COMPOSITIO MATHEMATICA

ARMAND BRUMER
KENNETH KRAMER

The conductor of an abelian variety

Compositio Mathematica, tome 92, n° 2 (1994), p. 227-248
<http://www.numdam.org/item?id=CM_1994__92_2_227_0>

Compositio Mathematica **92**: 227–248, 1994.

The conductor of an abelian variety

ARMAND BRUMER[1] & KENNETH KRAMER[2]

[1]*Mathematics Dept., Fordham University, Bronx, NY 10458;* [2]*Mathematics Dept., Queens College (CUNY), Flushing, NY 11367*

Received 26 February 1993; accepted in revised form 14 June 1993

1. Introduction

In a recent paper, Lockhart, Rosen and Silverman [7] find bounds for the exponents of conductors of abelian varieties, which are fairly sharp in the case of elliptic curves except over certain 2-adic fields. They conjecture the correct upper bound for the conductor of elliptic curves in general and ask for the behavior of the conductor of an abelian variety in the case of wild ramification.

We settle these questions here by methods related to theirs. More systematic use of group theory enables us to derive all the bounds purely from the formalism of Artin conductors and the study of the two simplest cases. These correspond to extensions whose Galois group is either the quaternion group or cyclic of prime order.

Since some of the facts were not in the exact form needed here, we felt that the reader would be best served by a treatment as self-contained as possible.

The hope that one might get better bounds in the presence of real multiplications provided the original impetus for this work. An unexpected application of our results to endomorphism rings of modular abelian varieties can be found in [1].

A finite extension K of $\mathbb{Q}_p$ with absolute ramification index $e_K = v_K(p)$ will be called a p-adic field. Our results appear to be true over any Henselian field with perfect residue field and $v(p) < \infty$, but this is of no importance for our applications. We introduce the following function on integers:

$$\lambda_p(n) = \sum_{i=0}^{s} i r_i p^i,$$

where $n = \Sigma_{i=0}^{s} r_i p^i$ is the p-adic expansion of n, with $0 \leqslant r_i \leqslant p-1$.

Our main result gives a sharp answer (cf. Propositions 6.5 and 6.6) to the questions raised in [7].

THEOREM 6.2. *Let A be an abelian variety of dimension g defined over the*

p-adic field K. We have the following bound for the exponent of the conductor:

$$\mathbf{f}(A/K) \leqslant 2g + e_K[pd + (p-1)\lambda_p(d)],$$

where d is the greatest integer in $2g/(p-1)$.

If one has more information about the reduction, then the refined estimate of Proposition 6.11 may be used.

We deduce the results for abelian varieties from new bounds on the conductors of $F[G]$-modules V, where G is the Galois group of an extension L/K of p-adic fields. It is assumed throughout that F is a field of characteristic different from p and that modules are finitely generated. As usual, we write $F(\varphi)$ for the extension generated by the values of the character φ of a representation defined over a field containing F.

Our inequality is most easily stated here for the Artin conductor exponent of an irreducible complex character. See Theorem 5.5 for the more technical estimate needed in the application to abelian varieties.

THEOREM 5.1′. *Suppose that* φ *is an absolutely irreducible complex character of* $G = \mathrm{Gal}(L/K)$. *Let* φ_1 *be a non-trivial irreducible component, of degree* p^d, *of its restriction to the ramification group* G_1. *Then we have* $[\mathbb{Q}(\varphi_1):\mathbb{Q}] = (p-1)p^{h-1}$ *for some h and*

$$\mathbf{f}(\varphi, L/K) \leqslant \left[1 + e_K(h+d) + \frac{e_K}{p-1}\right]\varphi(1).$$

The following simpler consequence, which generalizes the bound for abelian characters ([15], p. 216), can also be proved more directly.

PROPOSITION 5.4′. *Write* $p^{h(G_1)}$ *for the exponent of* G_1 *and let* p^d *be the maximal dimension among absolutely simple components of V as an* $F[G_1]$-*module. Then*

$$\mathbf{f}(V, L/K) \leqslant \left[1 + e_K(h(G_1) + d) + \frac{e_K}{p-1}\right]\dim V.$$

Throughout, we write ζ_n for a primitive nth root of unity and let $\boldsymbol{\mu}_n = \langle\zeta_n\rangle$.

We are most grateful to the authors of [7] for making their preprint available and to Oisín McGuinness for his comments.

2. Preliminaries on conductors

Let K be a p-adic field and let L be Galois over K, with $G = \mathrm{Gal}(L/K)$. Write π_L for a uniformizer of L. We have the descending normal filtration of

ramification groups ([13], IV) in which G_0 is the inertia group and

$$G_i = \{\sigma \in G_0 \mid v_L(\sigma(\pi_L) - \pi_L) \geqslant i + 1\}.$$

Then $[G:G_0] = f_{L/K}$ is the residue degree, $[G_0:G_1]$ is the tame ramification degree and G_1 is a p-group.

For a finite dimensional $F[G]$-module V over a field F of characteristic 0 or $l \neq p$, the conductor exponent is defined by

$$\mathbf{f}(V, L/K) = \sum_{i \geqslant 0} \frac{g_i}{g_0} \dim_F(V/V_i), \tag{2.1}$$

where $V_i = V^{G_i}$ is the subspace of V fixed by G_i and g_i is the order of G_i. Note that this is an additive function of V and that it does not change under extensions of F.

We shall call the least integer c such that the kernel of the representation afforded by V contains G_{c+1} the depth of V *relative to* L/K. If V is a simple $F[G]$-module of depth c, we find that

$$\mathbf{f}(V, L/K) = \sum_{i=0}^{c} \frac{g_i}{g_0} \dim_F V. \tag{2.2}$$

We may express the conductor exponent as

$$\mathbf{f}(V, L/K) = \dim_F(V/V_0) + \mathbf{sw}(V, L/K), \tag{2.3}$$

where the Swan conductor is defined by

$$\mathbf{sw}(V, L/K) = \sum_{i \geqslant 1} \frac{g_i}{g_0} \dim_F(V/V_i).$$

By using the Swan conductor, the computation of conductors is reduced to consideration of the wild ramification group G_1. The following lemma is immediate from the definition and the fact that the order of G_1 is invertible in F.

LEMMA 2.4. *Denote the fixed field of* G_1 *by* K_1. *The Swan conductor* $\mathbf{sw}(V, L/K)$ *is additive on exact sequences of* $F[G]$*-modules and*

$$\mathbf{sw}(V, L/K) = \frac{g_1}{g_0} \mathbf{sw}(V/V_1, L/K_1).$$

The Artin conductor exponent of a class function φ on G, with values in a

field F of characteristic zero, is defined as (cf. [13], VI, §2)

$$\mathbf{f}(\varphi, L/K) = \sum_{i=0}^{\infty} \left(\frac{g_i}{g_0} \varphi(1) - \frac{1}{g_0} \sum_{\sigma \in G_i} \varphi(\sigma) \right).$$

In particular, if φ is the character afforded by an $F[G]$-module V, then $\mathbf{f}(V, L/K) = \mathbf{f}(\varphi, L/K)$. The Artin conductor behaves well with respect to induction or passage to a quotient. More precisely, let H be a subgroup of G whose fixed field M has discriminant $\mathfrak{d}_{M/K}$ and let χ be a character of H. Then the conductor of the induced character $\mathrm{ind}_H^G(\chi)$ is given by

$$\mathbf{f}(\mathrm{ind}_H^G(\chi), L/K) = \mathbf{f}(\chi, L/M) f_{M/K} + v_K(\mathfrak{d}_{M/K}) \deg \chi. \tag{2.5}$$

If L_φ is the subfield of L fixed by the kernel of the representation belonging to φ and $\bar{\varphi}$ is the corresponding faithful character of $\mathrm{Gal}(L_\varphi/K)$, then

$$\mathbf{f}(\varphi, L/K) = \mathbf{f}(\bar{\varphi}, L_\varphi/K). \tag{2.6}$$

When our representation is given over a field of non-zero characteristic, we may use the following lemma to lift to characteristic zero.

LEMMA 2.7. *Suppose that k is a field of prime characteristic l and the order of G is invertible in k. Let W be a $k[G]$-module affording the absolutely irreducible character χ. Then there is a finite extension F of $\mathbb{Q}_l$ and an absolutely simple $F[G]$-module V, with character χ_F, such that χ is the reduction of χ_F modulo the prime above l.*

We have $\dim_k W^N = \dim_F V^N$ for every subgroup N of G. In particular W and V have the same dimension and the same conductor.

Proof. Over a finite extension k_0 of $\mathbf{F}_l(\chi)$, there exists an absolutely simple $k_0[G]$-module W_0 affording the character χ, and $k \otimes_{k_0} W_0 = W$. Replacing W and k by W_0 and k_0, we may assume that $k = k_0$ is a finite field. There exists a finite extension F of $\mathbb{Q}_l$, with ring of integers $\mathcal{O}$ and residue field $k' \supset k$, and a torsion-free $\mathcal{O}[G]$-module T such that $k' \otimes_{\mathcal{O}} T = k' \otimes_k W$ (see [5], V, §12). Moreover, $V = F \otimes_{\mathcal{O}} T$ is absolutely simple. It now suffices to assume that $k' = k$.

Let N be a subgroup of G. Let $\lambda : T \to T$ be multiplication by a prime element of $\mathcal{O}$. If l does not divide $|N|$, then λ induces an isomorphism on $H^1(N, T)$. Taking invariants of the exact sequence

$$0 \to T \xrightarrow{\lambda} T \to W \to 0$$

yields the exact sequence

$$0 \to T^N \xrightarrow{\lambda} T^N \to W^N \to 0.$$

It follows that $\operatorname{rank}_{\mathcal{O}} T^N = \dim_k W^N$. Clearly $\dim_F V^N = \operatorname{rank}_{\mathcal{O}} T^N$ and therefore $\dim_F V^N = \dim_k W^N$. □

3. The cyclic and quaternion cases

In this section, L/K is a totally *wildly* ramified extension with Galois group G. Our goal is to bound the conductor in the special case where G is either cyclic of order p or quaternion of order 8, and only complex characters of G are considered. We also describe the conditions under which the bounds are achieved. In order to study the rationality of the Artin representation, Fontaine [3] gives a wealth of information on ramification groups. The reader will find in his Propositions 4.2 and 4.3 results related to some of the material presented here.

We shall need Hensel's estimate on the discriminant, as quoted by Serre ([13], III, §6). The proof is reviewed here to emphasize that the bound is attained precisely when $v_K(\mathfrak{d}_{L/K}) \equiv -1 \pmod{p^n}$.

LEMMA 3.1. *If L is a totally ramified extension of K of degree p^n, then*

$$v_K(\mathfrak{d}_{L/K}) \leqslant p^n - 1 + np^n e_K,$$

with equality if and only if $v_K(\mathfrak{d}_{L/K}) \equiv -1 \pmod{p^n}$.

Proof. We have $v_K(\mathfrak{d}_{L/K}) = v_L(\mathfrak{D}_{L/K})$, where $\mathfrak{D}_{L/K}$ is the different. Suppose that L is obtained from K by adjoining a root π_L of an Eisenstein equation

$$f(x) = a_{p^n}x^{p^n} + \cdots + a_1 x + \pi_K$$

with $v_K(a_{p^n}) = 0$. Then $v_L(ja_j\pi_L^{j-1}) \equiv j - 1 \pmod{p^n}$ are distinct for $j = 1, \ldots, p^n$. Therefore, we have

$$\begin{aligned} v_L(\mathfrak{D}_{L/K}) = v_L(f'(\pi_L)) &= \min_{1 \leqslant j \leqslant p^n} \{v_L(ja_j\pi_L^{j-1})\} \\ &\leqslant v_L(p^n\pi_L^{p^n-1}) = np^n e_K + p^n - 1 \end{aligned}$$

and clearly $v_L(ja_j\pi_L^{j-1}) \equiv -1 \pmod{p^n}$ if and only if $j = p^n$. □

COROLLARY 3.2. *Suppose that G is cyclic of order p and let φ be a non-trivial character of G of degree* 1. *Then*

$$\mathbf{f}(\varphi, L/K) \leqslant 1 + pe_K/(p-1)$$

with equality if and only if $\mathbf{f}(\varphi, L/K) \equiv 1 \pmod{p}$. *View* $V = \mathbb{Q}(\boldsymbol{\mu}_p)$ *as a faithful* $\mathbb{Q}[G]$*-module. Then* $\mathbf{f}(V, L/K) \leqslant p - 1 + pe_K$.

Proof. We apply the lemma and (2.5), noting that V affords the regular representation of G less the identity. By transport of structure, conjugates of φ have the same conductor. Hence

$$(p-1)\mathbf{f}(\varphi, L/K) = \mathbf{f}(V, L/K) = v_K(\mathfrak{d}_{L/K}) \leqslant p - 1 + pe_K. \qquad \square$$

REMARK 3.3. Another description of when a cyclic extension attains the maximal conductor may be found in ([11], Satz 1). With the notation above, the equalities $v_K(\mathfrak{d}_{L/K}) = p - 1 + pe_K$ and $\mathbf{f}(\varphi, L/K) = 1 + pe_K/(p-1)$ occur if and only if $\boldsymbol{\mu}_p \subset K$ and there exists an element $a \in K$ such that $a \in L^p$ and $v_K(a) \not\equiv 0 \pmod{p}$.

The remaining lemmas are needed to treat the quaternions, but they are just as easily proved for general residue characteristic and may also be useful in strengthening the bound for certain absolutely irreducible representations of dimension p. Recall that the index function is defined by $i(\tau) = v_L(\tau(\pi_L) - \pi_L)$ for $\tau \in G - \{1\}$. The minimal break in the ramification numbering is controlled in the following lemma. Here $\Phi(G)$ denotes the Frattini subgroup of G, generated by pth powers and commutators.

LEMMA 3.4. *Suppose that the first gap in the lower ramification numbering occurs at* $G = G_{f_0 - 1} \neq G_{f_0}$. *If* $\tau \in G - G_{f_0}$, *then* $\tau \notin \Phi(G)$. *We have the bound*

$$i(\tau) = f_0 \leqslant 1 + pe_K/(p-1).$$

If equality holds, then G is cyclic.

Proof. Since G_{f_0} is a normal subgroup of G and G/G_{f_0} is an elementary abelian p-group, we have $\Phi(G) \subset G_{f_0}$ and therefore $\tau \notin \Phi(G)$.

Let χ be a non-trivial character of G of degree 1 whose kernel contains G_{f_0}. By the definition of conductor exponent and (2.6), we have $f_0 = \mathbf{f}(\chi, L/K) = \mathbf{f}(\bar{\chi}, L_\chi/K)$. Then $f_0 \leqslant 1 + pe_K/(p-1)$ by Corollary 3.2 applied to the extension L_χ over K.

Suppose that equality holds. Let K' be the fixed field of τ and let K'' be the fixed field of τ^p. Choose a non-trivial character φ of $\mathrm{Gal}(L/K')$ of degree 1 which vanishes on $\mathrm{Gal}(L/K'')$. By (2.1) and (2.6), we have $f_0 = \mathbf{f}(\varphi, L/K') = \mathbf{f}(\bar{\varphi}, K''/K')$. In view of the fact that $f_0 \equiv 1 \pmod{p}$, we have

$f_0 = 1 + pe_{K'}/(p-1)$ by Corollary 3.2 applied to K'' over K'. It follows that $e_{K'} = e_K$; hence $K' = K$ and $G = \langle\tau\rangle$ is cyclic. □

An improvement in the standard conductor bound for a cyclic tower is possible if the beginning of the tower is "small" in the sense of [12]. Let

$$U_K^{(m)} = \{u \in K \mid v_K(u-1) \geqslant m\}$$

and let N_K^L be the norm map from L to K.

LEMMA 3.5. *Suppose that φ is an irreducible character of the cyclic group G. Then, for any integer t such that $\mathbf{f}(\varphi^{p^t}, L/K) \leqslant 1 + e_K/(p-1)$, we have $\mathbf{f}(\varphi, L/K) \leqslant 1 + te_K + e_K/(p-1)$.*

Proof. By (2.6), we may assume that φ is faithful. If M is the subfield of L fixed by the kernel of φ^{p^t}, then $\mathbf{f}(\varphi^{p^t}, L/K) = \mathbf{f}(\varphi^{p^t}, M/K) = f$, say. According to ([13], XV, §2, Cor. 2 to Thm. 1), f is the usual conductor of abelian local class field theory, in the sense that it is the minimal integer such that $U_K^{(f)} \subset N_K^M(U_M)$.

Fix m to be the greatest integer less than or equal to $1 + te_K + e_K/(p-1)$. If $u \in U_K^{(m)}$, then u is a p^t power in K, say $u = u_1^{p^t}$ for some $u_1 \in U_K^{(m-te_K)}$. Since $m - te_K \geqslant f$ by assumption, u_1 is a norm from M. Write $u_1 = N_K^M(u_M)$ for some $u_M \in U_M$. Then

$$N_K^L(u_M) = N_K^M(u_M^{p^t}) = u.$$

Thus every element of $U_K^{(m)}$ is a norm from L. We conclude that $\mathbf{f}(\varphi, L/K) \leqslant m$. □

REMARK 3.6. A partial inverse of Lemma 3.5 may be found in ([3], Prop. 4.3), or proved by class field theory as above. Namely, if $\mathbf{f}(\varphi^{p^t}, L/K) \geqslant 1 + e_K/(p-1)$, then $\mathbf{f}(\varphi, L/K) = \mathbf{f}(\varphi^{p^t}, L/K) + te_K$.

PROPOSITION 3.7. *Suppose G is the quaternion group of order 8. If ψ is the character of a faithful representation of G of dimension 2, then $\mathbf{f}(\psi, L/K) \leqslant 2 + 6e_K$. Equality holds if and only if there exists an element $a \in K$ such that $a \in L^2$ and $v_K(a)$ is odd.*

Proof. For any $\tau \in G - \{1\}$, of order 4, let K_τ be its fixed field and choose a faithful linear character χ_τ of $H = \mathrm{Gal}(L/K_\tau)$. Since the kernel of χ_τ^2 is $H_{i(\tau)}$, the definition of conductor or (2.2) gives us

$$\mathbf{f}(\chi_\tau^2, L/K_\tau) = i(\tau). \tag{3.8}$$

In particular, suppose that $\tau \in G$ has minimal index. Then by Lemma 3.4, τ has order 4 and $i(\tau) \leqslant 2e_K$. It follows from (3.8) and the bound of Lemma 3.5

that $\mathbf{f}(\chi_\tau, L/K_\tau) \leqslant 1 + 4e_K$. Then by (2.5) and Lemma 3.1, we have

$$\begin{aligned}\mathbf{f}(\psi, L/K) &= \mathbf{f}(\chi_\tau, L/K_\tau) + v_K(\mathfrak{d}_{K_\tau/K}) \\ &\leqslant (1 + 4e_K) + (1 + 2e_K) = 2 + 6e_K. \end{aligned} \tag{3.9}$$

According to Remark 3.3, if there is no element $a \in K$ such that $a \in L^2$ and $v_K(a)$ is odd, then $v_K(\mathfrak{d}_{K_\tau/K}) \leqslant 2e_K$. Therefore, the inequality in (3.9) is strict, as claimed. Assume there is such an element a. We must show that $f(\psi, L/K) = 2 + 6e_K$.

Among elements of G of order 4, choose another $\sigma \neq \tau$ of maximal index. Let φ_τ (resp. φ_σ) be a character of degree 1 on G with kernel equal to $\mathrm{Gal}(L/K_\tau)$, (resp. $\mathrm{Gal}(L/K_\sigma)$). By (2.6) and the definition of conductor (2.1), we have

$$\mathbf{f}(\bar{\varphi}_\tau, K_\tau/K) = \mathbf{f}(\varphi_\tau, L/K) = \tfrac{1}{2}[i(\sigma) + i(\tau)]$$

and

$$\mathbf{f}(\bar{\varphi}_\sigma, K_\sigma/K) = \mathbf{f}(\varphi_\sigma, L/K) = i(\tau).$$

But by Remark 3.3, precisely two of the three quadratic extensions of K in L have conductor exponent $1 + 2e_K$. Since $i(\tau) \leqslant 2e_K$ we must have $(i(\sigma) + i(\tau))/2 = 1 + 2e_K$. Therefore, $i(\sigma) = 2 + 4e_K - i(\tau)$. In particular, $i(\sigma) > 1 + 2e_K$.

By (3.8) with τ replaced by σ, we have $\mathbf{f}(\chi_\sigma^2, L/K_\sigma) = i(\sigma)$. Remark 3.6 therefore gives us

$$\mathbf{f}(\chi_\sigma, L/K_\sigma) = i(\sigma) + e_{M_\sigma} = 2 + 6e_K - i(\tau).$$

Then by (2.5), we have

$$\begin{aligned}\mathbf{f}(\psi, L/K) &= \mathbf{f}(\chi_\sigma, L/K_\sigma) + v_K(\mathfrak{d}_{K_\sigma/K}) \\ &= [2 + 6e_K - i(\tau)] + i(\tau) = 2 + 6e_K. \end{aligned}$$

□

4. Some representation theory of *p*-groups

Conductors were bounded for cyclic and quaternion groups in the last section. The group-theoretical results gathered here will be used to handle the general case. The reader may consult [2] for representation theory and [5] for p-groups.

In this section, G will always denote a p-group and F a field in which p is

invertible. For any commutative ring R, any R-algebra S and R-module M, we use the notations M_S for $S \otimes_R M$ and $n \cdot M$ for the direct sum of n copies of M.

We recall the decomposition of the character ψ of a simple $F[G]$-module V in terms of the Galois conjugates of a character χ afforded by an absolutely simple component:

$$\psi = m \sum_{\sigma \in \mathrm{Gal}(F(\chi)/F)} \chi^{\sigma}, \tag{4.1}$$

where $m = m_F(V)$ is the Schur index of V over F. The division algebra $\mathrm{End}_G(V)$ has degree m^2 over its center, which is isomorphic to $F(\chi)$, the field of character values of χ. The Hurwitz order $\Lambda = \mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}, (1 + \mathbf{i} + \mathbf{j} + \mathbf{k})/2]$ in the usual quaternions $\mathbb{K}$ over $\mathbb{Q}$ will be of particular importance for the case $p = 2$.

By abuse of language, we shall say that an $F[G]$-module V is *real* if it is $F[G]$-isomorphic to its contragredient $V^* = \mathrm{Hom}_F(V, F)$. A simple $F[G]$-module will be called *unitary* if it is not real. We say that a real module is $*$-simple if it does not contain a non-trivial proper real submodule. Because $*$ is an involution on the isomorphism classes of $F[G]$-modules, if V is $*$-simple but not simple, then $V \cong W \oplus W^*$ with W unitary. It follows that any real module is the direct sum of $*$-simple $F[G]$-modules.

Note that if V admits a non-degenerate bilinear form $\langle , \rangle : V \times V \to F$ which is G-invariant in the sense that $\langle gv, gw \rangle = \langle v, w \rangle$ for all $v, w \in V$ and $g \in G$, then V is real.

Recall the representations of abelian groups.

LEMMA 4.2. *Let A be an abelian p-group and let V be a simple $F[A]$-module. For some $n \geqslant 0$, we have $V \cong F(\boldsymbol{\mu}_{p^n})$, with the action of A on V induced by a surjection $\chi : A \to \boldsymbol{\mu}_{p^n}$. Two choices of χ lead to $F[A]$-isomorphic modules V exactly when they are $\mathrm{Gal}(F(\boldsymbol{\mu}_{p^n})/F)$-conjugate, and V^* corresponds to χ^{-1}. If V is faithful, then χ is an isomorphism and A is cyclic.*

Special attention will be paid to the non-abelian 2-groups with a cyclic subgroup $\langle x \rangle$ of order 2^n and index 2. They are given by $G = \langle x, y \rangle$, where $yxy^{-1} = x^{\alpha}$ and exactly one of the following holds:

$y^2 = 1$ and $\alpha = -1$ for the dihedral group D_n $(n \geqslant 3)$,

$y^2 = 1$ and $\alpha = -1 + 2^{n-1}$ for the semi-dihedral group S_n $(n \geqslant 3)$,

$y^2 = x^{2^{n-1}}$ and $\alpha = -1$ for the generalized quaternions Q_n $(n \geqslant 2)$,

$y^2 = 1$ and $\alpha = 1 + 2^{n-1}$ for $n \geqslant 2$.

LEMMA 4.3 (Cf. [5], I §14.9 and III §7.6). *Let G be a p-group. Then one of the following holds*:

(i) *G is cyclic,*
(ii) *$G = D_n$, S_n or Q_n, as above,*
(iii) *G has a non-cyclic abelian normal subgroup.*

The theorem of Blichfeldt asserts that absolutely irreducible representations of p-groups are monomial. We need two refinements for F-rational representations. To ease the notation, we omit the subscript F on the Schur index when the context makes it clear.

PROPOSITION 4.4. *Assume that the field F satisfies $[F(\mu_{p^n}):F] = p^{n-1}(p-1)$ for $n = 2$ when p is odd (resp. $n = 3$ when $p = 2$). Let G be a p-group and let V be a non-trivial simple, faithful $F[G]$-module. Then one of the following holds:*

(i) *G is cyclic of order p and $m(V) = 1$;*
(ii) *$G = Q_2$ and $m(V) = 1$ or 2 according as the F-central simple algebra $\Lambda \otimes_{\mathbb{Z}} F$ splits or not;*
(iii) *there is a proper subgroup H of G and a simple $F[H]$-module W with $m(W) \cdot V \cong m(V) \cdot \mathrm{ind}_H^G(W)$.*

Proof. Let A be an abelian normal subgroup of G and let W_0 be a simple $F[A]$-submodule of $\mathrm{res}_A^G(V)$. From Lemma 4.2, we have $W_0 \cong F(\mu_{p^n})$, with the action of A given by a surjection $\chi: A \to \mu_{p^n}$. Define $H = \{g \in G \mid gW_0 \cong W_0 \text{ as } F[A]\text{-module}\}$, that is $H = \{g \in G \mid \chi^g = \chi^\sigma \text{ for some } \sigma \in \mathrm{Gal}(F(\mu_{p^n})/F)\}$. Clifford's theorem shows that $V \cong \mathrm{ind}_H^G(W)$ with $W = \Sigma_{g \in H} gW_0$. It follows that $\mathrm{res}_A^G(V) = \bigoplus g_i W$, where g_i runs through a system of left coset representatives for G modulo H and so the restrictions to A of distinct conjugates of W have no components in common. *A fortiori*, absolutely irreducible components can only occur with the same multiplicity in V as in W. Hence $m(V) = m(W)$. If H is a proper subgroup of G, case (iii) holds.

We may thus assume that $H = G$ which implies that χ^g is a power of χ for each g in G and so $\mathrm{res}_A^G(V)$ is a sum of powers of χ. Because V is faithful, χ must be injective and we conclude that A is cyclic. Moreover, there is a homomorphism

$$\phi: G/A \hookrightarrow \mathrm{Gal}(E/F) \hookrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$$

such that $\chi(g^{-1}ag) = \chi(a)^{\phi(g)}$.

We have a contradiction unless every abelian normal subgroup of G is cyclic. This leaves the groups listed in Lemma 4.3(i) or (ii). Our assumption on roots of unity, which forces $[F(\mu_{p^j}):F] = p^{j-1}(p-1)$ for all $j \geqslant 1$, will now be used.

Suppose that $G = A$ is cyclic. When $n = 1$, we are in case (i) and otherwise V is induced from the unique faithful module for the cyclic subgroup of G of order p. The proposition therefore holds for abelian groups, with $m(V) = m(W) = 1$.

Let G be one of the non-abelian 2-groups in Lemma 4.3(ii). Write σ_α for the element of $\mathrm{Gal}(E/F)$ which acts by $\sigma_\alpha(\zeta_{2^n}) = \zeta_{2^n}^\alpha$ on $E = F(\boldsymbol{\mu}_{2^n})$. If $G = D_n$ or S_n, then $\mathrm{res}_A^G(V) \cong E$ has the structure of an $F[G]$-module with the action of y induced by σ_α. Consider the subgroup $C = \langle x^{2^{n-1}}, y\rangle$ of order 4 and a one-dimensional $F[C]$-representation Z affording a character $\lambda: C \to \{\pm 1\}$ with $\lambda(x^{2^{n-1}}) = -1$. Then $V = \mathrm{ind}_C^G(Z)$ and case (iii) holds with $m(V) = m(W) = 1$.

Suppose $G = Q_n$ and $E_n^+ = F(\zeta_{2^n} + \zeta_{2^n}^{-1})$. Then G has a unique faithful, simple representation V_n over F whose Schur index is 1 or 2 according as $\Lambda \otimes_{\mathbb{Z}} E_n^+$ splits or not. Since (ii) holds when $n = 2$, we may assume $n > 2$, in which case G properly contains the usual quaternions $C = \langle x^{2^{n-2}}, y\rangle \cong Q_2$ of order 8. Then $V = V_n$ satisfies

$$m(V_2) \cdot V \cong m(V) \cdot \mathrm{ind}_C^G(V_2). \qquad \square$$

REMARK. We have $m_{\mathbb{Q}}(V) = m_{\mathbb{Q}}(W)$ in case (iii) above. In contrast, when $F = \mathbb{Q}(\sqrt{-7})$, we have $2 \cdot V_3 = \mathrm{ind}_{Q_2}^{Q_3}(V_2)$ and $m_F(V_2) = 2$ while $m_F(V_3) = 1$.

COROLLARY 4.5. *Let V be a simple $F[G]$-module with F as in the Proposition. Then there is a finitely generated torsion-free $\mathbb{Z}[G]$-module M such that $M_{\mathbb{Q}}$ is simple and*

$$m_{\mathbb{Q}}(M_{\mathbb{Q}}) \cdot V \cong m_F(V) \cdot M_F.$$

Moreover $m_{\mathbb{Q}}(M_{\mathbb{Q}})\mathbf{f}(V, L/K) = m_F(V)\mathbf{f}(M_{\mathbb{Q}}, L/K)$.

Proof. We use the associativity and additivity of tensor products, as well as the Galois condition, to conclude the claim from the case in which V is faithful and simple and $G = 1$, $G = \mathbb{Z}/p\mathbb{Z}$ or $G = Q_2$. The modules in those cases were explicitly described above and can be defined over $\mathbb{Z}$. The simplicity of $M_{\mathbb{Q}}$ may be proved as in the more delicate version given in the next proposition. $\square$

We next show that real modules may be lifted.

PROPOSITION 4.6. *Assume G is a 2-group, $[F(\boldsymbol{\mu}_8): F] = 2$ and $2 \notin F^2$. Then all G-modules have trivial Schur multipliers. Let V be a $*$-simple, faithful $F[G]$-module. Then there is a finitely generated torsion-free $\mathbb{Z}[G]$-module M such that $M_{\mathbb{Q}}$ is simple and $m_{\mathbb{Q}}(M_{\mathbb{Q}}) \cdot V \cong M_F$. Moreover, $m_{\mathbb{Q}}(M_{\mathbb{Q}})\mathbf{f}(V, L/K) = \mathbf{f}(M_{\mathbb{Q}}, L/K)$.*

Proof. Under our assumptions on F, the Galois group $\Gamma_n = \mathrm{Gal}(F(\boldsymbol{\mu}_{2^n})/F)$ is generated by $\sigma_l: \zeta \mapsto \zeta^l$, with $l \equiv \pm 3 \pmod 8$. The key is that the action of the group generated by Γ_∞ and $*$ on the representation ring of $F[G]$ mimics that of $\mathrm{Gal}(\mathbb{Q}(\boldsymbol{\mu}_{2^\infty})/\mathbb{Q})$ on the representation ring of $\mathbb{Q}[G]$.

The proof will be by induction on the size of G once the special 2-groups are handled.

First let G be cyclic of order 2^n. Our claim holds when $n = 0$ or 1. For $n \geqslant 3$, we note from the description in Lemma 4.2 that there are two non-isomorphic simple $F[G]$-modules, interchanged by $*$ and corresponding to orbits of absolutely irreducible characters under Γ_n. Hence the only $*$-simple module is their sum, which is induced from the non-trivial representation on the subgroup of G of order two. The same conclusion obtains in case $n = 2$, except that the $*$-simple module is $F[G]$-simple when $\boldsymbol{\mu}_4 \not\subset F$.

Similarly, the groups $G = S_n$, D_n and Q_n each admit a unique $*$-simple and faithful $F[G]$ module V. The reduction of the $\mathbb{Z}[G]$-module M referred to in the last corollary is V when $G = S_n$ or D_n and two copies of V when $G = Q_n$. So the proposition is verified when all abelian normal subgroups of G are cyclic.

Let A be a *non-cyclic* abelian normal subgroup and let W_0 be a $*$-simple $F[A]$-submodule of $\mathrm{res}_A^G(V)$. As before, define

$$H = \{g \in G \mid gW_0 \cong W_0 \text{ as } F[A]\text{-modules}\}$$

and $W = \Sigma_{g \in H} gW_0$. Then $W \cong W^*$ and Clifford's theorem shows that $V \cong \mathrm{ind}_H^G(W)$. Again, the simple components of W are isomorphic to $E = F(\boldsymbol{\mu}_{2^n})$ with an action induced by a surjection $\chi : A \to \boldsymbol{\mu}_{p^n}$. If H were equal to G, we would conclude that $\mathrm{res}_A^G(V)$ is a sum of powers of χ because χ^g would be $\mathrm{Gal}(E/F)$-conjugate to $\chi^{\pm 1}$ for each $g \in G$. Because V is faithful, χ would then be injective and A cyclic, in violation of our hypothesis.

So H is a proper subgroup of G. The induction hypothesis provides us with a $\mathbb{Z}[H]$ module N such that $m(N_{\mathbb{Q}}) \cdot W \cong N_F$. The desired lifting is provided by the induced module $M = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} N$. In fact, our construction and the Galois condition imply that the restrictions to A of $g_1 W$ and $g_2 W$ (resp. $g_1 N_{\mathbb{Q}}$ and $g_2 N_{\mathbb{Q}}$) can have components in common only if $g_1 H = g_2 H$ since all the odd powers of χ (resp. of a lift of χ) must occur in W (resp. in $\mathrm{res}_A^G(N_{\mathbb{Q}})$). Hence the multiplicities occurring in V and W (resp. in $M_{\mathbb{Q}}$ and $N_{\mathbb{Q}}$) are the same, so that the Schur indices are also equal.

Finally, we specialize the Mackey formalism (cf. [2], Theorem 10.23) to prove irreducibility. Namely, for any commutative ring R, any subgroup H of a group G and any $R[H]$-module L, write $H_x = xHx^{-1} \cap H$ and ${}^xL$ for the R-module L with action of $y \in xHx^{-1}$ given by $l \mapsto x^{-1}yxl$. Then one has

$$\mathrm{Hom}_{R[G]}(\mathrm{ind}_H^G L, \mathrm{ind}_H^G L) \cong \bigoplus_{x \in H \backslash G / H} \mathrm{Hom}_{R[H_x]}(L, {}^xL)$$

where x runs through a set of double coset representatives for $H\backslash G/H$. In particular, $\mathrm{Hom}_{\mathbb{Q}[A]}(N_{\mathbb{Q}}, {}^xN_{\mathbb{Q}})$ vanishes unless x belongs to H and we conclude that

$$\mathrm{End}_{\mathbb{Q}[G]}(M_{\mathbb{Q}}) = \mathrm{End}_{\mathbb{Q}[H]}(N_{\mathbb{Q}}).$$

It follows from the simplicity of $N_{\mathbb{Q}}$ that these are the same division algebra and so $M_{\mathbb{Q}}$ is simple. □

5. Conductor bounds

We derive bounds for the conductor of a finitely generated $F[G]$-module V, where G is the Galois group of an extension L/K of p-adic fields and the characteristic of F is different from p. For typographical reasons, we introduce the notation

$$\delta_F(V) = \mathrm{ord}_p(\dim_F V) - \mathrm{ord}_p(m),$$

for V simple with Schur index $m = m_F(V)$. The subscript F may be omitted when it is clear from the context.

We begin by assuming that L/K is totally wildly ramified, so that G is a p-group.

THEOREM 5.1. *Suppose that L/K is totally wildly ramified. Let φ be a non-trivial absolutely irreducible complex character of G of degree p^d. Then*

$$\mathbf{f}(\varphi, L/K) \leqslant \left[1 + e_K(h + d) + \frac{e_K}{p-1}\right]\varphi(1)$$

where h is defined by $[\mathbb{Q}(\varphi):\mathbb{Q}] = (p-1)p^{h-1}$. If V is a simple $\mathbb{Q}[G]$-module, then

$$\mathbf{f}(V, L/K) \leqslant \dim V + [\delta_{\mathbb{Q}}(V) + p/(p-1)]e_K \dim V.$$

Proof. For a character φ afforded by an absolutely simple component of V, we have $\dim V = m(V)[\mathbb{Q}(\varphi):\mathbb{Q}]\varphi(1)$ according to (4.1). Since conjugates of φ have the same conductor, $\mathbf{f}(V, L/K) = m(V)[\mathbb{Q}(\varphi):\mathbb{Q}]\mathbf{f}(\varphi, L/K)$. It follows that the claimed bounds are equivalent.

We prove the second one by induction on the order of G. By (2.6), we may assume that V is faithful. Our bound is valid for G cyclic of order p by Corollary 3.2 and for $G = Q_2$ by Proposition 3.7.

Otherwise, Proposition 4.4 shows that there is a proper subgroup H of G of index p^n and a simple $\mathbb{Q}[H]$-module W with $m(W)\cdot V \cong m(V)\cdot \mathrm{ind}_H^G(W)$. Let M be the fixed field of H. The induction hypothesis, the discriminant bound of Lemma 3.1 and (2.5) imply that

$$m(W)\mathbf{f}(V, L/K) = m(V)[\mathbf{f}(W, L/M) + v_K(\mathfrak{d}_{M/K}) \dim W]$$

$$\leqslant m(V)\left[\left(1 + e_M\delta(W) + \frac{pe_M}{p-1}\right) + (p^n - 1 + np^n e_K)\right] \dim W$$

$$\leqslant m(W)[1 + e_K\delta(V) + pe_K/(p-1)] \dim V$$

since $m(W) \dim V = p^n m(V) \dim W$ and $e_M = p^n e_K$. □

As a corollary, we show that the bound above may be used to control the conductor of an $F[G]$-module V over a more general field F. We continue to assume that L/K is totally ramified. Suppose that χ is an absolutely irreducible character which is defined over a field containing F. One sees that there is a complex character φ and a choice of homomorphism $\iota: \mathbb{Z}[\varphi] \to F[\chi]$, such that $\iota(\varphi(g)) = \chi(g)$ for all $g \in G$, using Lemma 2.7 to pass through an l-adic field when the characteristic of F is $l \neq p$. By abuse of language, we refer to φ as a *lift* of χ. Let us define the *slippage* $s(\chi, \varphi) = s_F(\chi, \varphi)$ by

$$[\mathbb{Q}(\varphi) : \mathbb{Q}(\boldsymbol{\mu}_p)] = [F(\chi) : F(\boldsymbol{\mu}_p)]p^{s(\chi,\varphi)}.$$

Recall that the depth of V relative to L/K is the least integer c such that G_{c+1} is in the kernel of the representation afforded by V.

COROLLARY 5.2. *Suppose that L/K is totally wildly ramified and that V is a simple $F[G]$-module of depth c relative to L/K. Let φ be the character afforded by any absolutely irreducible complex representation of G/G_{c+1} which is not trivial on G_c. Write $[\mathbb{Q}(\varphi) : \mathbb{Q}] = (p-1)p^{h-1}$ and $\varphi(1) = p^d$. Then*

$$\mathbf{f}(V, L/K) \leqslant \left[1 + e_K(d + h) + \frac{e_K}{p-1}\right] \dim V.$$

Furthermore, we have $\mathbf{sw}(V, L/\mathfrak{K}) \leqslant [\delta_F(V) + s_F(\chi, \varphi) + p/(p-1)]e_K \dim V$.

Proof. According to the relation (2.2) for simple representations, we have

$$\mathbf{f}(V, L/K)/\dim V = \mathbf{f}(\varphi, L/K)/\varphi(1).$$

Our first inequality follows from the bound on the conductor of φ in Theorem 5.1.

In particular, we may choose φ to be a lift of χ described above. By definition of slippage and the decomposition into absolutely irreducible characters (4.1), we have $\dim V = mp^{d+h-1-s_F(\chi,\varphi)}[F(\boldsymbol{\mu}_p) : F]$. We conclude by using the

first inequality and (2.3). Note that since V is simple, we may assume that $V_0 = 0$. □

COROLLARY 5.3. *Suppose that L/K is totally wildly ramified. Assume that W is an $F[G]$-module and one of the following holds*:

(i) *W is simple and either p is odd with $[F(\mu_{p^2}):F] = p(p-1)$, or $p = 2$ with $[F(\mu_8):F] = 4$;*
(ii) *W is real and $*$-simple, $p = 2$, $[F(\mu_8):F] = 2$ and $2 \notin F^2$.*

Then $\mathbf{sw}(W, L/K) \leqslant [\delta_F(W) + p/(p-1)]e_K \dim W$.

Proof. We saw in Corollary 4.5 and Proposition 4.6 that there is a $\mathbb{Z}[G]$-module M such that $M_{\mathbb{Q}}$ is $\mathbb{Q}$-simple, $m_{\mathbb{Q}}(M_{\mathbb{Q}})W \cong m_F(W)M_F$ and

$$m_{\mathbb{Q}}(M_{\mathbb{Q}})\mathbf{f}(W, L/K) = m_F(W)\mathbf{f}(M_{\mathbb{Q}}, L/K).$$

By rewriting the bound for $\mathbf{f}(M_{\mathbb{Q}}, L/K)$ given in Theorem 5.1 in terms of $\dim W$ and $\delta_F(W)$, we find that

$$\mathbf{f}(W, L/K) \leqslant \dim W + [\delta_F(W) + p/(p-1)]e_K \dim W.$$

We may assume $W_0 = 0$, so that $\mathbf{sw}(W, L/K) = \mathbf{f}(W, L/K) - \dim W$ by (2.3). □

We now suppose that L is not necessarily totally ramified over K. Recall that K_1 is the fixed field of G_1 and that we write $V_0 = V^{G_0}$ and $V_1 = V^{G_1}$. Depending on how much information is available about the $F[G_1]$-simple components W of V/V_1, one may bound the conductor of V by using Corollaries 5.2 or 5.3 to control $\mathbf{sw}(W, L/K_1)$ and applying (2.3) and Lemma 2.4.

PROPOSITION 5.4. *Write $p^{h(G_1)}$ for the exponent of G_1 and let p^d be the maximal dimension among absolutely simple components of V/V_1 as a G_1-module. Then*

$$\mathbf{f}(V, L/K) \leqslant \dim(V/V_0) + \left[d + h(G_1) + \frac{1}{p-1}\right] e_K \dim(V/V_1).$$

Proof. By extending the field of scalars, we may assume that V/V_1 splits completely as an $F[G_1]$-module. Denote any component by W and its character by χ. By assumption, $\delta(W) \leqslant d$. We may apply Corollary 5.2 with the crude estimate $s_F(\chi, \varphi) \leqslant h(G_1) - 1$ to obtain the bound

$$\mathbf{sw}(W, L/K_1) \leqslant [d + h(G_1) + 1/(p-1)]e_{K_1} \dim W.$$

To prove the claimed inequality, we now use additivity, (2.3) and Lemma 2.4, noting that $g_1 e_{K_1} = g_0 e_K$. □

We now proceed to our main result for the conductors of Galois modules, stated here in terms of the Swan conductor. One may use (2.3) to obtain a bound for $\mathbf{f}(V, L/K)$.

THEOREM 5.5. *Let L/K be a Galois extension of p-adic fields with $G = \mathrm{Gal}(L/K)$ and let V be an $F[G]$-module. Assume one of the following holds:*

(i) *either p is odd with $[F(\boldsymbol{\mu}_{p^2}):F] = p(p-1)$, or $p = 2$ with $[F(\boldsymbol{\mu}_8):F] = 4$;*
(ii) *$p = 2$, $V \cong V^*$ as G_1-modules, $[F(\boldsymbol{\mu}_8):F] = 2$ and $2 \notin F^2$.*

Then we have the bound

$$\mathbf{sw}(V, L/K) \leqslant e_K[pd_1 + (p-1)\lambda_p(d_1)],$$

where the integer d_1 is defined by $\dim(V/V_1) = (p-1)d_1$.

Proof. Write $\bar{V} = V/V_1$ and let $\bar{V} = \oplus W_j$ be the decomposition as a direct sum of simple or $*$-simple $F[G_1]$-modules according as we are in case (i) or case (ii). By additivity and Corollary 5.3, we have

$$\mathbf{sw}(\bar{V}, L/K_1) \leqslant e_{K_1} \sum_j \delta(W_j) \dim W_j + \frac{pe_{K_1}}{p-1} \dim \bar{V}. \tag{5.6}$$

Because W_j does not admit the identity representation of G_1, one sees from (4.1) that $\dim W_j = m(W_j)(p-1)p^i$ with $i = \delta(W_j)$. Define integers s_i by

$$s_i = \sum_{\delta(W_j) = i} m(W_j),$$

so that $d_1 = \Sigma_i s_i p^i$ and $\Sigma_j \delta(W_j) \dim W_j = (p-1)\Sigma_i i s_i p^i \leqslant (p-1)\lambda_p(d_1)$, because of the basic observation that $\Sigma i r_i p^i \leqslant \lambda_p(\Sigma r_i p^i)$ for any non-negative integers r_i.

The bound for $\mathbf{sw}(V, L/K)$ results from (5.6) and Lemma 2.4, since $g_1 e_{K_1} = g_0 e_K$.

REMARK 5.7. Suppose that we drop the assumption $V \cong V^*$ in case (ii) above. Note that $2\mathbf{f}(V, L/K) = \mathbf{f}(V \oplus V^*, L/K)$. By applying Theorem 5.5 to the real module $V \oplus V^*$ and using (2.3), we find the weaker inequality

$$\mathbf{f}(V, L/K) \leqslant \dim(V/V_0) + e_K[3d_1 + \lambda_2(d_1)],$$

with $d_1 = \dim(V/V_1)$.

This bound is in fact taken on. Suppose that $\boldsymbol{\mu}_{2^n} \subset K$ and let L be

the splitting field of the Eisenstein polynomial $h(x) = x^{2^n} - \pi_K$. Then $G = \mathrm{Gal}(L/K)$ acts on $V = \mathbf{F}_l(\zeta_{2^n})$ by multiplication by ζ_{2^n}. For $l \equiv \pm 3 \pmod 8$, we have $\dim V = 2^{n-2}$. Since $V \oplus V^*$ is induced from the non-trivial one-dimensional representation of the subgroup of G of order 2, it follows from (2.5), Lemma 3.1 and Remark 3.3 that $\mathbf{f}(V, L/K) = 2^{n-2}[1 + (n+1)e_K]$.

6. Conductors of abelian varieties

As the main application of our bounds, we estimate the conductor of an abelian variety A, defined over a p-adic field K.

Write $V_l(A) = T_l(A) \otimes \mathbb{Q}_l$, where $T_l(A)$ is the l-adic Tate module. Denote the kernel of multiplication by l by $A[l]$ and the l-division field by $L = K(A[l])$. Let $G = \mathrm{Gal}(L/K)$ and let $I = I(\bar{K}/K)$ be the inertia group.

According to Grothendieck ([4], §4), for $l \neq p$, the conductor exponent of A is

$$\mathbf{f}(A/K) = \varepsilon(A/K) + \mathbf{sw}(A[l], L/K), \tag{6.1}$$

where $\varepsilon(A/K) = \dim(V_l(A)/V_l(A)^I)$ is the *tame* conductor. Each term above is independent of $l \neq p$.

THEOREM 6.2. *Let A be an abelian variety of dimension g defined over the p-adic field K. We have the following bound for the exponent of the conductor:*

$$\mathbf{f}(A/K) \leqslant 2g + e_K[pd + (p-1)\lambda_p(d)],$$

where d is the greatest integer in $2g/(p-1)$.

Proof. We may choose l to be a primitive root mod p^2 if p is odd (resp. $l \equiv \pm 3 \pmod 8$, if $p = 2$), prime to the degree of some polarization† of A defined over K. The latter condition implies that the Weil pairing induces a non-degenerate G_1-invariant symplectic form on $A[l]$. Therefore $A[l]$ is real as G_1-module and Theorem 5.5 yields the estimate

$$\mathbf{sw}(A[l], L/K) \leqslant e_K[pd_1 + (p-1)\lambda_p(d_1)],$$

with $(p-1)d_1 = \dim A[l] - \dim A[l]^{G_1}$. Since $\varepsilon(A/K) \leqslant \dim V_l(A) = 2g$, we obtain an inequality from (6.1) at least as good as the stated bound on $\mathbf{f}(A/K)$. □

This bound is best possible in a strong sense; it is attained for each integer g and p-adic field K. We present two families of examples.

†We thank Alice Silverberg for reminding us to include this assumption.

The following general construction was suggested by [6] and ([7], §3).

LEMMA 6.3. *Let K be a p-adic field, with p odd. Suppose that $h(x)$ is a separable polynomial in $K[x]$ of odd degree $2g+1 \geqslant 3$ and that B is the Jacobian variety of the hyperelliptic curve $y^2 = h(x)$ of genus g. Suppose that $h = h_1 \cdots h_r$ with h_i irreducible over K. Let θ_i be a root of $h_i(x)$ and $M_i = K(\theta_i)$. We have*

$$\mathbf{f}(B/K) \geqslant \mathbf{f}(B[2], L/K) = \sum_{i=1}^{r} v_K(\mathfrak{d}_{M_i/K}) f_{M_i/K},$$

where $L = K(B[2])$. Equality holds when h is irreducible and the extension M_1/K is totally ramified.

Proof. Denote by ∞ the unique point at infinity on the hyperelliptic curve. Note that L is the splitting field of h. For each i, with $1 \leqslant i \leqslant r$, write $H_i = \mathrm{Gal}(L/M_i)$ and $P_{i,\sigma} = (\sigma(\theta_i), 0) - \infty$, where σ ranges over G/H_i. The divisors $P_{i,\sigma}$ represent points of order 2 on B which span $B[2]$ over $\mathbf{F}_2$, with the only relation $\Sigma_{i,\sigma} P_{i,\sigma} \sim 0$.

Define the $\mathbb{Z}_2[G]$-module X by the exact sequence

$$0 \to \mathbb{Z}_2 \xrightarrow{\iota} \bigoplus \mathbb{Z}_2[G/H_i] \to X \to 0, \tag{6.4}$$

in which the G-map ι is determined by

$$\iota(1) = \sum_{i=1}^{r} \sum_{\sigma \in G/H_i} \sigma H_i.$$

There is a splitting of ι induced by $\sigma H_i \mapsto 1/(2g+1)$. Since H_i is the stabilizer of θ_i in the permutation representation of G acting on the roots of h, we see that $B[2] = \mathbf{F}_2 \otimes X$.

The sequence (6.4) remains exact upon tensoring wih either $\mathbf{F}_2$ or $\mathbb{Q}_2$ or passing to submodules fixed by any subgroup of G. Let $W = \bigoplus \mathbb{Q}_2[G/H_i] = \bigoplus \mathrm{ind}_{H_i}^{G}(1_{H_i})$. We find that $\mathbf{f}(B[2], L/K) = \mathbf{f}(W, L/K)$. Computing the latter by additivity and (2.5), we obtain

$$\mathbf{f}(B[2], L/K) = \sum_{i=1}^{r} v_K(\mathfrak{d}_{M_i/K})\, f_{M_i/K}.$$

We write V for the 2-adic Tate space of B. In view of the inequality $\dim_{\mathbb{Q}_2} V^I \leqslant \dim_{\mathbf{F}_2} B[2]^{G_0}$ it follows from (2.3) and (6.1) that

$$\mathbf{f}(B/K) \geqslant \mathbf{f}(B[2], L/K).$$

When h is irreducible over K, we write $H = H_1$ and $M = M_1$. For any normal subgroup N of G, the submodule of $\mathrm{ind}_H^G(1_H)$ fixed by N has dimension $[G:NH]$. Since $[G:G_0H]$ equals the inertial degree $f_{M/K}$, we conclude from (6.4) that the submodule of $B[2]$ fixed by G_0 is trivial when $f_{M/K} = 1$. In that case, $V^I = 0$ and $\mathbf{f}(B/K) = \mathbf{f}(B[2], L/K)$. □

PROPOSITION 6.5. *Suppose that p is odd and let A be the Jacobian variety of the hyperelliptic curve* $y^2 = x^{p^s} - \pi_K$ *over any p-adic field K. Then* $\mathbf{f}(A/K)$ *attains the bound in Theorem* 6.2.

Proof. The proof of Lemma 3.1 shows that if θ is a root of $h(x) = x^{p^s} - \pi_K$, then $K(\theta)$ has the largest discriminant among extensions of degree p^s over K. Namely, $v_K(\mathfrak{d}_{K(\theta)/K}) = p^s - 1 + sp^s e_K$. This equals $\mathbf{f}(A/K)$ by Lemma 6.3 and is the bound in Theorem 6.2, with $2g = p^s - 1$. □

PROPOSITION 6.6. *For any positive integer g and any p-adic field K, there is an abelian variety of dimension g for which the bound in Theorem* 6.2 *is attained.*

Proof. Our construction proceeds in two steps. First consider the extension M/K obtained by adjoining a root of the Eisenstein polynomial $g(X) = X^{p^s} - \pi_K$. We saw in Lemma 3.1 that $v_K(\mathfrak{d}_{M/K}) = p^s - 1 + sp^s e_K$.

For odd p, consider the Jacobian variety B of the hyperelliptic curve $y^2 = x^p - \pi_M$, whose conductor is $\mathbf{f}(B/M) = p - 1 + pe_M$, by Proposition 6.5. This example was treated differently in ([7], §3).

Let $A = R_{M/K}(B)$ be Weil's restriction of scalars, denoted $N_{M/K}(B)$ by Milne. To compute the conductor of A, we recall some functorial properties from [9]. In general, if B is an abelian variety of dimension m defined over an extension M of K of degree n, then A is an abelian variety of dimension mn. As in ([9], Prop. 1), since the Tate module of A is induced from that of B, we see that the exponents of the conductors of A and B are related as follows:

$$\mathbf{f}(A/K) = \mathbf{f}(B/M) + 2mv_K(\mathfrak{d}_{M/K}). \tag{6.7}$$

For our choices of M and B above, $A = R_{M/K}(B)$ has dimension $g = p^s(p-1)/2$ and

$$\begin{aligned}\mathbf{f}(A/K) &= (p - 1 + pe_M) + (p-1)(p^s - 1 + sp^s e_K)\\ &= 2g + e_K[sp^s(p-1) + p^{s+1}].\end{aligned}$$

The case $p = 2$ is handled by the same construction, but taking for B the elliptic curve already introduced in ([7], §6) and defined over M by $y^2 = x^3 + \pi_M x$. The authors of [7] deduce that $\mathbf{f}(B/M) = 2 + 6e_M$ from a formula of Ogg, proved by Saito in [17]. Lemma 6.8 below avoids this. The

abelian variety $A = R_{M/K}(B)$ has dimension $g = 2^s$. It follows from (6.7) that its conductor exponent is $\mathbf{f}(A/K) = 2^{s+1}[1 + e_K(s + 3)]$.

For an arbitrary positive integer g, write $2g = d(p - 1) + r$, with $0 \leqslant r \leqslant p - 2$. We see that r is even and so $r = 0$ for $p < 5$. If d has the p-adic expansion $d = \Sigma_s c_s p^s$ one easily checks that the bound of Theorem 6.2 is attained by the obvious product of c_s copies of abelian varieties A as above, of dimensions p^s with varying s, together with $r/2$ copies of elliptic curves with additive reduction. Note that if $p \geqslant 5$, then the conductor exponent of such elliptic curves necessarily equals 2. □

LEMMA 6.8. *If M is a 2-adic field, then the conductor exponent of the elliptic curve $B: y^2 = x^3 + \pi_M x$ is $\mathbf{f}(B/M) = 2 + 6e_M$.*

Proof. We have $\mathbf{f}(B/M) \geqslant \mathbf{f}(B[3], L/M)$, where $L = M(B[3])$. According to ([14], §5.4), $\boldsymbol{\mu}_3 \subset L$ and the field generated by the abscissas of the 3-division points of B is the splitting field of the polynomial

$$3x^4 + 6\pi_M x^2 - \pi_M^2. \tag{6.9}$$

Since the conductor is not changed by unramified extension of M, we may assume that $\boldsymbol{\mu}_3 \subset M$. Then the action of Galois on $B[3]$ provides a representation of $G = \mathrm{Gal}(L/M)$ as a subgroup of the quaternion group in $\mathrm{SL}(2, \mathbf{F}_3)$.

From the discriminant of (6.9) we see that $i \in L$ and by the quadratic formula, we get the equation

$$x^2 + \pi_M\left(1 + \frac{2\sqrt{2}}{3}\right) = 0. \tag{6.10}$$

Note that B admits complex multiplication over $M(i)$, given by $\mathbf{i}(x, y) = (-x, iy)$.

Suppose first that $M(i)$ is unramified over M. Without changing the conductor, we may assume that $i \in M$. Fix a root θ of (6.10) and a point P of order 3 on B with $x(P) = \theta$. Since the Eisenstein equation (6.10) is irreducible over M, there exists an element $\sigma \in G$, obtained by extension from $\sigma(\theta) = -\theta$, such that $\sigma(P) = \mathbf{i}P$. Therefore, G is cyclic of order 4. Let χ be a faithful character of G of degree 1. In view of (6.10), we have $\mathbf{f}(\chi^2, L/M) = 1 + 2e_M$ by Remark 3.3. Therefore $\mathbf{f}(\chi, L/M) = 1 + 3e_M$ by Remark 3.6. Since $\dim B[3] = 2$, we have $\mathbf{f}(B[3], L/M) = 2 + 6e_M$.

Suppose that $M(i)$ is ramified over M. We may fix another root θ' of (6.9) such that $\theta\theta' = \pi_M/\sqrt{-3}$. Then

$$(\theta + \theta')^2 = -\frac{4}{3}\pi_M(\zeta + 2),$$

with $\zeta = (-1 + \sqrt{-3})/2$. By Kummer theory, G is not cyclic and each of the quadratic extensions of M in L is ramified. It follows that G is the quaternion group and L/M is totally ramified, so that $\mathbf{f}(B[3], L/M) = 2 + 6e_M$ by Proposition 3.7. Since this is the maximum possible value of $\mathbf{f}(B/M)$, we are done. □

We can improve the conductor bound of Theorem 6.2 if we know the nature of the bad reduction. When l is odd, the abelian variety A over K acquires semi-stable reduction over $L = K(A[l])$. For any extension M of K, let $\mathscr{A}_M$ be the Néron model for A over $\mathrm{Spec}(\mathcal{O}_M)$, where $\mathcal{O}_M$ is the ring of integers of M. By Chevalley's theorem, the special fiber has a natural decomposition of algebraic groups

$$0 \to \mathscr{U}_M \times \mathscr{T}_M \to (\mathscr{A}_M)_v \to \mathscr{B}_M \to 0$$

where $\mathscr{B}_M$ is an abelian variety, $\mathscr{T}_M$ is toroidal and $\mathscr{U}_M$ is unipotent.

Write $\dim \mathscr{B}_M = a_M$, $\dim \mathscr{U}_M = u_M$ and $\dim \mathscr{T}_M = t_M$. The variety has semi-stable reduction when $u_M = 0$ and in particular if $L \subseteq M$. So we may define the semi-stable toroidal and abelian dimensions $t_{ss} = t_L$ and $a_{ss} = a_L$.

PROPOSITION 6.11. *With the notation above, let K_1 be the subfield of L fixed by the first ramification group of $G = \mathrm{Gal}(L/K)$. The conductor exponent is bounded by*

$$\mathbf{f}(A/K) \leqslant t_K + 2u_K + 2(d_t + d_a)pe_K + (p-1)[2\lambda_p(d_t) + \lambda_p(2d_a)]e_K,$$

where the integers d_t and d_a are defined by $t_{ss} - t_{K_1} = (p-1)d_t$ and $a_{ss} - a_{K_1} = (p-1)d_a$ respectively.

Proof. According to ([4], §4), we have $\varepsilon(A/K) = t_K + 2u_K$. In view of (6.1), it remains to bound $\mathbf{sw}(A[l], L/K)$.

We know from Grothendieck ([4], §2), [8], [10], that there is a 2-step filtration $T_l(A) \supset T_1 \supset T_2$, in which $T_l(A)/T_1$ is dual to T_2 with respect to the Weil pairing. Each graded piece of

$$T_l(A)/T_1 \oplus T_1/T_2 \oplus T_2 \tag{6.12}$$

admits an action of G. Moreover, the $\mathbb{Z}_l$ ranks of T_2 and $T_2^{G_1}$ are t_{ss} and t_{K_1}, while the $\mathbb{Z}_l$ ranks of T_1/T_2 and $(T_1/T_2)^{G_1}$ are $2a_{ss}$ and $2a_{K_1}$ respectively.

Consider the grading $X \oplus Y \oplus Z$ on $A[l]$ obtained by tensoring (6.12) with $\mathbf{F}_l$. Then $Z = X^*$ and $Y^* = Y$. By Lemma 2.4, we have

$$\mathbf{sw}(A[l], L/K) = \mathbf{sw}(X \oplus X^*, L/K) + \mathbf{sw}(Y, L/K).$$

Choose l to be a primitive root mod p^2 when p is odd (resp. $l \equiv \pm 3 \pmod 8$ when $p = 2$). Our claim now follows from Theorem 5.5, since the relevant dimensions are $\dim_{\mathbf{F}_l}(Y/Y^{G_1}) = 2a_{ss} - 2a_{K_1}$ and by duality,

$$\dim_{\mathbf{F}_l}(Z/Z^{G_1}) = \dim_{\mathbf{F}_l}(X/X^{G_1}) = t_{ss} - t_{K_1}. \qquad \square$$

References

1. A. Brumer: The rank of $J_0(N)$. Submitted to Astérisque.
2. C. W. Curtis and I. Reiner: *Methods of Representation Theory*. 2 vols. John Wiley, New York, 1987.
3. J.-M. Fontaine: Groupes de ramification et représentation d'Artin. *Ann. Sci. E.N.S.* (4) 4 (1971) 337–392.
4. A. Grothendieck: Modèles de Néron et monodromie. *SGA 7, Exposé IX, Lecture Notes in Math.* 288, 313–523, Springer-Verlag: Berlin, New York, 1970.
5. B. Huppert: *Endliche Gruppen I*. Springer-Verlag: Berlin, New York, 1967.
6. H. W. Lenstra, F. Oort: Abelian varieties having purely additive reduction. *J. Pure and Applied Algebra* 36 (1985) 281–298.
7. P. Lockhart, M. I. Rosen, J. Silverman: An upper bound for the conductor of an abelian variety. *Journal of Algebraic Geometry* 2 (1993) 569–601.
8. D. Lorenzini: Groups of components of Néron models of Jacobians. *Compositio Math.* 73 (1990) 145–160.
9. J. Milne: The arithmetic of abelian varieties. *Inv. Math.* 17 (1972) 177–190.
10. F. Oort: Good and stable reduction of abelian varieties. *Manuscripta Math.* 11 (1974) 171–197.
11. O. Ore: Abriss einer arithmetischen theorie der Galoischen Körper. *Math. Ann.* 100 (1928) 650–673.
12. S. Sen: Ramification in p-adic Lie extensions. *Inv. Math.* 17 (1972) 44–50.
13. J.-P. Serre: *Corps locaux*. Hermann, Paris, 1962, or Grad. Texts in Math. 67, Springer-Verlag: Berlin, New York, 1979.
14. J.-P. Serre: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inv. Math.* 15 (1972) 259–331.
15. J.-P. Serre: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. *Duke Math. J.* 54 (1987) 179–230.
16. J.-P. Serre, J. Tate: Good reduction of abelian varieties. *Annals of Mathematics* 88 (1968) 492–517.
17. T. Saito*: Conductor, discriminant and the Noether formula for arithmetic surfaces. *Duke Math. J.* 57 (1988) 151–173.

*The authors thank Qin Liu for providing this reference.