\ell - 1)$ and λ over ℓ, using the upper ramification numbering as in §5.

We denote by V a finite dimensional vector space over the finite field $\mathbb{F}$ of characteristic ℓ with $q = |\mathbb{F}|$. Additional structure on V, such as a symplectic pairing or Galois action, is often imposed.

Definition 1.2. Let V be an $\mathbb{F}[G_\mathbb{Q}]$-module and $F = \mathbb{Q}(V)$. The set S of rational primes $p \neq \ell$ ramified in $F/\mathbb{Q}$ comprises the *bad primes* of V. Declare V to be *semistable* if F is (ℓ, N_S)-controlled and $(\sigma_v - 1)^2(V) = 0$ for all v lying over the primes of S.

Throughout, $A_{/\mathbb{Q}}$ is a semistable abelian variety with good reduction at ℓ and $\mathrm{End}_\mathbb{Q} A = \mathfrak{o}$ is the ring of integers in a totally real number field. If $\mathfrak{l}$ is a prime over ℓ in $\mathfrak{o}$ and $\mathfrak{o}/\mathfrak{l} = \mathbb{F}$, then $V = A[\mathfrak{l}]$ is semistable [9, 7]. The conductor of A has the form $N_A = N^d$ with $d = [\mathfrak{o}:\mathbb{Z}]$. Since inertia over each bad prime p is tame,

$$\mathrm{ord}_p(N) = \dim_\mathbb{F} V/V^{\mathcal{I}} = \dim_\mathbb{F} (\sigma_v - 1)V. \tag{1.3}$$

In §2, we use known results on symplectic representations generated by transvections to describe $\mathrm{Gal}(\mathbb{Q}(W)/\mathbb{Q})$ for constituents W of V with squarefree conductor, assuming $\mathfrak{l}$ lies over 2.

Received by the editors March 26, 2011.
2010 *Mathematics Subject Classification.* Primary 11F80; Secondary 11S15, 11G10, 11Y40.
Key words and phrases. Semistable Galois representation, transvection, stem field discriminant, bounded ramification.
The research of the second author was partially supported by NSF grant DMS 0739346.

A *stem field* for a Galois extension F/k is an intermediate field K whose Galois closure over k is F. If $G = \mathrm{Gal}(F/k)$ acts faithfully and transitively on a set X, the fixed field of the stabilizer G_x of any x in X is a stem field. A formula for the discriminant $d_{K/k}$ is given in §3 and applied to semistable Galois modules. By relating number-theoretic properties of K and F, certain computations may become feasible, since K has a smaller degree and discriminant than F.

Suppose $E/\mathbb{Q}_\ell$ is a Galois extension of ℓ-adic fields satisfying Definition 1.1(iii). In §5, we find conditions on the ray class conductor of an abelian extension L/E so that Definition 1.1(iii) also holds for the Galois closure of $L/\mathbb{Q}_\ell$. The maximal $(2, N)$-controlled extension for all odd $N \leq 79$ and for $N = 97$ is determined in §6, thanks to §5 and Odlyzko's GRH bounds. We also construct a $(2, 127)$-controlled extension of degree 161280 with root discriminant just above the asymptotic Odlyzko bound, but finiteness of a maximal one is unknown to us.

A finite flat group scheme $\mathcal{V}$ over $\mathbb{Z}_\ell$ admits a filtration $0 \subseteq \mathcal{V}^m \subseteq \mathcal{V}^0 \subseteq \mathcal{V}$ with connected component $\mathcal{V}^0$, étale quotient $\mathcal{V}^{et} = \mathcal{V}/\mathcal{V}^0$, multiplicative subscheme $\mathcal{V}^m$ and biconnected subquotient $\mathcal{V}^b = \mathcal{V}^0/\mathcal{V}^m$. Let λ be a place over ℓ in $F = \mathbb{Q}(V)$ and $\mathcal{D}_\lambda$ be its decomposition group. We denote the corresponding $\mathbb{F}[\mathcal{D}_\lambda]$-modules of F_λ-valued points by V, V^{et}, V^m and V^b, respectively.

Definition 1.4 ([4])**.** $A_{/\mathbb{Q}}$ is $\mathfrak{o}$-*paramodular* if $\dim A = 2d$, with $d = [\mathfrak{o} : \mathbb{Z}]$.

Let A be $\mathfrak{o}$-paramodular, with $\mathfrak{o}/\mathfrak{l} \simeq \mathbb{F}_2$. When $A[\mathfrak{l}]$ is irreducible, estimates for the discriminant of a stem field of $\mathbb{Q}(A[\mathfrak{l}])$ are obtained in §4. The reducible case leads to ray class fields whose conductors are controlled by the results of §5. This information depends on the structure of $A[\mathfrak{l}]$ as a group scheme and is used in [4].

2. Mod 2 representations generated by transvections

A *transvection* on V is an automorphism of the form $\tau(x) = x + \psi(x)\, z$, with $\psi : V \to \mathbb{F}$ a non-zero linear form and $z \neq 0$ in $\ker \psi$. Assume V admits a non-degenerate alternating pairing $[\,,\,] : V \times V \to \mathbb{F}$ preserved by τ and let $\dim V = 2n$. Then $\tau(x) = x + a\,[z, x]z$ for some $z \in V$ and $a \in \mathbb{F}^\times$. When a is a square in $\mathbb{F}$, we may take $a = 1$. For x and z in V, define $\tau_{[z]}$ by

$$\tau_{[z]}(x) = x + [z, x]z. \tag{2.1}$$

Assume that $\ell = 2$ for the rest of this section, unless otherwise noted.

A quadratic form θ on the symplectic space V is called a *theta characteristic* if $\theta(x+y) = \theta(x)+\theta(y)+[x, y]$ for all x, y in V. Theta characteristics form a principal homogeneous space over V, with $(\theta + a)(x) = \theta(x) + [a, x]^2$ for a in V. We identify a with $[\,a, -]$ under the Galois isomorphism $V \simeq \mathrm{Hom}_{\mathbb{F}}(V, \mathbb{F})$. Elements σ in $\mathrm{Sp}(V)$ act by $\sigma(\theta)(x) = \theta(\sigma(x))$. Then $\sigma(\theta + a) = \sigma(\theta) + \sigma(a)$ and

$$\tau_{[z]}(\theta) = \theta + \sqrt{1 + \theta(z)}\, z. \tag{2.2}$$

Fix a symplectic basis $\{e_1, \ldots, e_{2n}\}$ for V with $[e_i, e_j] = 1$ if $|i - j| = n$ and 0 otherwise. Let $\wp(x) = x^2 - x$ be the Artin-Schreier function. Depending on whether or not the Arf invariant $\mathrm{Arf}(\theta) = \sum_i \theta(e_i)\theta(e_{i+n})$ vanishes in $\mathbb{F}/\wp(\mathbb{F})$, we say θ is even or odd and write $O^{\pm}_{2n}$ for the corresponding orthogonal group. Further, $\mathrm{Sp}(V)$ acts transitively on the sets $\Theta^{\pm}_{2n}$ of even and odd characteristics and

$$|\Theta^{\pm}_{2n}| = \frac{1}{2} q^n (q^n \pm 1). \tag{2.3}$$

Denote the symmetric, alternating, dihedral and cyclic groups by $\mathcal{S}_n$, $\mathcal{A}_n$, D_n and C_n respectively.

Proposition 2.4 ([17]). *If $\mathbb{F} = \mathbb{F}_2$ and $G \subsetneq \mathrm{SL(V)}$ is an irreducible subgroup generated by transvections, then $\dim V = 2n$ with $n \geq 2$ and G is $O^{\pm}_{2n}(\mathbb{F}_2)$, $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ or $\mathcal{S}_m$ with $2n+1 \leq m \leq 2n+2$. Also, G has a trivial center and is self-normalizing in $\mathrm{SL(V)}$.*

Proposition 2.5. *Let V be a symplectic space of dimension $2n$. An irreducible subgroup G of $\mathrm{Sp}(V)$ generated by transvections is one of the following, with $\mathbb{F}' \subseteq \mathbb{F}$:*

i) *dihedral, D_m with m dividing one of $|\mathbb{F}| \pm 1$ and $n = 1$;*
ii) *orthogonal, $O^{\pm}_{2n}(\mathbb{F}')$ for $n \geq 2$;*
iii) *symplectic, $\mathrm{Sp}_{2n}(\mathbb{F}')$;*
iv) *symmetric, $\mathcal{S}_m$ for $n \geq 2$ and $2n + 1 \leq m \leq 2n + 2$.*

Moreover, G has trivial center and is self-normalizing in $\mathrm{Sp}(V)$.

Proof. If V is imprimitive, then V is monomial [22], say $V = \mathrm{Ind}^G_{H_1}(V_1)$, with $V_1 = \mathbb{F}e_1$ and $[G : H_1] = \dim V = 2n$. Arrange that $G = \bigcup g_i H_1$, with $g_1 = 1$ and $V_i = g_i(V_1) = \mathbb{F}e_i$, and let $\pi : G \to \mathcal{S}_{2n}$ by $gV_i = V_{\pi(g)i}$. Since $\pi(G)$ is transitive and generated by transpositions, namely the images of the transvections, $\pi(G) = \mathcal{S}_{2n}$. For h in $H = \ker \pi$, we have $he_i = \chi_i(h)e_i$, and so the pairing on V satisfies $[e_i, e_j] = [he_i, he_j] = \chi_i(h)\chi_j(h)[e_i, e_j]$. Hence $[e_i, e_j] = 0$ or $\chi_i(h)\chi_j(h) = 1$. Because the pairing is perfect and $\pi(G)$ is doubly transitive, we must have $[e_i, e_j] \neq 0$ and $\chi_i(h)\chi_j(h) = 1$ for all $i \neq j$. If $n \geq 2$, then $\chi_i(H) = 1$ for all i, $H = 1$ and π is an isomorphism. The stabilizer H_1 of V_1 is isomorphic to $\mathcal{S}_{2n-1}$, and so the character $\chi_1 : H_1 \to \mathbb{F}^\times$ is trivial. Since $\sum g_i(e_1)$ is a non-trivial fixed point, V is reducible. Now combine [11, Ch. II, §8.27] and [15, 16] to get our list.

If g in $\mathrm{Sp}_{2n}(\mathbb{F})$ normalizes G and σ is in $\mathrm{Gal}(\mathbb{F}/\mathbb{F}')$, then $g^\sigma g^{-1}$ centralizes G. Our representations are absolutely irreducible and the center of $\mathrm{Sp}_{2n}(\mathbb{F})$ is trivial, so g is in $\mathrm{Sp}_{2n}(\mathbb{F}')$. To verify that the center is trivial and $G = \mathcal{S}_m$ is self-normalizing in $\mathrm{Sp}_{2n}(\mathbb{F}_2)$ when $m \neq 6$, use the fact that all automorphisms are inner and absolute irreducibility. Note that $\mathcal{S}_6 \simeq \mathrm{Sp}_4(\mathbb{F}_2)$. The dihedral case is easily checked. See [6] for the other cases. □

Remark 2.6. As to (iv) above, note that $\mathcal{S}_m$ acts by permutation on

$$Y = \{(a_1, ..., a_m) \in \mathbb{F}_2^m \mid a_1 + \cdots + a_m = 0\}$$

with pairing $[(a_i), (b_i)] = \sum a_i b_i$. Let $V = Y/\langle(1, \ldots, 1)\rangle$ or $V = Y$ according as m is even or odd. Then V is irreducible and transpositions in $\mathcal{S}_m$ correspond to transvections on V. This action of $\mathcal{S}_m$ and that of Galois on $J[2]$ for a hyperelliptic Jacobian are compatible.

Lemma 2.7. *Let V be an irreducible $\mathbb{F}[G]$-module and let P be the subgroup of G generated by transvections. If P is not trivial, then $V_{|P}$ is the direct sum of r irreducible $\mathbb{F}[P]$-modules W_i and $P = Q_1 \cdots Q_r$ is a direct product, with $Q_i = \langle \sigma \in P \mid \sigma_{|W_i}$ is a transvection and $\sigma_{|W_j} = 1$ for all $j \neq i\rangle$. If V is symplectic, then the W_i are symplectic and the sum is orthogonal.*

Proof. Since P is normal, Clifford's theorem applies. Let W_1 be an irreducible submodule of $V_{|P}$, $H = \{h \in G \mid h(W_1) \simeq W_1$ as P-module$\}$ and $X = \sum_{h \in H} h(W_1)$. Then $V = \mathrm{ind}^G_H(X)$ and $X_{|P} \simeq eW_1$ is isotypic. If $G = \bigcup_1^r g_i H$ is a coset decomposition with $g_1 = 1$, then $V_{|P} \simeq \bigoplus_1^r eW_i$ with $W_i = g_i(W_1)$. For any transvection τ,

we have $1 = \dim(\tau - 1)(V) = e \sum_1^r \dim(\tau - 1)(W_i)$. Thus $e = 1$ and τ is in Q_i for a unique index i. Moreover, $Q_i = g_i Q_1 g_i^{-1}$ is normal in P and $P = Q_1 \cdots Q_r$ is a direct product.

Suppose V is symplectic and τ is a transvection in Q_i. Then $(\tau - 1)W_i = \langle z \rangle$ with z in $W_i \cap W_j^{\perp}$ for all $j \neq i$, but not in $W_i^{\perp}$. Irreducibility of W_i implies that $W_i \subseteq W_j^{\perp}$ and $W_i \cap W_i^{\perp} = 0$. Hence W_i is symplectic. □

Proposition 2.8. *Let V be an irreducible symplectic $\mathbb{F}[G_{\mathbb{Q}}]$-module with squarefree conductor N and let $F = \mathbb{Q}(V)$. Let P be the subgroup of $G = \mathrm{Gal}(F/\mathbb{Q})$ generated by transvections. If $P = G$, then G is as in* Proposition 2.5.

Otherwise, $V = \mathrm{ind}_P^G W$ and $G \simeq Q \wr C_2$, where Q is in the list in Proposition 2.5. *Moreover, $F^P = \mathbb{Q}(i)$ and $N = \mathfrak{n}\overline{\mathfrak{n}}$ in $\mathbb{Z}[i]$, where $\mathfrak{n}$ generates the conductor ideal of W as an $\mathbb{F}[G_{\mathbb{Q}(i)}]$-module.*

Proof. Since $\mathrm{ord}_{p_v}(N) = 1$, any generator σ_v of $\mathcal{I}_v(F/\mathbb{Q})$ is a transvection. Proposition 6.2 shows that the fixed field $F^P = \mathbb{Q}(i)$. The restriction $V_{|P}$ is reducible by Lemma 2.5 and so V is induced. Hence $H = P \simeq Q_1 \times Q_2$ and $G \simeq Q_1 \wr C_2$ is a wreath product, thanks to Lemma 2.7. The conductor formula for an induced module gives $N = \mathfrak{n}\overline{\mathfrak{n}}$, where $\mathfrak{n} \in \mathbb{Z}[i]$ is the odd part of the Artin conductor of W, since $\mathbb{Q}(i)$ is unramified at odd places. □

Remark 2.9. In Proposition 2.8, if we take $\mathbb{F} = \mathbb{F}_2$ but do not assume V symplectic, the conclusions hold, with "Proposition 2.5" replaced by "Proposition 2.4".

Remark 2.10. The conjugacy class of any involution σ in $\mathrm{Sp}(V)$ has invariants $t = \mathrm{rank}(\sigma - 1)$ and δ, with $\delta = 0$ if $[v, (\sigma - 1)v] = 0$ for all v in V and $\delta = 1$ otherwise. If $t = n$ and σ is in $O_{2n}^-(\mathbb{F})$, then $\delta = 1$. If t is odd, then $\delta = 1$.

For the last result in this section, $\ell = 3$.

Proposition 2.11. *Let V be an irreducible symplectic $\mathbb{F}_3[G_{\mathbb{Q}}]$-module with squarefree conductor N. Set $2n = \dim_{\mathbb{F}} V$, $F = \mathbb{Q}(V)$ and $G = \mathrm{Gal}(F/\mathbb{Q})$. Then*

i) *$G \simeq \mathrm{GSp}_{2n}(\mathbb{F}_3)$ or*
ii) *n is even, $G \simeq \mathrm{Sp}_n(\mathbb{F}_3) \wr C_2$ and $N = \mathfrak{n}\overline{\mathfrak{n}}$ in $\mathbb{Z}[\boldsymbol{\mu}_3]$.*

Proof. An irreducible proper subgroup of $\mathrm{SL}_{2n}(\mathbb{F}_3)$ generated by transvections is isomorphic to $\mathrm{Sp}_{2n}(\mathbb{F}_3)$; cf. [16]. The pairing on V implies that F contains $\boldsymbol{\mu}_3$. The subgroup P of G generated by all transvections fixes $K = \mathbb{Q}(\boldsymbol{\mu}_3)$ and F^P is unramified outside 3∞, so $F^P = K$ by Proposition 6.2. If $V_{|P}$ is irreducible, then (i) holds. If $V_{|P}$, is reducible, the arguments in the proofs of Lemma 2.7 and Proposition 2.8 give (ii), with $\mathfrak{n}$ a generator for the conductor ideal of the $\mathbb{F}[G_{\mathbb{Q}(\boldsymbol{\mu}_3)}]$-module W. □

3. Discriminants of stem fields

Let F/k be a Galois extension of number fields with group G. Let $\mathcal{D}$ be the decomposition group of a fixed prime π_F of F and $\mathcal{I}_m$ be the m^{th} ramification group (see §5), with $\mathcal{I} = \mathcal{I}_0$ the inertia group. For intermediate fields L, set $\pi_L = \pi_F \cap L$.

Theorem 3.1. *Let G act transitively on X. If K is the fixed field of G_x and $\mathcal{I}_m\backslash X$ is the set of $\mathcal{I}_m$-orbits of X, then*

$$\operatorname{ord}_{\pi_k}(d_{K/k}) = \sum_{m\geq 0} \frac{1}{[\mathcal{I} : \mathcal{I}_m]} \quad (|X| - |\mathcal{I}_m\backslash X|)\,.$$

Proof. If $H = G_x$ and I is any subgroup of G, then $HgI \leftrightarrow Ig^{-1}x$ is a bijection between the set of double cosets $H\backslash G/I$ and the set of orbits $I\backslash X$. Thus,

$$\sum_{HgI\,\in\, H\backslash G/I} [I : (I \cap H^g)] = [G : H], \tag{3.2}$$

where $H^g = g^{-1}Hg$. Suppose further that J is a normal subgroup of I so that $(I \cap H^g)J = I \cap H^g J$ is a subgroup of I. For each $g \in G$, we have

$$HgI = \bigsqcup Hgz_iJ, \tag{3.3}$$

where z_i runs over a set of representatives for the right cosets $I/(I \cap H^g)J$. The isomorphism $(I \cap H^g)/(J \cap H^g) \simeq (I \cap H^g)J/J$ implies that

$$\begin{aligned} \sum_{HgI\,\in\, H\backslash G/I} \frac{|J \cap H^g|}{|I \cap H^g|} &= \sum_{HgJ\,\in\, H\backslash G/J} \frac{1}{[I : (I \cap H^g)J]} \quad \frac{|J \cap H^g|}{|I \cap H^g|} \\ &= \sum_{HgJ\,\in\, H\backslash G/J} \frac{1}{[I : J]} = \frac{|H\backslash G/J|}{[I:J]}. \end{aligned} \tag{3.4}$$

The ramification groups for π_F inside H are given by $\mathcal{I}_m \cap H$, and the different ideal $\mathfrak{D}_{F/k}$ satisfies $\operatorname{ord}_{\pi_F}(\mathfrak{D}_{F/k}) = \sum_{m=0}^{\infty}(|\mathcal{I}_m| - 1)$. By transitivity of differents,

$$\begin{aligned} \operatorname{ord}_{\pi_K}(\mathfrak{D}_{K/k}) &= \frac{1}{|\mathcal{I} \cap H|}\operatorname{ord}_{\pi_F}(\mathfrak{D}_{K/k}) \\ &= \frac{1}{|\mathcal{I} \cap H|}\left(\operatorname{ord}_{\pi_F}(\mathfrak{D}_{F/k}) - \operatorname{ord}_{\pi_F}(\mathfrak{D}_{F/K})\right) \\ &= \sum_{m\geq 0} \frac{|\mathcal{I}_m| - |\mathcal{I}_m \cap H|}{|\mathcal{I} \cap H|}. \end{aligned} \tag{3.5}$$

Each prime of K over π_k has the form $g(\pi_F) \cap K$, corresponding to a unique double coset HgD in $H\backslash G/\mathcal{D}$. Since the decomposition and inertia groups of $g(\pi_F)$ inside G are $g\mathcal{D}g^{-1}$ and $g\mathcal{I}g^{-1}$, the ramification and residue degrees of $g(\pi_F) \cap K$ over π_k are given by

$$e(HgD) = [\mathcal{I} : (\mathcal{I} \cap H^g)] \text{ and } f(HgD) = [\mathcal{D} : (\mathcal{D} \cap H^g)\mathcal{I}]. \tag{3.6}$$

By conjugation, (3.5) implies that the exponent of $g(\pi_F) \cap K$ in $\mathfrak{D}_{K/k}$ is

$$x(HgD) = \sum_{m\geq 0} \frac{|\mathcal{I}_m| - |\mathcal{I}_m \cap H^g|}{|\mathcal{I} \cap H^g|}. \tag{3.7}$$

Moreover,

$$\operatorname{ord}_{\pi_k}(d_{K/k}) = \sum_{HgD\,\in\, H\backslash G/\mathcal{D}} x(HgD)f(HgD). \tag{3.8}$$

In view of (3.3) and (3.6), $Hg\mathcal{D}$ is the disjoint union of $f(Hg\mathcal{D})$ distinct elements of $H\backslash G/\mathcal{I}$. By (3.8) and (3.7), we now have

$$\mathrm{ord}_{\pi_k}(d_{K/k}) = \sum_{Hg\mathcal{I}\in H\backslash G/\mathcal{I}} = \sum_{m\geq 0}\ \sum_{Hg\mathcal{I}\in H\backslash G/\mathcal{I}} \frac{|\mathcal{I}_m| - |\mathcal{I}_m\cap H^g|}{|\mathcal{I}\cap H^g|}.$$

But (3.2) implies that

$$\sum_{Hg\mathcal{I}\in H\backslash G/\mathcal{I}} \frac{|\mathcal{I}_m|}{|\mathcal{I}\cap H^g|} = \sum_{Hg\mathcal{I}\in H\backslash G/\mathcal{I}} \frac{[\mathcal{I}:(\mathcal{I}\cap H^g)]}{[\mathcal{I}:\mathcal{I}_m]} = \frac{[G:H]}{[\mathcal{I}:\mathcal{I}_m]} = \frac{[K:k]}{[\mathcal{I}:\mathcal{I}_m]},$$

while (3.4) with $J=\mathcal{I}_m$ gives

$$\sum_{Hg\mathcal{I}\in H\backslash G/\mathcal{I}} \frac{|\mathcal{I}_m\cap H^g|}{|\mathcal{I}\cap H^g|} = \frac{|H\backslash G/\mathcal{I}_m|}{[\mathcal{I}:\mathcal{I}_m]}.$$

Substituting the last two identities in the previous double sum proves our claim. □

Corollary 3.9. *If π_k is tame in F, with ramification degree $|\mathcal{I}(F/k)| = \ell$ prime, then* $\mathrm{ord}_{\pi_k}(d_{K/k}) = (1-\ell^{-1})(|X| - |X^{\mathcal{I}}|)$.

Proof. Theorem 3.1 implies the claim, since $\mathcal{I}_1$ is trivial and there are $|X^{\mathcal{I}}|$ orbits of size 1, while the others have size ℓ. □

We now apply these results to semistable $G_{\mathbb{Q}}$-modules V of conductor N. We write $F=\mathbb{Q}(V)$ and $G=\mathrm{Gal}(F/\mathbb{Q})$.

Corollary 3.10. *Let $t=\mathrm{ord}_p(N)\geq 1$ and $s=\dim_{\mathbb{F}} V$. If G acts transitively on $X=V-\{0\}$ and $K=F^{G_x}$, then* $\mathrm{ord}_p(d_{K/\mathbb{Q}}) = (1-\ell^{-1})\,(q^s - q^{s-t})$.

Proof. Our claim follows from Corollary 3.9, since $\dim V^{\mathcal{I}} = s-t$ by (1.3). □

Now assume that $\ell=2$ and V is symplectic of dimension $2n$. Let K be the fixed field of G_x, where G acts transitively on X, as below:

i) $G\simeq \mathcal{S}_m = \mathrm{Sym}(X)$ and V is the representation in Remark 2.6.
ii) $X=\Theta_{2n}^-$ or $X=\Theta_{2n}^- - \{\theta_0\}$, with θ_0 fixed by G.

Proposition 3.11. *Let $\mathcal{I}_v=\langle\sigma\rangle\subseteq G$ be an inertia group at v over $p\,|\,N$.*

i) *If $G\simeq\mathcal{S}_m$ and σ is the product of s disjoint transpositions, then* $\mathrm{ord}_p(d_{K/\mathbb{Q}}) = s$ *and* $\mathrm{ord}_p(N)=\min(s,n)$.
ii) *If $G\simeq \mathrm{Sp}_{2n}(\mathbb{F})$ or $O_{2n}^{\pm}(\mathbb{F})$, then* $\mathrm{ord}_p(d_{K/\mathbb{Q}}) = \frac{1}{4}q^n(q^n - q^{n-t} - \delta)$, *with δ as in* Remark 2.10.

Proof. i) Since $|X^{\mathcal{I}_v}| = m-2s$, we have $\mathrm{ord}_p(d_{K/\mathbb{Q}})=s$ by Corollary 3.9 and, by (1.3), $\mathrm{ord}_p(N)=\dim_{\mathbb{F}}(\sigma-1)(V)=\min(s,n)$.

ii) We give a proof for $t=1$. Thus σ is a transvection and we choose a symplectic basis for V as in §2, such that $\sigma=\tau_{[e_n]}$. For the even theta characteristic $\theta(x_1,\dots,x_{2n}) = \sum_{j=1}^n x_j x_{n+j}$, by (2.1) and (2.2), we have

$$\sigma(\theta+a) = \theta + a + (1+[a,e_n])\,e_n.$$

Thus, σ fixes $\theta+a$ if and only if $[a,e_n]=1$. Let $V' = (\mathrm{span}\{e_n,e_{2n}\})^{\perp}$ and $\theta'(y)=\sum_{j=1}^{n-1} y_j y_{n+j}$. Assume $[a,e_n]=1$ and write $a=y+a_ne_n+e_{2n}$ with y in V'. In $\mathbb{F}/\wp(\mathbb{F})$, we have

$$\mathrm{Arf}(\theta+a) = \mathrm{Arf}(\theta)+\theta(a) = a_n + \theta'(y).$$

Hence $\theta + a$ is in Θ^-_{2n} precisely when one of the following conditions holds:

$$\text{(a) } a_n \in \wp(\mathbb{F}) \text{ and } \theta'(y) \notin \wp(\mathbb{F}) \quad \text{or} \quad \text{(b) } a_n \notin \wp(\mathbb{F}) \text{ and } \theta'(y) \in \wp(\mathbb{F}).$$

If $n = 1$, only (b) applies, yielding $\frac{1}{2}q$ choices of a. If $n \geq 2$, y is in $\wp(\mathbb{F})$ exactly when $\theta' + y$ is in Θ^+_{2n-2}. Hence there are $\frac{1}{2}q\,|\Theta^-_{2n-2}|$ choices of a in case (a) and $\frac{1}{2}q\,|\Theta^+_{2n-2}|$ choices in case (b). But $|\Theta^+_{2n-2}| + |\Theta^-_{2n-2}| = |V'| = q^{2n-2}$, and so $|(\Theta^-_{2n})^{\mathcal{I}_v}| = \frac{1}{2}q^{2n-1}$. □

Definition 3.12. A semistable Galois module V is *ordinary at* 2 if it is symplectic and $\mathfrak{a}^2\,V = 0$, where $\mathfrak{a}$ is the augmentation ideal in $\mathbb{F}[\mathcal{I}_\lambda]$ for any λ over 2 in F.

Let V be the Galois module of a finite flat group scheme $\mathcal{V}$ over $\mathbb{Z}_2$. Then $\mathcal{I}_\lambda$ acts trivially on V^m and V^{et}. If the biconnected subquotient $\mathcal{V}^b$ is trivial, then $(\sigma - 1)(\sigma' - 1)(V) = 0$ for all σ, σ' in $\mathcal{I}_\lambda$, whence V is ordinary. If $\mathcal{V}^b \neq 0$, then $\mathcal{I}_\lambda$ is not even a 2-group.

We next treat the power of 2 in $d_{K/\mathbb{Q}}$ when V is ordinary.

Lemma 3.13. *We have $\mathfrak{a}\,V \subseteq Z \subseteq V^{\mathcal{I}_\lambda}$ for some maximal isotropic subspace Z of V. If $H = G_\theta$ stabilizes an odd theta characteristic θ, then $|\mathcal{I}_\lambda/(\mathcal{I}_\lambda \cap H)| \leq \frac{1}{2}q^n$.*

Proof. Set $\mathcal{I} = \mathcal{I}_\lambda$. Since $\mathfrak{a}^2\,V = 0$ and $\mathcal{I} \subseteq \mathrm{Sp}(V)$, we find $\mathfrak{a}\,V \subseteq V^{\mathcal{I}} = (\mathfrak{a}\,V)^\perp$. Thus, $\mathfrak{a}\,V$ is contained in a maximal isotropic space Z and, by duality, $Z \subseteq V^{\mathcal{I}}$.

If Γ is the subgroup of $\mathrm{Sp}_{2n}(\mathbb{F})$ fixing both Z and V/Z pointwise, then we have $(g-1)(g'-1)(V) = 0$ for all g, g' in Γ. Hence $\psi(g) = (g-1)\theta$ defines a homomorphism $\Gamma \to V$. In the notation of (2.1), Γ is generated by the transvections $\tau_{[z]}$ with z in Z. Since we may identify $(\tau_{[z]} - 1)\theta$ with $\sqrt{1 + \theta(z)}\,z$, the homomorphism ψ takes values in Z. We next verify the exactness of the sequence

$$0 \to \Gamma \cap H \to \Gamma \xrightarrow{\psi} Z \xrightarrow{\theta} \mathbb{F}/\wp\mathbb{F} \to 0. \tag{3.14}$$

Since Z is isotropic, θ is linear on Z and θ is surjective because it is odd. Clearly $\theta(\psi(\tau_{[z]}))$ is in $\wp\mathbb{F}$. Conversely, if $\theta(z) = a^2 + a$ and $y = (1/\sqrt{a})z$, then $\psi(\tau_{[y]}) = z$. This proves exactness around Z, and the rest is clear.

Finally, $\mathcal{I} \subseteq \Gamma$, and therefore $|\mathcal{I}/(\mathcal{I} \cap H)| \leq |\Gamma/(\Gamma \cap H)| = \frac{1}{2}q^n$. □

Proposition 3.15. *If V is ordinary at 2 and G is transitive on Θ^-_{2n} or $\Theta^-_{2n} - \{\theta_0\}$, then $\mathrm{ord}_2(d_{K/\mathbb{Q}}) \leq (q^n - 2)(q^n - 1 - \epsilon)$, where $\epsilon = 0$ or 1, respectively.*

Proof. Since $\mathcal{I}$ is a 2-group, $\mathcal{I}_0 = \mathcal{I}_1$. The definition of the upper numbering (see §5) and the bound on wild ramification (Definition 1.1(iii)) imply that $\mathcal{I}_2 = 1$. By Theorem 3.1, $\mathrm{ord}_2(d_{K/\mathbb{Q}}) = 2(|X| - |\mathcal{I}\backslash X|)$.

By Lemma 3.13, each $\mathcal{I}$-orbit of X has at most $\frac{1}{2}q^n$ elements and there are at least $2|\Theta^-_{2n}|/q^n = q^n - 1$ orbits when $\epsilon = 0$, proving the claim.

If $\epsilon = 1$, $\mathcal{I}$ fixes θ_0. The theta characteristic $\theta_0 + z$ is odd exactly if $\theta_0(z)$ is in $\wp\mathbb{F}$. By (3.14), there are $\frac{1}{2}q^n$ such $z \in Z$, giving at least $\frac{1}{2}q^n - 1$ orbits of size 1 for $\mathcal{I}$ acting on X. The number of orbits not accounted for is at least

$$\frac{|X| - (\frac{1}{2}q^n - 1)}{\frac{1}{2}q^n} = q^n - 2,$$

and so $|\mathcal{I}\backslash X| \geq \frac{1}{2}q^n - 1 + (q^n - 2) = \frac{3}{2}q^n - 3$. Hence our claim. □

Proposition 3.16. *If V is ordinary and G is a transitive subgroup of $\mathcal{S}_m$, then $\mathrm{ord}_2(d_{K/\mathbb{Q}}) \leq 2\lfloor m/2 \rfloor$, unless $m = 4$ or 8, when $\mathrm{ord}_2(d_{K/\mathbb{Q}}) \leq 3m/2$.*

Proof. We find lower bounds for the number of $\mathcal{I}$-orbits and apply Theorem 3.1. Since there is at least one orbit, our claims hold for $m \leq 4$. Assume $m \geq 5$ and refer to the explicit representation (2.6). Let $y_{i,j} \in Y$ denote the vector with non-zero entries only in coordinates i and j. Write $\overline{y} \in V$ for the coset of $y \in Y$ when m is even and $\overline{y} = y$ otherwise.

Suppose distinct letters i, j lie in the same $\mathcal{I}$-orbit. If we can find a permutation σ in $\mathcal{I}$ such that $\sigma(i) = j$ and $\sigma(k) = k$, then $\overline{y}_{i,j} = (\sigma - 1)(\overline{y}_{i,k}) \in \mathfrak{a}\, V$ is fixed by $\mathcal{I}$. It follows that $\tau(y_{i,j}) = y_{i,j}$ for all τ in $\mathcal{I}$, and so $\{i, j\}$ is an $\mathcal{I}$-orbit.

A larger orbit can exist only if $m = 2n + 2$ is even and $\mathcal{I}$ contains a product of $n + 1$ disjoint transpositions, say

$$\sigma = (1, n + 2)(2, n + 3) \cdots (n + 1, 2n + 2).$$

Treat subscripts modulo $2n + 2$, fix k and consider $j \notin \{k, k + n + 1\}$. Then

$$\overline{x}_j := \overline{y}_{j,j+n+1} - \overline{y}_{k,k+n+1} = (\sigma - 1)(\overline{y}_{j,k}) \in \mathfrak{a}\, V$$

is fixed by $\mathcal{I}$. If $m \neq 8$, $\overline{x}_j$ has a unique representative $x_j \in Y$ with exactly 4 non-zero entries, and so $\tau(x_j) = x_j$ for all τ in $\mathcal{I}$. Since

$$\tau(k) \in \bigcap_{j \notin \{k,k+n+1\}} \{j, j + n + 1, k, k + n + 1\} = \{k, k + n + 1\},$$

$\{k, k + n + 1\}$ is an $\mathcal{I}$-orbit and every $\mathcal{I}$-orbit has 2 elements. If $m = 8$, the $\mathcal{I}$-orbits have size at most 4, giving the weaker bound. □

4. Stem field discriminant for $\mathbb{Q}(A[\mathfrak{l}])$ in a special case

In this section, $A_{/\mathbb{Q}}$ is $\mathfrak{o}$-paramodular with good reduction at 2, $\mathfrak{l}$ is a prime of $\mathfrak{o}$ with residue field $\mathbb{F}_2$ and $V = A[\mathfrak{l}]$ is irreducible. Thus V admits a symplectic pairing [4, §3]. Let $F = \mathbb{Q}(V)$ and $G = \mathrm{Gal}(F/\mathbb{Q})$. The elements of V correspond to differences $\theta_i - \theta_j$ of the 6 odd theta characteristics, and we view G as a subgroup of $\mathcal{S}_6$, via its action on Θ^-. Irreducibility of V implies that G has an orbit $\Sigma \subseteq \Theta^-$ of size 5 or 6. If $H = G_\theta$ stabilizes θ in Σ, then $K = F^H$ is a stem field for F, with $[K : \mathbb{Q}] = |\Sigma|$.

The following local building blocks are used in the next result. Let X be the irreducible $G_{\mathbb{Q}_2}$-module such that $\dim_{\mathbb{F}_2} X = 2$ and $\tilde{E} = \mathbb{Q}_2(X) = \mathbb{Q}_2(\boldsymbol{\mu}_3, \sqrt[3]{2})$. The exhaustive list [13] of 2-adic fields of low degree, or class field theory, shows that there is a unique quartic extension $\tilde{M}/\mathbb{Q}_2$ whose Galois closure $\tilde{L}$ has non-trivial tame ramification, necessarily of degree 3. Then $\tilde{M}/\mathbb{Q}_2$ is totally ramified, $\mathrm{ord}_2(d_{\tilde{M}/\mathbb{Q}_2}) = 4$, $\tilde{L}$ contains $\tilde{E}$ and $\mathrm{Gal}(\tilde{L}/\mathbb{Q}_2) \simeq \mathcal{S}_4$, with inertia subgroup $\mathcal{A}_4$.

Proposition 4.1. $\mathrm{ord}_2(d_{K/\mathbb{Q}}) \leq 4$ (*resp.* 6) *if* $[K : \mathbb{Q}] = 5$ (*resp.* 6).

Proof. If V is ordinary at 2, the result follows from Proposition 3.15 or 3.16. Hence we suppose F has non-trivial tame ramification over 2. Among primes over 2 in K, choose λ with maximal ramification degree $e_\lambda(K)$ and consider all possibilities:

i) $e_\lambda(K) = 5$. Then $(2)\mathcal{O}_K = \lambda^5$ or $\lambda^5\lambda'$, depending on whether K is quintic or sextic, and $\mathrm{ord}_2(d_{K/\mathbb{Q}}) = 4$ by tame theory.

ii) $e_\lambda(K) = 3$. If K is quintic, the worst case occurs when $(2)\mathcal{O}_K = \lambda^3(\lambda')^2$, and then we have $\mathrm{ord}_2(d_{K/\mathbb{Q}}) = \mathrm{ord}_2(d_{K_\lambda/\mathbb{Q}_2}) + \mathrm{ord}_2(d_{K_{\lambda'}/\mathbb{Q}_2}) = 2 + 2 = 4$. Suppose K is sextic. If $(2)\mathcal{O}_K = (\lambda\lambda')^3$ or λ^3 with residue degree $f_\lambda(K) = 2$, we have

$\mathrm{ord}_2(d_{K/\mathbb{Q}}) = 4$. In the remaining cases, at most one more prime λ' over 2 ramifies in K, with $e_{\lambda'}(K) = 2$, and we conclude as for quintics.

iii) $e_\lambda(K) = 4$. Then the completion $K_\lambda = \tilde{M}$. If $[K:\mathbb{Q}] = 5$, the other prime over 2 in K is unramified, but if $[K:\mathbb{Q}] = 6$, there may at worst be some λ' with $e_{\lambda'}(K) = 2$. Hence

$$\mathrm{ord}_2(d_{K/\mathbb{Q}}) \le \begin{cases} 4 & \text{if } [K:\mathbb{Q}] = 5, \\ 4+2=6 & \text{if } [K:\mathbb{Q}] = 6. \end{cases}$$

iv) $e_K(\lambda) = 6$, so $[K:\mathbb{Q}] = 6$, $(2)\mathcal{O}_K = \lambda^6$ and the inertia group $\mathcal{I}$ of λ acts transitively on Θ^-. Since a non-zero fixed point for the action of $\mathcal{I}$ on V corresponds to a pair of theta characteristics preserved by $\mathcal{I}$, contradicting transitivity, there are none. The tame ramification group $\mathcal{I}/\mathcal{I}_1$ is a cyclic subgroup of $\mathcal{S}_6$ whose order is odd and a multiple of 3. Hence $|\mathcal{I}/\mathcal{I}_1| = 3$.

Because $\mathcal{I}_1$ is a non-trivial 2-group, normal in its decomposition group $\mathcal{D}$, the fixed space $W = V^{\mathcal{I}_1}$ is a non-zero $\mathcal{D}$-module, properly contained in V. Viewed as an $\mathcal{I}/\mathcal{I}_1$-module, W is semisimple. But $\mathcal{I}/\mathcal{I}_1$ has no non-zero fixed points on W, as they would be fixed points of $\mathcal{I}$, so $\dim W = 2$ and $W \simeq X$.

Viewed as a finite flat group scheme over $\mathbb{Z}_2$, $\mathcal{V} = A[\mathfrak{l}]$ is Cartier self-dual. The multiplicative component $\mathcal{V}^m$ cannot have order 4, since $\mathcal{I}$ is not a 2-group, nor can it have order 2, since $\mathcal{I}$ has no non-trivial fixed points. Hence $\mathcal{V}^m = 0$ and $\mathcal{V}$ is fully biconnected. There is a subgroup scheme $\mathcal{W}$ of $\mathcal{V}$ with $\mathcal{D}$-module W, and $\mathcal{V}/\mathcal{W}$ is biconnected, so its $\mathcal{D}$-module also is isomorphic to X.

Schoof [20, Prop, 6.4] showed that if V is an extension of X by X as a $\mathcal{D}$-module, then $\mathbb{Q}_2(V)$ is contained in the maximal elementary 2-extension $\tilde{L}_1$ of $\tilde{E}$ with ray class conductor exponent 2. One checks that $\tilde{L}_1$ is an unramified central extension of degree 2 over $\tilde{L}$ and the root discriminant of $\tilde{L}_1/\mathbb{Q}_2$ is 7/6. Since $\mathrm{ord}_2(d_{K/\mathbb{Q}})$ is even, we have $\mathrm{ord}_2(d_{K/\mathbb{Q}}) \le 6$, as claimed. □

5. Preserving the Fontaine bound

Let K'/K be a Galois extension of ℓ-adic fields with Galois group G. Denote the ring of integers of K' by $\mathcal{O}'$ and a prime element by λ'. Set

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

so G_0 is the inertia group and $t_{K'/K} = [G_0 : G_1]$ is the degree of tame ramification. If $\lfloor x \rfloor = m$, the Herbrand function is given by

$$\varphi_{K'/K}(x) = \frac{1}{|G_0|}\left(|G_1| + \cdots + |G_m| + (x-m)|G_{m+1}| \right) \tag{5.1}$$

and is continuous and increasing. In the upper numbering used by Serre [21, IV], $G^m = G_n$, with $m = \varphi_{K'/K}(n)$. In the numbering of [7] or [13], this group is denoted by $G^{(m+1)}$. Let $\psi_{K'/K}$ be the inverse of $\varphi_{K'/K}$.

Notation 5.2. Let $c = c_{K'/K}$ be the maximal integer such that $G_c \ne 1$. We omit the lower field if $K = \mathbb{Q}_\ell$. Let $m_{K'} = \psi_{K'/\mathbb{Q}_\ell}(\frac{1}{\ell-1})$.

Wild ramification in K'/K is equivalent to $c_{K'/K} \ge 1$. If G_1 is not abelian, then $c_{K'/K} \ge 2$, since successive quotients in the ramification filtration are elementary abelian ℓ-groups. By (5.1), $m_{K'}$ is an integer when $(\ell-1)$ divides $t_{K'/\mathbb{Q}_\ell}$.

Lemma 5.3. *Let $E \supset F$, both Galois over K, $G = \mathrm{Gal}(E/K)$ and $H = \mathrm{Gal}(E/F)$. Then $1 \to H^{\psi_{F/K}(x)} \to G^x \xrightarrow{res} \mathrm{Gal}(F/K)^x \to 1$ is exact. In addition,*

$$m_E \geq t_{E/F} m_F \quad \text{and} \quad c_{E/K} \geq t_{E/F} c_{F/K}. \tag{5.4}$$

Proof. By compatibility with quotients, *res* is surjective and its kernel is

$$G^x \cap H = G_{\psi_{E/K}(x)} \cap H = H_{\psi_{E/K}(x)} = H^{\varphi_{E/F}\psi_{E/K}(x)} = H^{\psi_{F/K}(x)},$$

since $\psi_{E/K} = \psi_{E/F}\,\psi_{F/K}$. Thus the sequence is exact.

Equation (5.1) implies that $t_{E/F}\varphi_{E/F}(z) \leq z$, so $\psi_{E/F}(z) \geq t_{E/F} z$. If $x = \varphi_{F/K}(c_{F/K})$, then $G_{\psi_{E/K}(x)} = G^x \neq 1$ by surjectivity of *res*. Hence

$$c_{E/K} \geq \psi_{E/K}(x) = \psi_{E/F}\psi_{F/K}(x) = \psi_{E/F}(c_{F/K}) \geq t_{E/F}\, c_{F/K},$$

and similarly for $m_E \geq t_{E/F}\, m_F$. □

Definition 5.5. Let F be the Galois closure of $K/\mathbb{Q}_\ell$. We say K is *Fontaine* if $\mathrm{Gal}(F/\mathbb{Q}_\ell)^u = 1$ for all $u > \frac{1}{\ell-1}$ or, equivalently, $c_F \leq m_F$.

Lemma 5.6. *Let $E \supset F$, both Galois over $\mathbb{Q}_\ell$, $G = \mathrm{Gal}(E/\mathbb{Q}_\ell)$ and $H = \mathrm{Gal}(E/F)$. Then:*

i) *If $t_{F/\mathbb{Q}_\ell} = \ell - 1$, then $m_E \geq t_{E/F}$, with equality when G_0 is abelian.*
ii) *Let F be Fontaine, with non-trivial wild ramification. Then $1 \leq c_F \leq m_F$. Assume further that $t_{F/\mathbb{Q}_\ell} = \ell - 1$. Then $c_F = m_F = 1$ and, if E is Fontaine, then $c_E = m_E$.*

Proof. i) Since $\varphi_{F/\mathbb{Q}_\ell}(1) = \frac{1}{\ell-1}$, we have $m_F = 1$, so $m_E \geq t_{E/F}$ by (5.4). If G_0 is abelian and $t_{E/\mathbb{Q}_\ell}$ does not divide j, then $G_j = G_{j+1}$ by [21, IV, §2]. Thus the definition gives $\varphi_{E/\mathbb{Q}_\ell}(t_{E/F}) = \frac{1}{\ell-1}$, whence $m_E = t_{E/F}$.

ii) By Definition 5.5, $\varphi_{F/\mathbb{Q}_\ell}(c_F) \leq \frac{1}{\ell-1} = \varphi_{F/\mathbb{Q}_\ell}(m_F)$. Hence $c_F \leq m_F$. If $t_{F/\mathbb{Q}_\ell} = \ell - 1$, then $m_F = 1$, so $c_F = 1$. Surjectivity of *res* in Lemma 5.3 implies that $G^{\frac{1}{\ell-1}} \neq 1$. If E is Fontaine, it follows that $c_E = \psi_{E/\mathbb{Q}_\ell}(\frac{1}{\ell-1}) = m_E$. □

Example 5.7. By class field theory or the table of quartics [13], there is a unique Fontaine $\mathcal{S}_4$-extension $F/\mathbb{Q}_2$. The ramification subgroups of $\overline{G} = \mathrm{Gal}(F/\mathbb{Q}_2)$ are $\overline{G}_0 \simeq \mathcal{A}_4$, $\overline{G}_1 \simeq C_2^2$ and $\overline{G}_2 = 1$, so $c_F = 1$, $\varphi_{F/\mathbb{Q}_2}(x) = (4+(x-1))/12$ if $x \geq 1$ and $m_F = 9$. Moreover, $E = F(i)$ remains Fontaine, with $G = \mathrm{Gal}(E/\mathbb{Q}_2) \simeq \mathcal{S}_4 \times C_2$. Lemma 5.6(ii) may be used to show that $|G_0| = 24$, $|G_1| = 8$, $|G_2| = \cdots = |G_9| = 2$, $|G_{10}| = 1$ and $c_E = m_E = 9$. Alternatively, E has two stem fields of degree 6, and this determines E uniquely in [13].

Lemma 5.8. *Let M/F be abelian, with $F/\mathbb{Q}_\ell$ Galois. Then M is Fontaine if and only if F is Fontaine and the ray class conductor exponent $\mathfrak{f}(M/F) \leq \lfloor m_F \rfloor + 1$.*

Proof. If E is the Galois closure of $M/\mathbb{Q}_\ell$, then E/F is abelian and we have $\mathfrak{f}(E/F) = \mathfrak{f}(M/F) = \varphi_{E/F}(c_{E/F}) + 1$; cf. [21, XV, §2]. The exact sequence of Lemma 5.3 with $K = \mathbb{Q}_\ell$ implies our claim. □

Remark 5.9. Let E be a *number field* with root discriminant ϱ_E. Write $\tilde{E}$ for the completion of E at a prime $\lambda \,|\, \ell$ and $e_{\tilde{E}}$ for the absolute ramification degree. Suppose E contains F, both Galois over $\mathbb{Q}$, with $\tilde{E}$ Fontaine. Then

$$\mathrm{ord}_\ell(\varrho_E) \leq 1 + \tfrac{1}{\ell-1} - \tfrac{t_{\tilde{E}/\tilde{F}}\, c_{\tilde{F}}+1}{e_{\tilde{E}}}.$$

Indeed, if $\mathfrak{D}_{\tilde{E}/\mathbb{Q}_\ell}$ is the different, then [21, IV, Prop. 4] and [7, Prop. 1.3] give

$$\operatorname{ord}_\ell(\varrho_E) = \frac{1}{e_{\tilde{E}}} \operatorname{ord}_\lambda(\mathfrak{D}_{\tilde{E}/\mathbb{Q}_\ell}) = 1 + \varphi_{\tilde{E}/\mathbb{Q}_\ell}(c_{\tilde{E}}) - \frac{c_{\tilde{E}}+1}{e_{\tilde{E}}}.$$

We conclude by Definition 5.5 and equation (5.4). □

Because the upper numbering is compatible with quotients, the composition of Fontaine fields is Fontaine and there is a maximal field L, such that $\operatorname{Gal}(F/\mathbb{Q}_\ell)^u = 1$ for all Galois subfields F finite over $\mathbb{Q}_\ell$ and all $u > \frac{1}{\ell-1}$. Since $F = \mathbb{Q}_\ell(\boldsymbol{\mu}_\ell, (1-\ell)^{\frac{1}{\ell}})$ is contained in L, Lemma 5.6(ii) implies a gap in the upper numbering:

$$\operatorname{Gal}(L/\mathbb{Q}_\ell)^{\frac{1}{\ell-1}} \neq \operatorname{Gal}(L/\mathbb{Q}_\ell)^{\frac{1}{\ell-1}+\epsilon} \text{ for } \epsilon > 0.$$

Hajir and Maier [10] study number field extensions K'/K of *bounded depth*, i.e., with vanishing ramification groups $\mathcal{D}_\mathfrak{p}(K'/K)^x$ for all $x \geq \nu_\mathfrak{p}$. When there is deep wild ramification, the concept of Galois slope content introduced by Jones and Roberts [13] and used in [12, §1.4] leads to variants of (5.4) and Remark 5.9, not required for our applications, thanks to Definition 1.1(iii).

6. Using Odlyzko

We study some maximal (ℓ, N)-controlled extensions $L/\mathbb{Q}$ by means of Odlyzko's bounds [18, 19, 5]. If the $\mathbb{F}[G_\mathbb{Q}]$-module V is semistable and bad only at S, then $\mathbb{Q}(V)$ is (ℓ, N_S)-controlled. The converse holds for $\ell = 2$ but not for ℓ odd; e.g., if $\dim V = 2$, then $\operatorname{Sym}^2 V$ rarely is semistable.

By tameness at $p \,|\, N$ and the bound of Definition 1.1(iii), the root discriminant of $L/\mathbb{Q}$ satisfies $\varrho_L < \ell^{1+\frac{1}{\ell-1}} N^{1-\frac{1}{\ell}}$. More precisely,

$$\operatorname{ord}_p(\varrho_L) \leq 1 - \ell^{-1} \text{ for all } p \,|\, N \quad \text{and} \quad \operatorname{ord}_\ell(\varrho_L) < 1 + (\ell-1)^{-1}. \tag{6.1}$$

Proposition 6.2. *For $\ell \leq 13$, the maximal $(\ell, 1)$-controlled extension L is $\mathbb{Q}(\mu_{2\ell})$. Under GRH, the same is true for $\ell = 17$ and 19.*

Proof. For ℓ odd, $\mathbb{Q}(\boldsymbol{\mu}_\ell) \subseteq L$ and $n = [L:\mathbb{Q}]$ is a multiple of $\ell - 1$. From (6.1) and [18], we find M in Table 1 below such that $n \leq (\ell-1)M$. If $\ell = 13, 17, 19$, we see that $M < \ell$, so $L/\mathbb{Q}$ is tame at ℓ and $\varrho_L \leq \ell^{1-\alpha}$, with $\alpha = ((\ell-1)M)^{-1}$. One gets a new bound $n \leq (\ell-1)M'$ with $M' \leq 5$. If $\ell \leq 11$, we have $M \leq 5$. In both cases, L is abelian over $\mathbb{Q}(\boldsymbol{\mu}_{2\ell})$, and so $L = \mathbb{Q}(\boldsymbol{\mu}_{2\ell})$ by class field theory [3, Lem. 2.2]. Use $\mathbb{Q}(i) \subseteq L$ for $\ell = 2$. □

Table 1. Odlyzko bounds for $(\ell, 1)$-controlled fields

ℓ	2	3	5	7	11	13	17	19
$\varrho_L \leq$	4	5.197	7.477	9.682	13.981	16.099	20.294	22.377
M	2	3	3	3	5	7	8	10

Now suppose L is maximal $(2, N)$-controlled, so $\varrho_L < 4N^{\frac{1}{2}}$ by (6.1). If $n = [L:\mathbb{Q}]$ is finite, [18, Tables 3, 4] provides B, E, depending on a parameter b, such that $\varrho_L > Be^{-\frac{E}{n}}$. In Table 2 below, we find a best bound for $n < E/\log(B/4N^{\frac{1}{2}})$ by varying $B > 4N^{\frac{1}{2}}$, unconditionally for $N \leq 21$ and under GRH for larger N.

If V is an irreducible semistable $\mathbb{F}_2[G_\mathbb{Q}]$-module good outside S and $N_S | N$, then $\operatorname{Gal}(\mathbb{Q}(V)/\mathbb{Q})$ factors through $\overline{G} = G/H$, where H is the maximal normal

2-subgroup of $G = \mathrm{Gal}(L/\mathbb{Q})$. For odd $N \le 79$ and $N = 97$, we find a subfield F of L containing L^H by composing a solvable extension of $\mathbb{Q}$ with a subfield of $\mathbb{Q}(J_0(N)[2])$. Then we use the improvements in §5 on the bound (6.1) for ϱ_L, together with the Odlyzko tables and Magma [2] to control $[L:F]$.

TABLE 2. Bounds on $n = [L:\mathbb{Q}]$ for $(2,N)$-controlled fields L

N	3	5	7	11	13	15	17	19	21	23	29
$n \le$	10	16	22	42	56	74	100	138	192	98	155
N	31	33	35	37	39	41	43	47	51	53	55
$n \le$	181	210	244	284	330	385	449	615	852	1007	1196
N	57	59	61	65	67	69	71	73	77	79	97
$n \le$	1427	1710	2061	3046	3743	4638	5800	7332	12042	15766	470652

Theorem 6.3 (GRH)**.** *Let V be semistable and irreducible over $\mathbb{F}_2$. If V is bad exactly over S and $N = N_S \le 79$ or $N = 97$, the following hold:*

i) *no such V exists for N in $\{3,5,7,13,15,17,21,33,39,41,55,57,65,77\}$;*
ii) *V is unique and $\dim V = 2$ for N in $\{11,19,23,29,31,35,37,43,51,53,61\}$;*
iii) *V is unique for N in $\{23,31,47,71\}$;*
iv) *V is an irreducible $\mathbb{F}_2[\overline{G}]$-module with $\overline{G} = D_9$, $D_3 \times \mathcal{A}_5$, $\mathcal{A}_5$, $D_3 \times D_5$, $\mathrm{SL}_2(\mathbb{F}_8)$ when $N =$ 59, 67, 73, 79, 97 respectively.*

Remark 6.4. Aside from $\mathbb{F}_2$, there are exactly two irreducible $\mathbb{F}_2[\mathcal{A}_5]$-modules, both 4-dimensional, occurring as a submodule V_1 and quotient module V_2 of the permutation module. The non-trivial $\mathbb{F}_2[\mathrm{SL}_2(\mathbb{F}_8)]$-modules have dimensions 6, 8 and 12. Further, the irreducible modules for $G_1 \times G_2$ are the tensor products of irreducibles for G_1 and G_2.

Sketch of the proof. In (i), G is a 2-group, except for 33, 55, 57, 77, when $\overline{G} \simeq D_3$ has a representation whose conductor, 11 or 19, divides N properly. In (ii), $V \simeq C_N[2]$ for an elliptic curve C_N of conductor N, except that $V \simeq J_0(29)[\sqrt{2}]$ for $N = 29$. In (iii), V is the $\mathbb{F}_2[D_h]$-module of dimension $h-1$ induced by the Hilbert class field over $\mathbb{Q}(\sqrt{-N})$ of class number $h =$ 3, 3, 5, 7 corresponding to $N =$ 23, 31, 47, 71 respectively.

N $= 59$: The two irreducibles are the constituents of $J_0(59)[2]$, using an equation for $X_0(59)$, namely $y^2 = f(x)g(x)$ with $f = x^3 - x^2 - x + 2$ and

$$g = x^9 - 7x^8 + 16x^7 - 21x^6 + 12x^5 - x^4 - 9x^3 + 6x^2 - 4x - 4.$$

The Galois group of g is D_9, and a root of f gives a cubic subfield.

N $= 67$: Let $V_1 = C_{67}[2]$ and $V_2 = J_0^+(67)[2]$. Then $\mathrm{Gal}(\mathbb{Q}(V_2)/\mathbb{Q}) = \mathrm{SL}_2(\mathbb{F}_4)$ and $[L:\mathbb{Q}(V_1,V_2,i)] \le 2$.

We provide more details for $N = 73$, 77, 79 and 97. Let E be the maximal abelian extension of $\mathbb{Q}$ in L. Since G is generated by involutions, $E/\mathbb{Q}$ is the elementary 2-extension generated by i and $\sqrt{p}$ as p ranges over S.

Lemma 6.5. *Let $M \supset F$ be subfields of L containing E and Galois over $\mathbb{Q}$. Set $T = \mathrm{Gal}(M/F)$ and assume $\lambda \,|\, 2$ is totally ramified of odd degree $t = |T| > 1$ in M/F. Then $t = 3$ and the residue degree $f_\lambda(E/\mathbb{Q}) = 2$.*

Proof. Since the image of $\alpha\colon \mathrm{Gal}(M/\mathbb{Q}) \to \mathrm{Aut}(T)$ by conjugation is abelian, E contains $M_0 = L^{\ker \alpha}$, and so $f = f_\lambda(M_0/\mathbb{Q}) \le f_\lambda(E/\mathbb{Q}) \le 2$. Any Frobenius in $\mathcal{D}_\lambda(M/M_0)$ acts trivially on T. Thus $2^f \equiv 1 \pmod t$ and the claim ensues. □

Remark 6.6. Let $M \supseteq F$ be subfields of L containing $\mathbb{Q}(i, \sqrt{N})$ and Galois over $\mathbb{Q}$. Denote the residue, ramification and tame degree of λ in $F/\mathbb{Q}$ by f_0, e_0 and t_0 respectively. Given an *a priori* bound $[M\colon F] \le b$, consider possible factorizations $[M\colon F] = 2^s t_1 u_1$, where 2^s is the degree of wild ramification, t_1 the degree of tame ramification and $u_1 = f_1 g_1$ the unramifed (inert and split) degree of λ in M/F. The resulting tame ramification in $M/\mathbb{Q}$ requires that the completion M_λ contain $\boldsymbol{\mu}_{t_0 t_1}$, and so $2^{f_0 f_1} \equiv 1 \pmod{t_0 t_1}$.

For each s with $0 \le s \le \log_2 b$, let $t_1 \ge 1$ run through odd integers at most $b/2^s$. Set $\beta = (c_F\, t_1 + 1)/(2^s\, t_1\, e_0)$, as in Remark 5.9, and let n_β be the Odlyzko bound on $[M\colon\mathbb{Q}]$ when $\varrho_M \le 2^{2-\beta}\sqrt{N}$. Then $1 \le g_1 \le n_\beta/(2^s t_1 f_1\,[F\colon\mathbb{Q}])$. Values of s, t_1, f_1 not satisfying the congruence and inequality above are ruled out.

Let E_1 be the maximal subfield of L abelian over E. By Lemmas 5.6(ii) and 5.8, the ray class conductor of E_1/E divides $(1+i)^2\mathcal{O}_E$. Then class field theory or Magma gives Table 3 below.

TABLE 3. Decomposition type of $\lambda|2$ in E_1

N	$\mathrm{Gal}(E_1/E)$	$e_\lambda(E_1/\mathbb{Q})$	$f_\lambda(E_1/\mathbb{Q})$	$g_\lambda(E_1/\mathbb{Q})$
73	C_4	4	2	2
77	C_6	6	2	4
79	C_{15}	2	5	6
97	C_4	4	2	2

N = 73: The Jacobian $J_0^+(73)$ has RM by $\mathbb{Q}(\sqrt{5})$ and the Galois group of its 2-division field K is $\mathrm{SL}_2(\mathbb{F}_4) \simeq \mathcal{A}_5$. For the 5 primes over 2 in K, $f_\lambda(K/\mathbb{Q}) = 3$ and Frobenius acts irreducibly on $\mathcal{I}_\lambda(K/\mathbb{Q}) \simeq C_2^2$. Since Frobenius is reducible on $\mathcal{I}_\lambda(E_1/\mathbb{Q}) \simeq C_2^2$, we have $\mathcal{I}_\lambda(F/\mathbb{Q}) \simeq C_2^4$ for the compositum $F = E_1K$, thus $[F\colon\mathbb{Q}] = 960$. By Table 2, $[L\colon\mathbb{Q}] = 960r \le 7332$, so $r \le 7$. Lemma 6.5 implies the tame degree $t_\lambda(L/F) = 1$, so $e_\lambda(L/F)$ divides 4. Finally, $[L\colon F]$ divides 4 by Remark 6.6.

N = 77: In the $\mathcal{S}_3$-field $K_0 = \mathbb{Q}(J_0(11)[2]) = \mathbb{Q}(\sqrt{-11}, \theta)$, with $\theta^3 - 2\theta^2 + 2 = 0$, the decomposition type over 2 is $e_\lambda = 3$, $f_\lambda = 2$, $g_\lambda = 1$. If $K = E(\theta) = K_0(i, \sqrt{-7})$, then $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_2 \times C_2 \times \mathcal{S}_3$ and $\mathcal{I}_\lambda(K/\mathbb{Q}) \simeq C_6$, so $m_K = 3$ by Lemma 5.6(i). If F is the maximal subfield of L abelian over K, the ray class conductor of F/K divides $(1+i)^4\mathcal{O}_K = 4\mathcal{O}_K$ by Lemma 5.8. Then $\mathrm{Gal}(F/K) \simeq C_2 \times C_2 \times C_4$ and the decomposition type of 2 is $e_\lambda(F/\mathbb{Q}) = 48$, $f_\lambda(F/\mathbb{Q}) = 2$ and $g_\lambda(F/\mathbb{Q}) = 4$.

A group of order $3 \cdot 2^a$ admits a unique quotient isomorphic to C_3 or $\mathcal{S}_3$. If $[L\colon K_0] = 3 \cdot 2^a$, there is a C_3 or $\mathcal{S}_3$ extension of K_0. The latter provides a central quadratic M_0/K_0, with $M_0/\mathbb{Q}$ Galois and $\mathrm{Gal}(M_0/\mathbb{Q}) \simeq D_6$. In both cases, we find that $\mathrm{Gal}(M_0K/K) \simeq C_3$, contradicting $[F\colon K] = 16$.

We claim that $\mathrm{Gal}(L/F)$ is a 2-group. If not, since $[L\colon F] \le 31$ from Table 2 and $[L\colon F] \ne 3 \cdot 2^a$, the wild ramification degree $|\mathcal{I}_\lambda(L/F)_1|$ divides 4. Example 5.7 and (5.4) imply that $\mathcal{I}_\lambda(F/\mathbb{Q})_9 \ne 1$. Use Remark 6.6 with $c_F \ge 9$ to show that the only remaining case is $[L\colon F] = 10$, with tame degree $t_\lambda(L/F) = 5$ and wild degree 2. It is precluded by Lemma 6.5.

Thus the kernel of the surjection $G \xrightarrow{\eta} \mathrm{Gal}(\mathbb{Q}(J_0(11)[2])/\mathbb{Q}) \simeq \mathcal{S}_3$ is a 2-group and irreducible representations V of G factor through $\mathrm{Image}\,\eta$, of conductor 11, so there is no V of conductor 77.

$\mathbf{N} = 79$: The strict class fields $H^{\pm}$ of $\mathbb{Q}(\sqrt{\pm 79})$ have respective orders 3 and 5, and so $E_1 = H^+H^-$. Let $K^{\pm}$ be the maximal subfields of L abelian respectively over $H^{\pm}(i)$. Since $e_\lambda(H^{\pm}(i)/\mathbb{Q}) = 2$, the ray class conductors of $K^{\pm}/H^{\pm}(i)$ divide $(1+i)^2\mathcal{O}_{H^{\pm}(i)}$ by Lemma 5.8. Magma provides the following information:

$$\begin{aligned} \mathrm{Gal}(K^+/H^+(i)) &\simeq C_2^2 \times C_3, \quad \text{with } e_\lambda = 2,\ f_\lambda = 2,\ g_\lambda = 3; \\ \mathrm{Gal}(K^-/H^-(i)) &\simeq C_2^4 \times C_5, \quad \text{with } e_\lambda = 16,\ f_\lambda = 5,\ g_\lambda = 1. \end{aligned}$$

If $\mathrm{Gal}(E_1/E) = \langle\tau\rangle$, then τ^5 and τ^3 act trivially on K^+ and K^- respectively. Hence τ is trivial on $K^+ \cap K^-$ and $(K^+ \cap K^-)/E$ is abelian. Since $K^+ \cap K^-$ contains E_1, equality holds by maximality of E_1. For $F = K^+K^-$, we therefore have $[F : E_1] = 2^6$, $[F : \mathbb{Q}] = 3840$ and $[L : \mathbb{Q}] = 3840r$, with $r \le 3$. Because Frobenius acts irreducibly on $\mathcal{I}_\lambda(K^-/E_1) \simeq C_2^4$ but trivially on $\mathcal{I}_\lambda(K^+/E_1) \simeq C_2$, we see that $\mathcal{I}_\lambda(F/E_1) \simeq C_2^5$ and $e_\lambda(F/\mathbb{Q}) = 64$. By Lemma 6.5, $t_\lambda(L/F) = 1$, so $[L : F] \le 2$ by Remark 6.6. Thus the kernel of $G \twoheadrightarrow \mathrm{Gal}(H^+/\mathbb{Q}) \times \mathrm{Gal}(H^-/\mathbb{Q}) \simeq D_3 \times D_5$ is a 2-group.

$\mathbf{N} = 97$: There is a subfield K of $\mathbb{Q}(J_0(97)[2])$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{SL}_2(\mathbb{F}_8)$ and decomposition type $e_\lambda(K/\mathbb{Q}) = 8$, $f_\lambda(K/\mathbb{Q}) = 7$, $g_\lambda(K/\mathbb{Q}) = 9$. A Frobenius in $\mathcal{D}_\lambda(K/\mathbb{Q})$ acts irreducibly on $\mathcal{I}_\lambda(K/\mathbb{Q}) \simeq C_2^3$ but reducibly on $\mathcal{I}_\lambda(E_1/\mathbb{Q}) \simeq C_2^2$, so $\mathcal{I}_\lambda(F/\mathbb{Q}) \simeq C_2^5$ for the compositum $F = E_1K$. Table 2 implies that $[L : F] \le 58$, since $[F : \mathbb{Q}] = 504 \cdot 16 = 8064$. Thus the dimensions of irreducible representations of $\mathrm{SL}_2(\mathbb{F}_8)$ over $\mathbb{F}_p$ for small p force the action of $\mathrm{Gal}(F/E_1)$ on the maximal abelian quotient of $\mathrm{Gal}(L/F)$ to be trivial. But no central extension of $\mathrm{SL}_2(\mathbb{F}_8)$ is perfect [1, 11]. Hence L is the compositum of F with a solvable extension of E_1. The ray class extension of E_1 whose conductor divides $\prod \lambda^2$, as λ runs over the primes above 2 in $\mathcal{O}_{E_1}$, turns out to be trivial, whence $L = F$ by Lemmas 5.6(ii) and 5.8.

The asymptotic root discriminant bound of [19] is $8\pi e^\gamma \approx 44.763$, where γ is Euler's constant. Hence, by (6.1), the degree of L is finite for odd squarefree N at most 123. It would thus be entertaining to find L when $N = 127$. Below, we exhibit a subfield F of L of degree 161280 whose root discriminant ϱ_F just exceeds the asymptotic bound.

To construct F, we begin the solvable tower with $E_0 = E = \mathbb{Q}(i, \sqrt{127})$ and find successive maximal abelian extensions E_{j+1}/E_j in $L/\mathbb{Q}$. For ray class conductor $(1+i)^2\mathcal{O}_E$, we have $[E_1 : E] = 5$. Thus E_1 is the compositum of $\mathbb{Q}(i)$ and the Hilbert class field over $\mathbb{Q}(\sqrt{-127})$. Now $e_\lambda(E_1/\mathbb{Q}) = 2$, so the ray class conductor of E_2/E_1 divides $(1+i)^2\mathcal{O}_{E_1}$ and we have $\mathrm{Gal}(E_2/E_1) = C_2^4$. Moreover, any Frobenius in $\mathcal{D}_\lambda(E_2/\mathbb{Q})$ has irreducible action of order 5 on this ray class group. The decomposition type over 2 is $e_\lambda(E_2/\mathbb{Q}) = 32$, $f_\lambda(E_2/\mathbb{Q}) = 5$, $g_\lambda(E_2/\mathbb{Q}) = 2$. The ray class conductor of E_3/E_2 divides $\prod \lambda^2$, as λ runs over the primes of $\mathcal{O}_{E_2}$ above 2, but we do not know whether $E_3 = E_2$.

Also, there is a subfield K of $\mathbb{Q}(J_0(127)[2])$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{SL}_2(\mathbb{F}_8)$ and $e_\lambda(K/\mathbb{Q}) = 8$, $f_\lambda(K/\mathbb{Q}) = 7$, $g_\lambda(K/\mathbb{Q}) = 9$. Any Frobenius in $\mathcal{D}_\lambda(K/\mathbb{Q})$ has irreducible action of order 7 on $\mathcal{I}_\lambda(K/\mathbb{Q}) \simeq C_2^3$. For the compositum $F = E_2K$, of degree $320 \cdot 504 = 161280$, we therefore have $\mathcal{I}_\lambda(F/\mathbb{Q}) \simeq C_2^8$, and so $c_F = m_F = 1$ by Lemma 5.6. Then $\varrho_F = 2^{2-\frac{1}{128}}\sqrt{127} \approx 44.834$ by Remark 5.9.

References

[1] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 1986. MR895134 (89b:20001)

[2] W. Bosma, J. Cannon and C. Playoust. The Magma algebra system. I. The user language. J. Symb. Comp., **24** (1997) 235–265. MR1484478

[3] A. Brumer and K. Kramer, Semistable Abelian varieties with small division fields. *Galois Theory and Modular Forms*, Hashimoto, Miyake, Nakamura, eds., Kluwer, 2003, 13–38. MR2059756 (2005m:11106)

[4] A. Brumer and K. Kramer, Paramodular abelian varieties of odd conductor, math arXiv:1004.4699.

[5] F. Diaz y Diaz, Tables minorant la racine n-ième du discriminant d'un corps de degré n, Ph.D. Thesis, Publ. Math. Orsay, 1980.

[6] R.H. Dye, Interrelations of symplectic and orthogonal groups in characteristic two, J. of Algebra, **59** (1979) 202–221. MR541675 (81c:20028)

[7] J.-M. Fontaine, Il n'y a pas de variété abélienne sur $\mathbb{Z}$, Invent. Math., **81** (1985) 515–538. MR807070 (87g:11073)

[8] B. H. Gross and J. Harris, On some geometric constructions related to theta characteristics. *Contributions to automorphic forms, geometry, and number theory*, Hida et al., eds., Johns Hopkins, 2004, 279–312. MR2058611 (2005h:14079)

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

[10] F. Hajir and C. Maire, Extensions of number fields with wild ramification of bounded depth, Inter. Math. Res. Notices, **13** (2002) 667-696. MR1890847 (2002m:11096)

[11] B. Huppert, *Endliche Gruppen. I*, Springer-Verlag, 1967. MR0224703 (37:302)

[12] J. Jones, Wild ramification bounds and simple group Galois extensions ramified only at 2, Proc. Amer. Math. Soc., **139** (2011) 807–821. MR2745634

[13] J. Jones and D. Roberts, Local fields, J. Symbolic Computation, **41(1)** (2006) 80–97. MR2194887 (2006k:11230)

[14] J. Jones and D. Roberts, Galois number fields with small root discriminant, J. Number Theory, **122** (2007) 379–407. MR2292261 (2008e:11140)

[15] W.M. Kantor, Subgroups of classical groups generated by long roots, Trans. Amer. Math. Soc., **248** (1979) 347–379. MR522265 (80g:20057)

[16] G. Kemper and G. Malle, The finite irreducible linear groups with polynomial ring of invariants, Transformation Groups, **2** (1997) 57–89. MR1439246 (98a:13012)

[17] J. McLaughlin, Some subgroups of $\mathrm{SL}_n(\mathbb{F}_2)$, Ill. J. Math., **13** (1969) 108–115. MR0237660 (38:5941)

[18] A. Odlyzko, Lower bounds for discriminants of number fields. II, Tôhoku Math. J., **29** (1977) 209–216. MR0441918 (56:309)

[19] A. Odlyzko, Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: A survey of recent results, Sém. Théorie Nombres Bordeaux, **(2)2(1)** (1990) 119–141. MR1061762 (91i:11154)

[20] R. Schoof, Abelian varieties over cyclotomic fields with everywhere good reduction, Math. Ann., **325** (2003) 413–448. MR1968602 (2005b:11076)

[21] J.-P. Serre, *Local Fields*, Graduate Texts in Math., **67**, Springer-Verlag, 1979. MR0554237 (82e:12016)

[22] A. E. Zalesskii and V. N. Serežkin, Finite linear groups generated by reflections, Math. USSR Izv., **17** (1981) 477–503. MR603578 (82i:20060)

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

Department of Mathematics, Queens College and the Graduate Center (CUNY), 65-30 Kissena Boulevard, Flushing, New York 11367
E-mail address: kkramer@gc.cuny.edu