Mathematische Zeitschrift (2025) 309:56
https://doi.org/10.1007/s00209-024-03658-7

Mathematische Zeitschrift

Superelliptic curves with large Galois images

Pip Goodman[1]

Received: 10 November 2021 / Accepted: 4 November 2024 / Published online: 7 February 2025

Abstract

Let $r > 2$ and ℓ be primes. In this paper we study the mod ℓ Galois representations attached to curves of the form $y^r = f(x)$ where f is monic and has coefficients belonging to the rth cyclotomic field. We provide conditions on the coefficients (and degree) of f which allow one to verify the mod ℓ image is large outside of a (typically small) finite explicit set of primes. We allow all values of r for which the rth cyclotomic field has odd class number. This appears to be the first explicit result for abelian varieties of dimension greater than two and not of GL_2-type which allows the ground field to have unramified extensions. To determine the exact image we study the "endomorphism character", a certain algebraic Hecke character which generalises the CM character. This is achieved in entirety when $r = 3$. To the author's knowledge, this is the first accurate description of the full image in the literature. Finally, we give several examples with genus ranging from 10 to 36. Applications to the Inverse Galois Problem are also included.

Contents

✉ Pip Goodman
pip.goodman@ub.edu

[1] Universitat de Barcelona, Barcelona, Spain

1 Introduction

Let r be a prime number and ζ_r a primitive r-th root of unity. In this paper we study mod ℓ Galois representations attached to superelliptic curves

$$C\colon y^r = f(x) \in \mathbb{Q}(\zeta_r)[x].$$

We produce criteria for the mod ℓ image to be "large" outside a small finite explicit set for $r \geq 3$ and $\mathbb{Q}(\zeta_r)$ with odd class number. Our methods allow us to produce explicit examples with small coefficients; for example for $d \in \{12, 18, 24\}$ the curves

$$y^3 - \zeta_3^2 \pi y^2 - \zeta_3^2 y = x^d + x^{d-1} + 7x^3 + 14x^2 + 45\zeta_3\pi \tag{1.1}$$

where $\pi = 1 - \zeta_3$ have large image outside of a finite set of primes listed in Sect. 7.1. Note that here we have taken a translation of the usual model, the corresponding curves listed in Sect. 7.1 have the standard superelliptic model as do the other examples listed there.

In recent years there has been much work on finding explicit examples of abelian varieties over $\mathbb{Q}$ with trivial endomorphism ring and large mod ℓ images. This has seen considerable success for those of low dimension. For example, [10] provides an algorithm which for such abelian surfaces returns finitely many ℓ where the representation is not surjective. The paper [2] gives a genus 3 hyperelliptic curve with the images of the mod ℓ representations being as large as possible for all ℓ. Their methods require the curve to have everywhere semistable reduction. This is in contrast to our approach and that of [1] where primes of bad potentially good reduction play a crucial role.

In [1], the theory of clusters [12] is employed to determine the images of certain inertia subgroups. The authors of [1] then construct a genus 6 hyperelliptic curve with mod ℓ images as large as possible for all primes ℓ. To do this the Chinese Remainder Theorem is applied which in turn leads to the coefficients of the resulting hyperelliptic curve being large. Our method, however, uses Δ_v−regular curves [11]. This has a significant advantage in that the coefficients may be taken to be relatively small which allows the verification of large genus examples.

We also note the above references all require the ground field of their curves to have no unramified extensions, whereas we allow $\mathbb{Q}(\zeta_r)$ with odd class number.

The image of a mod ℓ representation attached to the jacobian of a hyperelliptic curve is well-known to lie inside $\mathrm{GSp}_{2g}(\ell)$, where g is the genus of the curve. Indeed, for any principally polarised abelian variety A/K the Weil pairing $\langle , \rangle\colon A[\ell] \times A[\ell] \to \mathbb{F}_\ell$ provides a non-degenerate symplectic pairing, which G_K, the absolute Galois group of the ground field, preserves up to similitude. The similitude factor is given by χ_ℓ the mod ℓ cyclotomic character, that is, for $P, Q \in A[\ell]$ and $\sigma \in G_K$ the relation $\langle \sigma(P), \sigma(Q)\rangle = \langle P, Q\rangle^{\chi_\ell(\sigma)}$ is satisfied.

Furthermore, for $\ell \neq 2$ there are no additional restrictions for a hyperelliptic curve with trivial endomorphism ring. Thus, as the cyclotomic character is surjective (over $\mathbb{Q}$), it suffices to show the mod ℓ image contains the isometry group $\mathrm{Sp}_{2g}(\ell)$ to conclude the representation is surjective.

The situation is radically different when A/K has non-trivial endomorphism ring. First, G_K must normalise the endomorphisms of A and further commute with those that are defined over K. Second, and more subtly, the action of the endomorphism ring on the space of regular differentials $\Omega^1(A)$ comes into play. This is discussed at length in Sect. 6.

Let us expand upon what the above conditions mean in our situation, where $J = \mathrm{Jac}(C)$ is a superelliptic jacobian $J/\mathbb{Q}(\zeta_r)$ with endomorphism ring $\mathrm{End}(J) = \mathrm{End}_{\bar{\mathbb{Q}}}(J) \cong \mathbb{Z}[\zeta_r]$.

First, $\mathrm{End}(J)$ is generated by the automorphism $[\zeta_r]\colon J \to J$ which arises from the automorphism on the curve sending $(x, y) \mapsto (x, \zeta_r y)$. This map preserves the Weil pairing (see Lemma 3.7). It follows that the image of $G_{\mathbb{Q}(\zeta_r)}$ is contained in the centraliser of $[\zeta_r]$ inside $\mathrm{GSp}_{2g}(\ell)$. The structure of this group is discussed in Sect. 3.2.

We say the image of $\rho_\ell\colon G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}(J[\ell])$ is *large* if it contains the largest perfect subgroup of the centraliser of $[\zeta_r]$ in $\mathrm{GSp}_{2g}(\ell)$, or equivalently, the limit of its derived series. In the case of hyperelliptic curves (defined over $\mathbb{Q}$), this means exactly that $\rho_\ell(G_{\mathbb{Q}})$ contains $\mathrm{Sp}_{2g}(\ell)$. We give a similar down to earth description for superelliptic curves in Sect. 3.3.

In fact, we prove the following theorem (see Sect. 7 for a more detailed statement). We note the class number of $\mathbb{Q}(\zeta_r)$ is non-trivial precisely when $r > 19$ [24]. Our notation for the various groups listed in the theorem below is detailed in Sect. 3.1. The powers on the groups refer to direct products.

Theorem 1.2 ($\subseteq$ Theorem 7.2). *Let $d \geq 12$ be a natural number divisible by $2r$ which is also the sum of two distinct primes $q_1 < q_2$.*

Suppose there exists a prime $q_2 < q_3 < d$. If $r > 23$ assume the class number of $\mathbb{Q}(\zeta_r)$ is odd and $d = q_3 + 1$.

Let $n = \frac{2g}{r-1}$. Then given a polynomial $f \in \mathbb{Q}(\zeta_r)[x]$ of degree d whose coefficients satisfy certain congruence conditions, the image of the representation $\rho_\ell\colon G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}(J[\ell])$ contains

- $\mathrm{SL}_n(\ell^i)^{\frac{r-1}{2i}}$ *if i the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)$ is odd; and*
- $\mathrm{SU}_n(\ell^{i/2})^{\frac{r-1}{i}}$ *if i the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)$ is even*

for all ℓ outside of a finite explicit set.

Identifying the exact image of ρ_ℓ is a more arduous task. We do this completely for $r = 3$ using the endomorphism character studied in Sect. 6 (see also Theorem 7.5). As far as the author is aware, this is the first time images of such representations have been correctly identified.[1] The images of the mod ℓ representations coming from the examples in (1.1) are (outside the finite set of ℓ listed in Sect. 7.1):

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{d-2}(\ell)^{\frac{d}{3},6} \rtimes \langle \chi_\ell \rangle \text{ for } \ell \equiv 1 \mod 3, \text{ and}$$
$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GU}_{d-2}(\ell)^{\frac{d}{3},6} \rtimes \langle \chi_\ell \rangle \text{ for } \ell \equiv 2 \mod 3.$$

The notation here is as follows

$$\mathrm{GL}_n(\ell)^{s,t} = \{\sigma \in \mathrm{GL}_n(\ell) | \det(\sigma) \in \langle a^s, b \rangle\}$$

where a generates $\mathbb{F}_\ell^*$ and $b \in \mathbb{F}_\ell^*$ has order t; and

$$\mathrm{GU}_n(\ell)^{s,t} = \{\sigma \in \mathrm{GU}_n(\ell) | \det(\sigma) \in \langle a^s, b \rangle\}$$

where a generates $(\mathbb{F}_{\ell^2}^*)^{\ell-1}$ and $b \in \mathbb{F}_{\ell^2}^*$ has order t.

[1] Upton considers curves of the form $y^3 = f(x)$ with $f \in \mathbb{Q}[\zeta_3]$ of degree 4 [36]. However an oversight when taking the determinant leads to the wrong image being stated.

In Sect. 2 we define representations ρ_λ of $G_{\mathbb{Q}(\zeta_r)}$ for $\lambda|\ell$. For $\ell \equiv 1 \mod r$, the maximal image of the $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is $\mathrm{GL}_n(\ell)$, where $n = \frac{2g}{r-1}$ and g is the genus of C. Whenever the image of ρ_ℓ is large, ρ_λ surjects (Proposition 6.11, see also Theorem 7.3). The examples in (1.1) thus also satisfy

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{d-2}(\ell) \text{ for } \ell \equiv 1 \mod 3.$$

For $\ell \equiv -1 \mod r$, the maximal image of the $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is $\Delta\mathrm{U}_n(\ell)$, the similitude group of a non-degenerate unitary pairing. However this upper bound is not achieved for all ℓ, though we can list values of ℓ for which it is (Proposition 6.12, see also Theorem 7.4). The examples in (1.1) satisfy

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \Delta\mathrm{U}_{d-2}(\ell) \text{ for } \ell \equiv 5, 29 \mod 36.$$

In Sect. 3 we give the relevant background on group theory. Including a discussion of centralisers in the symplectic group and the restrictions they impose on the Galois images, the classification of maximal subgroups of certain classical groups and products of classical groups. The classification of maximal subgroups uses modern tools from group theory. We believe these tools may be of significant use to number theorists studying questions related to images of Galois representations.

Section 4 gives local conditions on f which in turn provides a reasonably comprehensive description of possible inertia subgroups.

In Sect. 5, we use local Galois groups to rule out the images of the ρ_λ being contained in maximal subgroups.

Section 6 reviews well-known results on algebraic Hecke characters and explains their relevance to our setting in identifying the exact image of Galois. Several examples are given.

The last section ties together results from the previous sections and gives a method for constructing superelliptic jacobians with large images outside a finite explicit set of primes. We then finish by giving a number of examples.

2 λ-adic representations

Fix distinct primes r, ℓ. Let $f \in \mathbb{Q}(\zeta_r)[x]$ be a polynomial of degree $d \geq 5$ without repeated roots. The jacobian J of the superelliptic curve

$$C\colon y^r = f(x)$$

has a natural endomorphism $[\zeta_r]\colon J \to J$ which arises from the map on C defined by $(x, y) \mapsto (x, \zeta_r y)$. This endomorphism realises $\mathbb{Z}[\zeta_r]$ as a subring of $\mathrm{End}(J)$. For the ease of exposition, let us assume the endomorphism ring $\mathrm{End}(J)$ is isomorphic to $\mathbb{Z}[\zeta_r]$. In order to study the representation of the absolute Galois group $G_{\mathbb{Q}(\zeta_r)}$ on $J[\ell]$, the ℓ-torsion of J, we first study λ-adic representations of $G_{\mathbb{Q}(\zeta_r)}$ associated to J, where $\lambda|\ell$ is a prime above ℓ in $\mathbb{Q}(\zeta_r)$. Let us introduce these now.

The Galois group $G_{\mathbb{Q}(\zeta_r)}$ acts continuously on the Tate module $T_\ell(J)$, which gives rise to a $\mathbb{Q}_\ell$-representation,

$$\rho_{\ell^\infty}\colon G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}\,(V_\ell)$$

where $V_\ell(J) = T_\ell(J) \otimes \mathbb{Q}_\ell$. The action of the endomorphism algebra $\mathrm{End}^0(J) \cong \mathbb{Q}(\zeta_r)$ on $V_\ell(J)$ is compatible with that of $\mathbb{Q}_\ell$, allowing us to view $V_\ell(J)$ as a $\mathbb{Q}(\zeta_r)_\ell = \mathbb{Q}(\zeta_r) \otimes \mathbb{Q}_\ell$-module. The idempotents giving rise to the decomposition $\mathbb{Q}(\zeta_r)_\ell = \prod_{\lambda|\ell} \mathbb{Q}(\zeta_r)_\lambda$ thus

induce a decomposition $V_\ell = \prod_{\lambda|\ell} V_\lambda$. As the endomorphisms of J are defined over $\mathbb{Q}(\zeta_r)$, the idempotents commute with the action of $G_{\mathbb{Q}(\zeta_r)}$ on $V_\ell(J)$, leading to representations

$$\rho_{\lambda\infty} : G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}_{\mathbb{Q}(\zeta_r)_\lambda}(V_\lambda),$$

one for each $\lambda|\ell$. We call these λ-*adic representations*.

The dimension of each of the vector spaces V_λ over $\mathbb{Q}(\zeta_r)_\lambda$ is equal to $n = \frac{2g}{r-1}$, [28, Thm 2.1.1]. This entails that V_ℓ is a free $\mathbb{Q}(\zeta_r)_\ell$-module of rank n. In order to prove our main results, one may assume $n \geq 10$ throughout. However, many of the results presented here hold for smaller values of n and we indicate these as we go along.

As with V_ℓ, we may view T_ℓ as a $\mathbb{Z}[\zeta_r] \otimes \mathbb{Z}_\ell$-module. Since $\mathbb{Z}[\zeta_r]_\ell := \mathbb{Z}[\zeta_r] \otimes \mathbb{Z}_\ell$ is a product of discrete valuation rings it follows from the above that T_ℓ is a free $\mathbb{Z}[\zeta_r]_\ell$-module of rank n [28, Prop 2.2.1]. The module $T_\lambda = T_\ell \otimes_{\mathbb{Z}[\zeta_r]_\ell} \mathbb{Z}[\zeta_r]_\lambda$ is then a lattice in V_λ and setting $J[\lambda] = T_\lambda \otimes_{\mathbb{Z}[\zeta_r]_\lambda} k_\lambda$, where k_λ is the residue field, we obtain a representation

$$\rho_\lambda : G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}\,(J[\lambda]).$$

The image of this representation will be of central interest to us. In fact, the subgroup $G_\lambda = \rho_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})})$ of the image will be of even greater importance.

Work of Shimura [32, §11.10], [28, Thm 2.1.2] shows the system of representations $(\rho_{\lambda\infty})_\lambda$ is a strictly compatible system of $\mathbb{Q}(\zeta_r)$-rational representations. Let us recall what this means.

Definition 2.1 We say that a collection of representations $\rho_{\lambda\infty} : G_{\mathbb{Q}(\zeta_r)} \to \mathrm{GL}_n(\mathbb{Q}(\zeta_r)_\lambda)$ (one for each prime λ of $\mathbb{Q}(\zeta_r)$) forms a strictly compatible system if there exists a finite set S of primes of $\mathbb{Q}(\zeta_r)$ such that

- any $\rho_{\lambda\infty}$ is unramified outside of $S \cup S_\ell$ (where ℓ is the rational prime below λ, and S_ℓ contains the primes above ℓ in $\mathbb{Q}(\zeta_r)$);
- for each $\mathfrak{p} \notin S$, there is a monic polynomial $P_\mathfrak{p} \in \mathbb{Z}[\zeta_r][x]$ whose image in $\mathbb{Q}(\zeta_r)_\lambda[x]$ coincides with the characteristic polynomial of $\rho_{\lambda\infty}(\mathrm{Frob}_\mathfrak{p})$ for any λ whenever $\mathfrak{p} \notin S \cup S_\ell$.

The set S in our case is taken to be the primes of bad reduction for $J/\mathbb{Q}(\zeta_r)$.

It is clear from the above definition that the system of representations $(\det \circ \rho_{\lambda\infty})_\lambda$ is also strictly compatible. Each representation in this family is abelian, and so by [29, §1.1, Prop 1.4] (see also [28, Thm 2.13], [17, Main Thm]) there is an algebraic Hecke character Ω of $\mathbb{Q}(\zeta_r)$ with values in $\mathbb{Q}(\zeta_r)$ such that for every prime λ of $\mathbb{Q}(\zeta_r)$, the λ-adic avatar (see §6.1, or [29, §0.5]) Ω_λ equals $\det \circ \rho_{\lambda\infty}$. We call Ω the *endomorphism character*. In Sect. 6, we shall study Ω in detail and describe the mod λ images of its λ-adic avatars.

Finally, the following proposition will be useful in understanding the action of the inertia groups.

Proposition 2.2 *Let G be a group, $E/\mathbb{Q}$ a finite Galois extension, $n \geq 1$ an integer and V an $(E \otimes \mathbb{Q}_\ell)[G]$-module such that the underlying $E \otimes \mathbb{Q}_\ell$-module structure is free of rank n. Let θ denote the corresponding representation $\theta : G \to \mathrm{Aut}(V)$. Decompose V as above into $\prod_{\lambda|\ell} V_\lambda$ where λ runs through the primes above ℓ in E and label the corresponding E_λ-representations of G by θ^λ.*

Suppose that θ may be realised over $E \subset E \otimes \mathbb{Q}_\ell$ (where the inclusion is given by $\alpha \mapsto \alpha \otimes 1$). Then for each λ, there is an embedding $\tau : E \hookrightarrow E_\lambda$ such that for any $g \in G$, we have $\theta^\lambda(g) = \theta^\tau(g)$. That is, after fixing appropriate bases, the matrix $\theta^\lambda(g)$ is equal to the matrix obtained from applying τ to the entries of $\theta(g)$.

In particular, for λ, λ' primes above ℓ we have $\theta^{\lambda'} = (\theta^\lambda)^\gamma$ for some $\gamma \in \mathrm{Gal}(E/\mathbb{Q})$.

Proof Let us begin by fixing an isomorphism $\varphi\colon E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\sim} \prod_{\lambda|\ell} E_\lambda$. By the Primitive Element Theorem, we may write $E = \mathbb{Q}(\alpha)$ for some α with minimal polynomial f. Writing $f(x) = f_1(x)\cdots f_r(x)$ for the factorisation of $f(x)$ over $\mathbb{Q}_\ell$, we have $\varphi(\alpha \otimes 1) = (\alpha_1, \ldots, \alpha_r)$ where α_i is a root of $f_i(x)$ in $\bar{\mathbb{Q}}_\ell$ [25, pp. 163].

Now, by assumption, there is a basis $v_1, \ldots, v_n$ of V with respect to which θ takes values in E. Let e_λ denote the idempotent which cuts out V_λ from V. It is easy to see $e_\lambda v_1, \ldots, e_\lambda v_n$ form a basis of V_λ. Let $\tau\colon E \to E_\lambda$ be the embedding satisfying $\tau(\alpha) = e_\lambda \varphi(\alpha \otimes 1)$.

Let $g \in G$. We have $g \cdot v_i = \sum \varphi(\beta_{i,j} \otimes 1)v_j$ for some $\beta_{i,j} \in E$. The claim now follows by considering

$$g \cdot (e_\lambda v_i) = e_\lambda(g \cdot v_i) = e_\lambda \sum \varphi(\beta_{i,j} \otimes 1)v_j = \sum \tau(\beta_{i,j})e_\lambda v_j.$$

□

3 Group Theory

3.1 Classical groups and their automorphisms

Let $i \in \mathbb{N}_{>0}$ be a natural number and V be an n-dimensional vector space over $\mathbb{F}_{\ell^i}$. We denote the group of $\mathbb{F}_{\ell^i}$-semilinear invertible transformations of V by $\Gamma\mathrm{L}_n(\ell^i)$.

Let $\langle , \rangle\colon V \times V \to \mathbb{F}_{\ell^i}$ be either identically zero, a non-degenerate symplectic pairing or a non-degenerate unitary pairing. We note the last case may only occur if i is even.

We call a semisimilarity any element $\tau \in \Gamma\mathrm{L}_n(\ell^i)$ for which there exists $\chi(\tau) \in \mathbb{F}_{\ell^i}$, $\sigma \in \mathrm{Aut}(\mathbb{F}_{\ell^i})$ such that

$$\langle \tau v, \tau w\rangle = \chi(\tau)\langle v, w\rangle^\sigma$$

for all $v, w \in V$. The set of semisimilarities forms a group Γ. The similitude group $\Delta \leq \Gamma$ is the subgroup for which σ is the identity. This group coincides with $\Gamma \cap \mathrm{GL}_n(\ell^i)$ [18, Lemma 2.1.2 (iv)]. The isometry group $I \leq \Delta$ is the subgroup which preserves $\langle , \rangle$; that is the $\tau \in \Delta$ for which $\chi(\tau) = 1$. We denote the kernel of $\det\colon I \to \mathbb{F}_{\ell^i}$ by S. If $\langle , \rangle$ is identically zero, let $A = \Gamma\langle \iota \rangle$ where ι is the inverse-transpose map $u \mapsto u^{-T}$. Else let $A = \Gamma$.

When $\langle , \rangle$ is a unitary pairing, $\Delta\mathrm{U}_n(\ell^{i/2})$ denotes the similitude group, $\mathrm{GU}_n(\ell^{i/2})$ the isometry group, and $\mathrm{SU}_n(\ell^{i/2})$ the kernel of the determinant map $\det\colon \mathrm{GU}_n(\ell^{i/2}) \to \mathbb{F}_{\ell^i}$. If $\langle , \rangle$ is identically zero, the similitude and isometry group coincide with $\mathrm{GL}_n(\ell^i)$. When $\langle , \rangle$ is symplectic the similitude group is denoted by $\mathrm{GSp}_n(\ell^i)$. In this case the isometry group $\mathrm{Sp}_n(\ell^i)$ consists of determinant one matrices.

The above defines a natural chain of groups

$$S \leq I \leq \Delta \leq \Gamma \leq A.$$

This chain is A invariant, that is, each group is normalised by A.

The group of scalar matrices isomorphic to $\mathbb{F}_{\ell^i}^*$ is a normal subgroup of A. This allows us define $\bar{X}$ the reduction modulo scalars for any group X in the chain above.

For simplicity suppose $\ell \geq 5$ and $n \geq 4$. Then we have the following.

Theorem 3.1 [18, Theorems 2.1.3 and 2.1.4] *$\bar{S}$ is a non-abelian simple group and its automorphism group* $\mathrm{Aut}(\bar{S})$ *equals* $\bar{A}$.

References to both original and modern proofs of the above may be found on page 16 of [18].

Combining the above theorem with the well-known lemma below gives us a corollary of great importance for Sect. 3.5.

Lemma 3.2 *Let $\bar{S}$ be a non-abelian simple group. Let $\bar{S} \leq H \leq \mathrm{Aut}(\bar{S})$ where $\bar{S}$ is identified with its inner automorphism group. Then*

$$N_{\mathrm{Aut}(\bar{S})}(H) \cong \mathrm{Aut}(H)$$

via the canonical map.

Corollary 3.3 *Let $\bar{S} \leq H \leq \mathrm{Aut}(\bar{S})$, $n \geq 4$. Then if*

- *$\bar{S} = \mathrm{PSL}_n(\ell^i)$, every automorphism of H is of the form $u \mapsto (MuM^{-1})^\sigma$ or $u \mapsto (Mu^{-T}M^{-1})^\sigma$ where $M \in \mathrm{PGL}_n(\ell^i)$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{\ell^i})$.*
- *$\bar{S} = \mathrm{PSU}_n(\ell^{i/2})$, every automorphism of H is of the form $u \mapsto (MuM^{-1})^\sigma$ where $M \in \mathrm{PGL}_n(\ell^i)$ normalises $\bar{S}$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{\ell^i})$.*

We will make use of the following lemma in Sect. 5.3.

Lemma 3.4 *Let $M \in \mathrm{GSp}_{2g}(\ell^i)$, then ϕ, the minimal polynomial of M, satisfies*

$$\phi(x) = \frac{x^{2g}}{\chi(M)^g}\phi\left(\frac{\chi(M)}{x}\right).$$

Proof We have $M^T B M = \chi(M)B$, where B represents $\langle , \rangle$ with respect to some basis. Using this we obtain the following:

$$\begin{aligned}\det(M - xI_n) &= \det(BMB^{-1} - xI_n)\\ &= \det(M^{-T}\chi(M) - xI_n)\\ &= x^{2g}\det(M)^{-1}\det(M - \frac{\chi(M)}{x}I_n).\end{aligned}$$

The determinant of M is equal to $\chi(M)^g$ [18, Lemma 2.4.5], so the result follows. □

When necessary we shall write a subscript on the determinant map $\det_{\ell^i}$ to emphasise the determinant is being taken with the underlying vector space viewed over $\mathbb{F}_{\ell^i}$.

3.2 Centralisers in the symplectic group

In the next subsection, we will see that the automorphism $[\zeta_r]$ of J preserves the Weil pairing and commutes with the action of the Galois group $G_{\mathbb{Q}(\zeta_r)}$. Recall that in Sect. 2, we defined subrepresentations

$$\rho_\lambda : G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}\,(J[\lambda])$$

in order to help study the representation attached to the ℓ-torsion

$$\rho_\ell : G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}\,(J[\ell]).$$

In this subsection we will lay the purely group theoretic foundations needed to give a rough "upper bound" for the images of the above representations. That is, we shall now describe the centraliser of an element of prime order $r \neq \ell$ and trivial determinant in $\mathrm{GSp}_n(\ell)$.

The description of these centralisers is due to Wall [37], see also [5, Chapter 3.4.1]. Giving this description will rely upon various other facts about the classical groups and we will recall these as we go along, our main reference for these is [18].

Let $\zeta \in \mathrm{Sp}_{2g}(\ell)$ be an element of prime order $r \neq \ell$ which fixes no non-zero vector. Let i be the least positive integer such that $\mathbb{F}_{\ell^i}$ contains r-th roots of unity, equivalently, the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)$.

If i is *odd*, the characteristic polynomial of ζ is of the form

$$(\phi_1\bar{\phi}_1)^{a_1} \dots (\phi_t\bar{\phi}_t)^{a_t}$$

where each ϕ_j is irreducible of degree i and $\bar{\phi}_j$ is the polynomial whose roots are the multiplicative inverses of the roots of ϕ_j.

If i is *even* then the characteristic polynomial of ζ is of the form

$$\phi_1^{a_1} \dots \phi_t^{a_t}$$

and each ϕ_j is irreducible of degree i and has coefficients fixed by the involutory automorphism of $\mathbb{F}_{\ell^i}$.

In the following we let $G.n$ denote some extension of a group G by a cyclic group of order n. We note also that as 1 is not an eigenvalue of ζ, there is no $\mathrm{Sp}_e(\ell)$ factor as appears in [5] (See [5, Prop. 3.4.3]).

Theorem 3.5 [5, Remark 3.4.4], [37, Page 36] *The centraliser of ζ in $\mathrm{GSp}_{2g}(\ell)$ satisfies*

$$C_{\mathrm{GSp}_{2g}(\ell)}(\zeta) = C_{\mathrm{Sp}_{2g}(\ell)}(\zeta)\langle\chi\rangle = C_{\mathrm{Sp}_{2g}(\ell)}(\zeta).(\ell-1)$$

where χ acts as a similarity on each factor in an orthogonal decomposition fixed by ζ. Furthermore if i is odd, then

$$C_{\mathrm{Sp}_{2g}(\ell)}(\zeta) \cong \mathrm{GL}_{a_1}(\ell^i) \times \dots \times \mathrm{GL}_{a_t}(\ell^i),$$

if i is even, then

$$C_{\mathrm{Sp}_{2g}(\ell)}(\zeta) \cong \mathrm{GU}_{a_1}(\ell^{i/2}) \times \dots \times \mathrm{GU}_{a_t}(\ell^{i/2}).$$

We will need to switch between the mod ℓ and mod λ representations. Doing this amounts to understanding how the centralisers embed in $\mathrm{GSp}_{2g}(\ell)$.

Let us first consider i odd. In this case, using the characteristic polynomial, one can show ζ fixes an orthogonal decomposition of the form

$$(U_{1,1} \oplus U_{1,1}^*)\perp \dots \perp (U_{1,a_1} \oplus U_{1,a_1}^*)\perp \dots \perp (U_{t,1} \oplus U_{t,1}^*)\perp \dots \perp (U_{t,a_t} \oplus U_{t,a_t}^*)$$

where each $\{U_{j,k}, U_{j,k}^*\}$ is a pair of totally isotropic $\langle\zeta\rangle$-irreducible spaces of dimension i such that $U_{j,k} \oplus U_{j,k}^*$ is non-degenerate [5, Prop. 3.4.3]. Furthermore

$$U_j = U_{j,1}\perp \dots \perp U_{j,a_j}$$

is equal to the sum of eigenspaces of ζ with eigenvalues the roots of ϕ_j. Likewise

$$U_j^* = U_{j,1}^*\perp \dots \perp U_{j,a_j}^*$$

is equal to the sum of eigenspaces of ζ with eigenvalues the roots of $\bar{\phi}_j$.

An element in the centraliser of ζ must preserve each of the U_j and U_j^*. In fact, viewing U_j and U_j^* as a_j-dimensional spaces over $\mathbb{F}_{\ell^i}$, an element of $C_{\mathrm{Sp}_{2g}(\ell)}(\zeta)$, the centraliser of

ζ in $\mathrm{Sp}_{2g}(\ell)$, has, with respect to a suitable basis, a matrix on $U_j \oplus U_j^*$ of the form

$$\begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix} \text{ with } A \in \mathrm{GL}_{a_j}(\ell^i).$$

This describes an embedding $\mathrm{GL}_{a_j}(\ell^i) \hookrightarrow \mathrm{Sp}_{2a_j}(\ell^i) \leq \mathrm{GSp}_{2a_j}(\ell^i)$, which may be followed by embedding $\mathrm{GSp}_{2a_j}(\ell^i) \hookrightarrow \mathrm{GSp}_{2ia_j}(\ell)$. Running over all j we find $C_{\mathrm{Sp}_{2g}(\ell)}(\zeta) \leq \mathrm{GL}_{a_1}(\ell^i) \times \cdots \times \mathrm{GL}_{a_t}(\ell^i)$.

To correctly identify the image of Galois we need to go one step further and describe the centraliser of ζ in $\mathrm{GSp}_{2g}(\ell)$. As $U = U_1 \oplus \cdots \oplus U_t$ and $U^* = U_1^* \oplus \cdots \oplus U_t^*$ are both totally isotropic and $U \oplus U^*$ is non-degenerate, an element which acts as a scalar on U and the identity on U^* belongs to the similitude group $\mathrm{GSp}_n(\ell)$. In particular, if $\langle \mu \rangle = \mathbb{F}_\ell^*$, then

$$\begin{pmatrix} \mu I_g & 0 \\ 0 & I_g \end{pmatrix}$$

together with $\mathrm{Sp}_{2g}(\ell)$ generate $\mathrm{GSp}_{2g}(\ell)$.

The similitude factor χ of $\mathrm{GSp}_{2a_j}(\ell^i)$ agrees with that of $\mathrm{GSp}_{2ia_j}(\ell)$ on elements whose image lie in $\mathbb{F}_\ell$ [18, Lemma 4.3.5]. Thus by restricting the action of the above element to $U_j \oplus U_j^*$, we find

$$\begin{pmatrix} \mu I_{a_j} & 0 \\ 0 & I_{a_j} \end{pmatrix} \text{ and } \begin{pmatrix} A & 0 \\ 0 & A^{-T} \end{pmatrix} \text{ with } A \in \mathrm{GL}_{a_j}(\ell^i)$$

belong to the centraliser of ζ on $U_j \oplus U_j^*$. Ranging over j, we deduce $C_{\mathrm{GSp}_{2g}(\ell)}(\zeta) = C_{\mathrm{Sp}_{2g}(\ell)}(\zeta) \rtimes \langle \chi \rangle$.

Recall that when i is *even*, the characteristic polynomial of ζ is of the form

$$\phi_1^{a_1} \dots \phi_t^{a_t}$$

and each ϕ_j is irreducible of degree i and has coefficients fixed by the involutory automorphism of $\mathbb{F}_{\ell^i}$. In this case, ζ fixes an orthogonal decomposition of the form

$$U_{1,1} \perp \cdots \perp U_{1,a_1} \perp \cdots \perp U_{t,1} \perp \cdots U_{t,a_t}$$

where each $U_{j,k}$ is a non-degenerate $\langle \zeta \rangle$-irreducible space of dimension i [5, Prop. 3.4.3]. Furthermore

$$U_j = U_{j,1} \perp \cdots \perp U_{j,a_j}$$

is equal to the sum of eigenspaces of ζ with eigenvalues the roots of ϕ_j.

An element in the centraliser of ζ must preserve each U_j. In fact, viewing U_j as an a_j-dimensional space over $\mathbb{F}_{\ell^i}$, an element of $C_{\mathrm{Sp}_{2g}(\ell)}(\zeta)$, the centraliser of ζ in $\mathrm{Sp}_{2g}(\ell)$, preserves, when restricted to U_j, a non-degenerate unitary pairing. Thus there is a clear containment

$$C_{\mathrm{Sp}_{2g}(\ell)}(\zeta) \leq \mathrm{GU}_{a_1}(\ell^{i/2}) \times \cdots \times \mathrm{GU}_{a_t}(\ell^{i/2}).$$

Let us describe the structure of $C_{\mathrm{GSp}_{2g}(\ell)}(\zeta)$ and give an indication of how the $\mathrm{GU}_a(\ell^{i/2})$ factors are embedded into $\mathrm{Sp}_{2g}(\ell)$. This will be useful later when studying the image of our Galois representations in the quotient $\mathrm{GU}_a(\ell^{i/2})/\mathrm{SU}_a(\ell^{i/2})$.

Let $\langle , \rangle_\sharp \colon U_j \times U_j \to \mathbb{F}_{\ell^i}$ denote the unitary pairing from above. Let $\mu \in \mathbb{F}_{\ell^i}^*$ be an element sent to zero under the trace map $\mathrm{T} \colon \mathbb{F}_{\ell^i} \to \mathbb{F}_{\ell^{i/2}}$. Then the map $\mathrm{T}\left(\mu \langle , \rangle_\sharp\right) : U_j \times U_j \to \mathbb{F}_{\ell^{i/2}}$

is a symplectic pairing [18, pp. 117–118]. This provides us with an embedding of isometry groups $\mathrm{GU}_{a_j}(\ell^{i/2}) \hookrightarrow \mathrm{Sp}_{2a_j}(\ell^{i/2})$. In fact, as the image of the similitude group $\Delta\mathrm{U}_{a_j}(\ell^{i/2})$ of $\langle , \rangle_\sharp$ under the multiplier lands in $\mathbb{F}_{\ell^{i/2}}$ [18, pp.23], we also obtain an embedding of similitude groups $\Delta\mathrm{U}_{a_j}(\ell^{i/2}) \hookrightarrow \mathrm{GSp}_{2a_j}(\ell^{i/2})$ [18, pp.118]. Finally one embeds $\mathrm{GSp}_{2a_j}(\ell^{i/2})$ into $\mathrm{GSp}_{ia_j}(\ell) \leq \mathrm{GSp}_n(\ell)$ in the usual way. As the multiplier $\chi_\sharp$ of $\Delta\mathrm{U}_{a_j}(\ell^{i/2})$ agrees with that of $\mathrm{GSp}_{2a_j}(\ell^{i/2})$, we have that if $\sigma \in \Delta\mathrm{U}_{a_j}(\ell^{i/2})$ satisfies $\chi_\sharp(\sigma) \in \mathbb{F}_\ell$, then $\chi_\sharp(\sigma) = \chi(\sigma)$, where χ is the multiplier of $\mathrm{GSp}_{ia_j}(\ell)$ (and $\mathrm{GSp}_n(\ell)$) [18, Lemma 4.3.5].

The following corollary of Theorem 3.5 is of particular interest to us. We note that by H^t for H a group and $t \geq 1$ a natural number, we mean the direct product of t copies of H.

Corollary 3.6 *Let $n = \frac{2g}{r-1}$. Suppose the characteristic polynomial of $\zeta \in \mathrm{GSp}_{2g}(\ell)$ is*

$$(x^{r-1} + \cdots + x + 1)^n.$$

If i the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)$ is odd, then

$$C_{\mathrm{Sp}_{2g}(\ell)}(\zeta) \cong \mathrm{GL}_n(\ell^i)^t$$

where $2t$ is the number of distinct primes above ℓ in $\mathbb{Q}(\zeta_r)$.

If i is even, then

$$C_{\mathrm{Sp}_{2g}(\ell)}(\zeta) \cong \mathrm{GU}_n(\ell^{i/2})^t$$

where t is the number of distinct primes above ℓ in $\mathbb{Q}(\zeta_r)$.

Proof Immediate by Dedekind-Kummer and Theorem 3.5. □

3.3 Restrictions on the image of ρ_ℓ

We shall now use results of the previous subsection to describe restrictions on the image of ρ_ℓ. Further restrictions will be analysed in Sect. 6. Throughout this subsection we set $n = \frac{2g}{r-1}$.

Lemma 3.7 *The linear map induced by $[\zeta_r]$ on $J[\ell]$ is invertible and preserves the Weil pairing.*

Proof The inverse of $[\zeta_r]$ is given by taking its complex conjugate $[\bar{\zeta}_r]$. Indeed, as the eigenvalues of each of these maps are units they always induce non-singular linear maps modulo any given prime.

Standard properties of the Rosati involution [23, pgs. 189, 192] along with Albert's Classification [23, Thm. 2, pg. 201] give us the following equality:

$$\langle [\zeta_r]P, [\zeta_r]Q\rangle = \langle P, [\bar{\zeta}_r][\zeta_r]Q\rangle = \langle P, Q\rangle \text{ for } P, Q \in J[\ell]$$

where $\langle , \rangle$ denotes the Weil pairing in the above equality. □

Lemma 3.8 *The characteristic polynomial of $[\zeta_r]$ acting on $J[\ell]$ equals $(x^{r-1}+\cdots+x+1)^n$.*

Proof The characteristic polynomial of $[\zeta_r]$ on $T_\ell(J)$ equals $(x^{r-1} + \cdots + x + 1)^n$. Indeed, by [19, Thm. 3.6] and [33, §5 Lemma 1, pg. 35] the representation of $\mathrm{End}^0(J)$ on $V_\ell(J)$ is a sum of a multiple of the reduced representation of $\mathbb{Q}[\zeta_r] \cong \mathrm{End}^0(J)$ and a 0-representation. However, as $1 \in \mathbb{Q}[\zeta_r] \cong \mathrm{End}^0(J)$ does not kill any torsion points, we see there is no 0-representation. The claim for $T_\ell(J)$ then follows by restricting to $[\zeta_r]$ and for $J[\ell]$ by reducing modulo ℓ. □

Recall that we use χ_ℓ to denote the mod ℓ cyclotomic character.

Theorem 3.9 *If i, the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)$, is odd, then the image of $\rho_\ell\colon G_{\mathbb{Q}(\zeta_r)} \to Aut(J[\ell])$ is contained in a group isomorphic to*

$$\mathrm{GL}_n(\ell^i)^t\langle\chi_\ell\rangle$$

where $2t$ is the number of distinct primes above ℓ in $\mathbb{Q}(\zeta_r)$.

If i is even, then the image of $\rho_\ell\colon G_{\mathbb{Q}(\zeta_r)} \to Aut(J[\ell])$ is contained in a group isomorphic to

$$\mathrm{GU}_n(\ell^{i/2})^t\langle\chi_\ell\rangle$$

where t is the number of distinct primes above ℓ in $\mathbb{Q}(\zeta_r)$.

Proof Immediate from Theorem 3.5, Corollary 3.6 and Lemmas 3.7 and 3.8. □

We note that there are further restrictions on the image of the mod ℓ representation, as will be discussed in Sect. 6.

Theorem 3.10 *The image of $\rho_\ell\colon G_{\mathbb{Q}(\zeta_r)} \to Aut(J[\ell])$ is contained in $\mathrm{GL}_n(\ell^i)$ if i is odd and $\Delta\mathrm{U}_n(\ell^{i/2})$ if i is even.*

Moreover, the subgroup $G_\lambda = \rho_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})})$ is contained in $\mathrm{GL}(\ell^i)$ if i is odd and $\mathrm{GU}_n(\ell^{i/2})$ if i is even.

Proof By Dedekind-Kummer, we may write $\lambda = (\ell, \phi(\zeta_r))$ for ϕ some irreducible factor of Φ_r modulo ℓ. Thus the action of $[\zeta_r]$ on $J[\lambda] \cong T_\lambda/\lambda T_\lambda$ satisfies $\phi([\zeta_r]) = 0$ (recall that by abuse of notation we use $[\zeta_r]$ to denote both the endomorphism of J and the linear map it induces on $J[\lambda]$). As ϕ is irreducible, it coincides with the minimal polynomial of $[\zeta_r]$ on $J[\lambda]$.

Let $\lambda'|\ell$ be a prime above ℓ. Write $\lambda' = (\ell, \phi')$. If ϕ has a root in common with ϕ', then by irreducibility $\phi = \phi'$ and so $\lambda = \lambda'$. Thus by a dimension count, it is easy to see that the sum of eigenspaces (over $\mathbb{F}_\ell$) of $[\zeta_r]$ with eigenvalues roots of ϕ is $J[\lambda]$.

Hence, the discussion in Sect. 3.2 implies that $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is contained in $\mathrm{GL}_n(\ell^i)$ if i is odd, and in $\Delta\mathrm{U}_n(\ell^{i/2})$ if i is even. Moreover, it shows $\rho_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})})$ is contained in $\mathrm{GL}_n(\ell^i)$ if i is odd, and in $\mathrm{GU}_n(\ell^{i/2})$ if i is even. □

Since the image of the mod ℓ cyclotomic character sits diagonally in the action of $\rho_\ell(G_{\mathbb{Q}(\zeta_r)})$ on the $J[\lambda]$, we see the task of determining $\rho_\ell(G_{\mathbb{Q}(\zeta_r)})$ is really to determine the G_λ. We break this down into two parts: first showing G_λ contains $\mathrm{SL}_n(\ell^i)$ for i odd (resp. $\mathrm{SU}_n(\ell^{i/2})$ for i even), and then identifying $\det_{\ell^i}(G_\lambda)$.

Since $\mathrm{SL}_n(\ell^i)$ (resp. $\mathrm{SU}_n(\ell^{i/2})$) is perfect for $n \geq 3$ and $\ell \geq 5$, it suffices to prove $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ contains $\mathrm{SL}_n(\ell^i)$ (resp. $\mathrm{SU}_n(\ell^{i/2})$) for i odd (resp. even) to accomplish the first part.

To achieve this we study the maximal subgroups of $\mathrm{GL}_n(\ell^i)$ and $\Delta\mathrm{U}_n(\ell^{i/2})$ in Sect. 3.4. The image of inertia subgroups are then used to rule out the containment of $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ in any maximal subgroup which does not contain $\mathrm{SL}_n(\ell^i)$ when i is odd and $\mathrm{SU}_n(\ell^{i/2})$ when i is even. Our method for proving primitivity is dependent on unramified extensions of the base field, see Sect. 5.2. For this reason we work with $\rho(G_{\mathbb{Q}(\zeta_r)})$ rather than G_λ directly.

Let us now return to the definition of *large* used in Sect. 1. There we said the group $\rho_\ell(G_{\mathbb{Q}(\zeta_r)})$ was large if it contained the limit of the derived series of $C_{\mathrm{GSp}_{2g}(\ell)}(\zeta_r)$. It follows from Corollary 3.6 that this definition is equivalent to the following:

Definition 3.11 When i is odd, we say the image of $\rho_\lambda : G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}(J[\ell])$ is *large* if $\rho_\ell(G_{\mathbb{Q}(\zeta_r)})$ contains $\mathrm{SL}_n(\ell^i)^t$ where $2t$ is the number of distinct primes above ℓ in $\mathbb{Q}(\zeta_r)$.

When i is even, we say the image is *large* if $\rho_\ell(G_{\mathbb{Q}(\zeta_r)})$ contains $\mathrm{SU}_n(\ell^{i/2})^t$ where t is the number of distinct primes above ℓ in $\mathbb{Q}(\zeta_r)$.

For convenience, we make the definition:

Definition 3.12 We say G_λ is *large* when i is odd if G_λ contains $\mathrm{SL}_n(\ell^i)$. When i is even we say G_λ is *large* if it contains $\mathrm{SU}_n(\ell^{i/2})$.

3.4 Maximal subgroups of classical groups

In this section we will prove the necessary results concerning maximal subgroups of classical groups. For our applications in Sect. 7, we could, strictly speaking, get away with using results of Zalesskiĭ and Serežkin [40] which concern maximal subgroups of classical groups containing transvections. However, we prefer to give a classification of maximal subgroups containing a broader class of elements using techniques from modern group theory.

Our main reason for doing this is to provide the reader with alternative ways of constructing superelliptic curves with large Galois images should they desire it. Indeed, the reader will see that the tools provided by modern group theory allow one to easily classify maximal subgroups containing certain classes of elements.

Let S be one of $\mathrm{SL}_n(\ell^i)$, $\mathrm{SU}_n(\ell^{i/2})$, $\mathrm{Sp}_n(\ell^i)$ where $n > 4$, and G be a group satisfying $S \leq G \leq A$ (where A is as in Sect. 3.1). For $\tau \in G$, we define

$$\nu(\tau) \text{ to be the codimension of the largest eigenspace of } \tau.$$

For example, a transvection τ satisfies $\nu(\tau) = 1$. Indeed, the condition $\nu(\tau) = 1$ is equivalent to there being a constant $\mu \in \mathbb{F}_{\ell^i}$ such that $\tau - \mu I_n$ has rank one, and for a transvection we may simply take $\mu = 1$. In this section we shall give a description of maximal subgroups of G which contain an element τ of odd prime order with $\nu(\tau) = 1$.

To accomplish this task, we make use of the seminal work of Aschbacher [3], that of Kleidman and Liebeck [18], and of various other group theorists in recent times. Indeed, the maximal subgroups of G have been shown to belong to one of eight natural geometric collections $\mathcal{C}_1, \ldots, \mathcal{C}_8$ or an exceptional set $\mathcal{S}$.

Our first lemma will show any subgroup $H \leq G$ containing an element of the above form cannot lie in $\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_6$ or $\mathcal{C}_7$. For this reason we do not give a description of these families. On the other hand we now give a rough description of the groups belonging to $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_5$ and $\mathcal{C}_8$ along with the geometric structure they stabilise.

$\mathcal{C}_j$	Structure stabilised	Rough description in $\mathrm{GL}_n(\ell^i)$
$\mathcal{C}_1$	Non-degenerate or totally singular subspace	Maximal parabolic
$\mathcal{C}_2$	Decompositions of the form $V = \bigoplus_{j=1}^k V_j$, $\dim V_j = a$	$\mathrm{GL}_a(\ell^i) \wr S_k$, $n = ka$
$\mathcal{C}_5$	Subfields of $\mathbb{F}_{\ell^i}$ of prime index b	$\mathrm{GL}_n(\ell^{\frac{i}{b}})$, b prime
$\mathcal{C}_8$	Non-degenerate classical forms	$\mathrm{GSp}_n(\ell^i)$, n even $\mathrm{GO}_n^\varepsilon(\ell^i)$, ℓ odd $\mathrm{GU}_n(\ell^{i/2})$, i even

These families are referred to in the following way: $\mathcal{C}_1$ reducible subgroups; $\mathcal{C}_2$ imprimitive subgroups; $\mathcal{C}_5$ subfield subgroups; $\mathcal{C}_8$ classical subgroups.

Lemma 3.13 *Let G be as above, with $n > 4$ and suppose $\tau \in H < G$ has odd prime order and $\nu(\tau) = 1$. Then H is contained in a maximal subgroup of type $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_5, \mathcal{C}_8$ or $\mathcal{S}$.*

Proof We shall work through the subgroups of type $\mathcal{C}_3, \mathcal{C}_4, \mathcal{C}_6, \mathcal{C}_7$ successively showing τ cannot be contained in any of them.

We start with $\mathcal{C}_3$, the field extension subgroups. As $\nu(\tau) = 1$, the Jordan normal form of τ cannot be that of a field extension subgroup [20, Lemma 4.2]. Hence $H \notin \mathcal{C}_3$.

For $\mathcal{C}_4$ subgroups we use [20, Lemma 3.7] which tells us that an element with $\nu(\tau) = 1$ cannot preserve a non-trivial tensor decomposition. Thus $H \notin \mathcal{C}_4$.

Subgroups of type $\mathcal{C}_6$ may be dealt with using [6, Lemma 6.3], which states that any element σ belonging to a $\mathcal{C}_6$ type group must have $\nu(\sigma) \geq n/4$. As $n > 4$, and $\nu(\tau) = 1$, we deduce immediately that $H \notin \mathcal{C}_6$.

Finally, we deal with subgroups of type $\mathcal{C}_7$ by appealing to [6, Lemma 7.1]. Here, again, the fact that $\nu(\tau) = 1$ would force $n = 1$, but $n > 4$ so this is not possible. Hence $H \notin \mathcal{C}_7$. □

The groups belonging to $\mathcal{S}$ are known to be, modulo scalars, almost simple and act absolutely irreducibly on the underlying vector space. However a full list of possible groups in $\mathcal{S}$ is unknown. Nevertheless, results of Guralnick and Saxl [16] allow us to discount all groups appearing in $\mathcal{S}$.

Lemma 3.14 *Let $\ell \geq 5$ and G be as above with $n > 8$ (and $n \neq 10$ if $S = \mathrm{Sp}_n(\ell)$). Suppose $\tau \in H < G$ has odd prime order and $\tau - I_n$ has rank one. Then H belongs to a subgroup of type $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_5$, or $\mathcal{C}_8$.*

Proof By Lemma 3.13 and Theorem 7.1 of [16] (see also [7, Table 2.3] for the exception when $n = 10$) it suffices to show H is not the alternating or symmetric group of degree either $\dim V + 1$ or $\dim V + 2$ with V, the underlying vector space, isomorphic to the fully deleted permutation module.

Let us argue by the contrapositive. Then any element σ of order ℓ in H has $\nu(\sigma) \geq \ell - 3$. Indeed, let $\mathbb{F}[\Omega]$ be the corresponding permutation module (from which one obtains V). As a member of $\mathrm{Sym}(\Omega)$, our element σ is a product of ℓ-cycles, and thus as $\langle\sigma\rangle$-modules, we have

$$\mathbb{F}[\Omega] \cong \mathbb{F}[\sigma]^a \oplus \mathbb{F}^b$$

for some a, b with $a \neq 0$. The only eigenvalue of σ is 1 and the above description of $\mathbb{F}[\Omega]$ shows the codimension of the 1-eigenspace is $a(\ell - 1) \geq \ell - 1$. It follows that codimension of the 1-eigenspace of σ on V has dimension at least $\ell - 3$. Thus H does not contain transvections.

Furthermore, as the symmetric group has only two linear representations, $\det(V) \subseteq \{\pm 1\}$. It follows that H cannot contain such an element τ. This completes our proof by contrapositive, and hence the lemma. □

The following well-known lemma allows us to translate between the maximal subgroups of our groups $S \leq G \leq A$ and that of their projectivisations.

Lemma 3.15 *Let M be a maximal subgroup of G such that $MZ(G) = G$. Then M contains S.*

In particular, every maximal subgroup M of G not containing S, contains $Z(G)$ and hence gives rise to a maximal subgroup $\bar{M}$ of $\bar{G}$ not containing $\bar{S}$.

As the proof of this lemma is very short, we shall provide it for the reader's convenience.

Proof We have $M \geq [M, M] = [MZ(G), MZ(G)] = [G, G] \geq [S, S] = S$, as S is perfect [15, Thm. 1.7, Prop. 3.7, Thm. 11.22]. □

The next two theorems now follow directly from the above and the main theorem of [18].

Theorem 3.16 *Let H be a proper irreducible subgroup of G where $S = \mathrm{SU}_n(\ell^{i/2})$, $\ell \geq 5$, $n > 8$. Suppose $\tau \in H$ has odd prime order and $\tau - I_n$ has rank one. Then one of the following holds*

1. *H preserves a (transitive) imprimitivity decomposition of V;*
2. *H is contained in a subfield subgroup; or*
3. *H contains $\mathrm{SU}_n(\ell^{i/2})$.*

Theorem 3.17 *Let H be a proper irreducible subgroup of G where $S = \mathrm{SL}_n(\ell^i)$, $\ell \geq 5$, $n > 8$. Suppose $\tau \in H$ has odd prime order and $\tau - I_n$ has rank one. Then one of the following holds*

1. *H preserves a (transitive) imprimitivity decomposition of V;*
2. *H is contained in a subfield subgroup;*
3. *H is contained in a classical subgroup; or*
4. *H contains $\mathrm{SL}_n(\ell^i)$.*

3.5 Generating products of classical groups

Once we have shown $G_\lambda := \rho_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})})$ is large, we will need to argue $\rho_\ell(G_{\mathbb{Q}(\zeta_{r\ell})})$ is also large. To do this, we adapt a method pioneered by Serre and Ribet. Our starting point is Goursat's Lemma.

Lemma 3.18 (Goursat's Lemma) *Suppose H is a subgroup of a product of groups $G_1 \times G_2$ such that each projection map surjects $H \to G_1, G_2$. Let N_2 (resp. N_1) be the kernel of the projection onto G_1 (resp. G_2).*

Then, viewing N_1 (resp. N_2) as a subgroup of G_1 (resp. G_2), the image of H in $G_1/N_1 \times G_2/N_2$ is the graph of an isomorphism $\phi\colon G_1/N_1 \to G_2/N_2$.

As we will, in general, have more than two factors to deal with, Ribet's Lemma will prove indispensable.

Lemma 3.19 (Ribet's Lemma [28, Lemma 5.2.1]) *Let $S_1, \ldots, S_k$ be finite perfect groups. Let G be a subgroup of $S_1 \times \cdots \times S_k$ such that each projection $G \to S_i \times S_j$ $(1 \leq i < j \leq k)$ is surjective. Then $G = S_1 \times \cdots \times S_k$.*

Lemma 3.20 *Let $S \leq H$ be groups satisfying $S = [S, S] = [H, H]$ and writing $Z = Z(H)$ suppose that $\bar{S} = SZ/Z$ is a non-abelian simple group and the socle of $\bar{H} = H/Z$.*

Let N be a normal subgroup of H not containing S. Then $N \leq Z$ and $Z(H/N) = Z/N$.

Proof Since $N \lhd H$, the quotient group $\bar{N} = NZ/Z$ is normal in $\bar{H}$. As $\bar{S}$ is the unique minimal normal subgroup of $\bar{H}$, we have either $\bar{S} \lhd \bar{N}$, or $\bar{N} = 1$. If $\bar{N} = 1$, then $N \leq Z$. So suppose otherwise, so that $NZ \geq SZ \geq S$. Now, $[N, N] = [NZ, NZ] \geq [S, S] = S$. But $S = [H, H]$, so $S \geq [N, N]$. Hence $N \geq [N, N] = S$.

Let us now show the statement about $Z(H/N)$. As $Z(H/N)$ is a normal subgroup of H/N, its inverse image under the quotient map $H \to H/N$ is a normal subgroup of H containing N. Let us call this normal subgroup K.

If $K \supseteq S$, then K/N would be non-abelian as NS/N is non-abelian. Thus $K \not\supseteq S$ and we may apply the part of the lemma we have already proved to find $K \leq Z$. Hence $Z/N \supseteq Z(H/N)$.

The other inclusion is obvious, thus $Z/N = Z(H/N)$ as claimed. □

Recall from Corollary 3.6 that $C_{\mathrm{Sp}_{2g}(\ell)}(\zeta_r) \cong G_1 \times \cdots \times G_t$ where each $G_j \cong \mathrm{GL}_n(\ell^i)$ or $\mathrm{GU}_n(\ell^{i/2})$. In the following, we assume $\ell \geq 5, n \geq 4$.

Proposition 3.21 *Let H be a subgroup of $G = C_{\mathrm{Sp}_{2g}(\ell)}(\zeta_r) \cong G_1 \times \cdots \times G_t$ such that each projection H_j of H onto G_j contains the commutator subgroup S_j. Suppose there is an element $\tau \in H$ such that its projection onto each G_j has exactly one non-trivial eigenvalue of order r, and when viewed as an element of $\mathrm{Sp}_{2g}(\ell)$ its non-trivial eigenvalues are $\zeta_r, \zeta_r^2, \ldots, \zeta_r^{r-1}$ and all of multiplicity one. Then the image of $H \to G_j \times G_k$, $j \neq k$, contains $S_j \times S_k$.*

Proof Denote the image of $H \to G_j \times G_k$ by H_{jk}. Let N_j denote the kernel of $H_{jk} \to H_k$ and N_k the kernel of $H_{jk} \to H_j$. We may view N_j (resp. N_k) as a subgroup of H_j (resp. H_k). If either N_s contains S_s ($s = j, k$), then we are done.

Let us suppose this is not the case. As $\ell \geq 5, n \geq 4$ by Theorem 1.2 and [15, Thm. 1.7, Thm. 11.22], (note Theorem 1.2 also implies $\bar{S}_s$ is the socle of $\bar{H}_s$) we may apply Lemma 3.20. Thus N_s is contained in the centre Z_s of H_s.

Goursat's Lemma tells us the image of H_{jk} in $H_j/N_j \times H_k/N_k$ is the graph of an isomorphism $\phi\colon H_j/N_j \to H_k/N_k$. As ϕ maps the centre of H_j/N_j to the centre of H_k/N_k, there is an induced isomorphism $\bar{\phi}\colon H_j/Z_j \to H_k/Z_k$ (by Lemma 3.20 the centre of H_s/N_s is Z_s/N_s).

Now either $G_j \cong G_k \cong \mathrm{GL}_n(\ell^i)$ or $G_j \cong G_k \cong \mathrm{GU}_n(\ell^{i/2})$. Let us suppose for now we are in the first case. Then by Corollary 3.6 we see that for $(h_j, h_k) \in H_{jk}$, we have either $h_k = \chi(h_j)(Mh_jM^{-1})^\sigma$ or $h_k = \chi(h_j)(Mh_j^{-T}M^{-1})^\sigma$ where $M \in \mathrm{GL}_n(\ell^i)$, $\sigma \in \mathrm{Aut}(\mathbb{F}_{\ell^i}/\mathbb{F}_\ell)$ and $\chi\colon \mathrm{GL}_n(\ell^i) \to \mathbb{F}_{\ell^i}$ is a linear character.

Let τ_s denote the projection of τ to G_s and α_s be its non-trivial eigenvalue. The embeddings described in §3.2 show that when G_s is viewed as a subgroup of $\mathrm{GSp}_{2g}(\ell)$, then, on the corresponding subspace, τ has eigenvalues $\alpha_s^\sigma, \alpha_s^{-\sigma}$ as σ varies over all of $\mathrm{Aut}(\mathbb{F}_{\ell^i}/\mathbb{F}_\ell)$. As the non-trivial eigenvalues of τ, when viewed as an element of $\mathrm{Sp}_{2g}(\ell)$ are distinct, we see $\alpha_k \neq \alpha_j^\sigma, \alpha_j^{-\sigma}$ for any $\sigma \in \mathrm{Aut}(\mathbb{F}_{\ell^i}/\mathbb{F}_\ell)$.

As $\tau \in H$, we have by the above that either $\tau_k = \chi(\tau_j)(M\tau_jM^{-1})^\sigma$ or $\tau_k = \chi(\tau_j)(M\tau_j^{-T}M^{-1})^\sigma$. In either case, we must have $\chi(\tau_j) = 1$, because τ_j and τ_k have only one non-trivial eigenvalue. These equalities now imply $\alpha_k = \alpha_j^\sigma$ or $\alpha_j^{-\sigma}$ for some $\sigma \in \mathrm{Aut}(\mathbb{F}_{\ell^i}/\mathbb{F}_\ell)$, but this contradicts the above. We conclude $H_{jk} \supseteq S_j \times S_k$.

Let us now assume $G_j \cong G_k \cong \mathrm{GU}_n(\ell^{i/2})$. As above, Corollary 3.3 combined with Goursat's Lemma shows that for $(h_j, h_k) \in H_{jk}$, we have $h_k = \chi(h_j)(Mh_jM^{-1})^\sigma$. The above reasoning also applies to show the non-trivial eigenvalues of τ_j and τ_k cannot be Galois conjugate. These statements contradict, proving $H_{jk} \supseteq S_j \times S_k$. □

Applying Ribet's Lemma gives the following:

Theorem 3.22 *Let H be a subgroup of $C_{\mathrm{Sp}_{2g}(\ell)}(\zeta_r) \cong G_1 \times \cdots \times G_t$ such that each projection H_j of H onto G_j contains the commutator subgroup S_j. Suppose there is an element $\tau \in H$ such that its projection onto each G_j has exactly one non-trivial eigenvalue of order r, and when viewed as an element of $\mathrm{Sp}_{2g}(\ell)$ its non-trivial eigenvalues are $\zeta_r, \zeta_r^2, \ldots, \zeta_r^{r-1}$, all of multiplicity one. Then $H \supseteq S_1 \times \cdots \times S_t$.*

Proof Let $S = S_1 \times \cdots \times S_t$. Proposition 3.21 shows the image of the projection $H \cap S \to G_j \times G_k$ equals $S_j \times S_k$ for any $j \neq k$. Applying Ribet's Lemma (Lemma 3.19) to $H \cap S$ yields the result. □

4 Controlling inertia groups

In this section we continue to let ℓ, p, r be distinct primes. Let $F/\mathbb{Q}_p$ be a finite extension with ring of integers $\mathcal{O}_F$. Denote the discrete valuation of F by v_F, a uniformiser by π, and by $I_F \trianglelefteq \mathrm{Gal}(\overline{F}/F)$ the inertia subgroup.

For the convenience of the reader we recall the necessary notation from [11] for the below theorem.

Let $f = \sum_{i,j} a_{ij} x^i y^j \in F[x, y]$ be a non-zero polynomial, which is not a monomial. The following are Newton polytopes of f:

$$\begin{array}{ll} \Delta & = \text{convex hull}\big((i,j) \quad \big| \ a_{ij} \neq 0 \big) \subset \mathbb{R}^2, \\ \Delta_v & = \text{lower convex hull}\big((i,j,v_F(a_{ij})) \ \big| \ a_{ij} \neq 0 \big) \subset \mathbb{R}^2 \times \mathbb{R}. \end{array}$$

with Δ being the ordinary Newton polygon of f. For every point $P = (i, j) \in \Delta$, we have a corresponding point $v_F(a_{ij}) \in \mathbb{R}$. This gives us a piecewise affine map $v\colon \Delta \to \mathbb{R}$ which breaks Δ into 2-dimensional *v-faces* and 1-dimensional *v-edges*, the images of faces and edges of the polytope Δ_v under the homeomorphic projection to Δ.

Let us write $\Delta(\mathbb{Z})$ for the integer points lying inside Δ, that is $\Delta(\mathbb{Z}) = \text{interior}(\Delta) \cap \mathbb{Z}^2$. We write $\Delta(\mathbb{Z})^{\mathcal{F}} \subseteq \Delta(\mathbb{Z})$ for points that are in the interiors of v-faces, and $\Delta(\mathbb{Z})^L$ for those lying on the v-edges (note $\Delta(\mathbb{Z})^L = \Delta(\mathbb{Z}) \backslash \Delta(\mathbb{Z})^{\mathcal{F}}$). For any of the above sets, we write $\mathbb{Z}_p$ as a subscript to indicate the subset of points for which $v(P) \in \mathbb{Z}_p$.

We shall later state conditions which imply Δ_v-regularity, but we will not define it here. Instead, we refer the reader to [11, Definition 3.9].

Theorem 4.1 [11, Thm 6.4] *Suppose C/F is a Δ_v-regular curve, and $\ell \neq p$. For $P \in \Delta(\mathbb{Z})_{\mathbb{Z}_p}$ define a tame character*

$$\chi_p\colon I_F \to \{\text{roots of unity}\}, \qquad \sigma \mapsto \sigma(\pi^{v(P)})/\pi^{v(P)}$$

Let V_{tame}^{ab}, V_{tame}^{toric} be the unique continuous ℓ-adic representations of I_F that decompose over $\bar{\mathbb{Q}}_\ell$ as

$$V_{tame}^{ab} \cong_{\bar{\mathbb{Q}}_\ell} \bigoplus_{P \in \Delta(\mathbb{Z})^{\mathcal{F}}_{\mathbb{Z}_p}} \left(\chi_P \oplus \chi_P^{-1} \right), \qquad V_{tame}^{toric} \cong_{\bar{\mathbb{Q}}_\ell} \bigoplus_{P \in \Delta(\mathbb{Z})^{L}_{\mathbb{Z}_p}} \chi_P.$$

Then there are isomorphisms of I_F-modules,

$$H^1_{\acute{e}t}(C_{\overline{F}}, \mathbb{Q}_\ell)^{I_{wild}} \cong V_\ell(J(C))^{I_{wild}} \cong V_{tame}^{ab} \oplus V_{tame}^{toric} \otimes \mathrm{Sp}(2)$$

where Sp(2) *denotes the 2-dimensional special ℓ-adic representation (see* [35, 4.1.4, 4.2.1]*). In particular, $J(C)$ is wildly ramified $\iff$ $\Delta(\mathbb{Z})_{\mathbb{Z}_P} \subsetneq \Delta(\mathbb{Z})$.*

Remark 4.2 The representations V_{tame}^{ab}, V_{tame}^{toric} are rational, that is they may be realised over $\mathbb{Q}$, see the proof of [11, Thm. 6.4].

Remark 4.3 Let us briefly define the representation $\mathrm{Sp}(2)\colon I_F \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ and give a subgroup with respect to which it is rational.

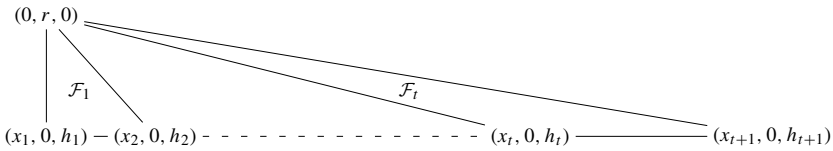
For every natural number n fix an ℓ^n-th root of unity ζ_{ℓ^n} such that $\zeta_{\ell^{n+1}}^{\ell} = \zeta_{\ell^n}$. Define the ℓ-adic tame character $t_\ell\colon I_F \to \mathbb{Z}_\ell$ by $\sigma \mapsto \sigma(\pi^{1/\ell^n}) = \zeta_{\ell^n}^{t_\ell(\sigma)}\pi^{1/\ell^n}$. Then $\mathrm{Sp}(2)\colon I_F \to \mathrm{GL}_2(\mathbb{Q}_\ell)$ is given by

$$\sigma \mapsto \begin{pmatrix} 1 & t_\ell(\sigma) \\ 0 & 1 \end{pmatrix}.$$

Clearly the preimage of matrices of the form $\left(\begin{smallmatrix} 1 & m \\ 0 & 1 \end{smallmatrix}\right)$, where $m \in \mathbb{Z}$, forms a subgroup of I_F whose image is rational.

Although we could get away with a less general version of the theorem below, we prove it in this form for its versatility, and afterwards deduce all cases we actually use as examples.

Theorem 4.4 *Suppose C/F is a Δ_v-regular curve, $p \neq r, \ell$ with Newton polytope Δ_v of the form:*



where

- $q_1, \ldots, q_t$ *is an increasing sequence of primes distinct from r and p;*
- $h_1, \ldots, h_t, h_{t+1}$ *a strictly decreasing sequence of natural numbers with $h_{t+1} = 0$; and*
- $x_{s+1} = \sum_{j=1}^{s} q_j$, *in particular $x_1 = 0$.*

Let $D_s := h_s - h_{s+1}$ for $1 \leq s \leq t$. Define the symbol γ_s to be 0 if $r | x_s$ and 1 otherwise. Define $\delta_s = 0$ if $q_s h_s + D_s x_s \equiv 0 \mod r$ and 1 otherwise. Then as I_F-modules,

$$V_{tame}^{ab} \cong_{\bar{\mathbb{Q}}_\ell} \bigoplus_{s=1}^{t} (\mathbb{Q}_\ell[C_{q_s}]^{D_s} \ominus \mathbb{Q}_\ell) \otimes (\mathbb{Q}_\ell[C_r]^{\delta_s} \ominus \mathbb{Q}_\ell) \oplus (\mathbb{Q}_\ell[C_r]^{\delta_s} \ominus \mathbb{Q}_\ell)^{\oplus \gamma_s + \gamma_{s+1} - 1}$$

$$V_{tame}^{toric} \cong_{\bar{\mathbb{Q}}_\ell} \bigoplus_{s=2}^{t} (\mathbb{Q}_\ell[C_r]^{h_s} \ominus \mathbb{Q}_\ell)^{\oplus(1-\gamma_s)}$$

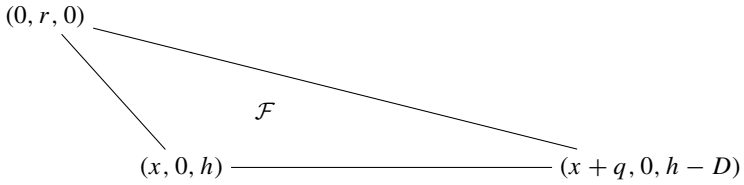
where $\mathbb{Q}_\ell[C_*]^a$ means we raise each individual irreducible constituent of $\mathbb{Q}_\ell[C_*]$ to the power of a.

Moreover, I_F acts tamely on $V_\ell(J(C))$ and as I_F-modules,

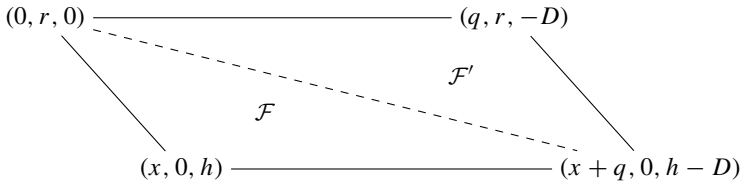
$$V_\ell(J(C)) \cong V_{tame}^{ab} \oplus V_{tame}^{toric} \otimes \mathrm{Sp}(2).$$

Note $\dim V_{tame}^{ab} + 2 \dim V_{tame}^{toric} = (r-1)(x_{t+1} - 2 + \gamma_{t+1}) = 2g$.

Proof Let us begin by looking at the contribution of one face at a time. To simplify notation, let us work with the face $\mathcal{F}$ as labelled below.



The points on $\mathcal{F}$ satisfy the equation $rDX + (qh + Dx)(Y - r) + rqZ = 0$. To apply Theorem 4.1, it will be easier to work with the following extension of $\mathcal{F}$,



We denote by $\hat{\mathcal{F}}$ the parallelogram obtained by joining $\mathcal{F}$ and $\mathcal{F}'$. We shall call an integral point of $\hat{\mathcal{F}}$ a point (X, Y, Z) lying on the interior of $\hat{\mathcal{F}}$ (in particular, not on its boundary) with integral X, Y values. There are $(q-1)(r-1)$ many integral points on $\hat{\mathcal{F}}$ if r divides x and $q(r-1)$ otherwise. If $r|x+q$, then $r-1$ of these points lie on the line L connecting $(0, r, 0)$ to $(x+q, 0, h-D)$. We call the denominator of an integral point the denominator of Z expressed in lowest terms. Note the denominator of an integral point divides rq and so by assumption is never divisible by p. Thus $\Delta(\mathbb{Z})_{\mathbb{Z}_P} = \Delta(\mathbb{Z})$ and $J(C)$ is tamely ramified by Theorem 4.1.

There is a bijection between integral points on $\mathcal{F}$ and $\mathcal{F}'$ given by

$$(X, Y, Z) \leftrightarrow (X, Y, Z)' = (x + q - X, r - Y, h - D - Z).$$

In the notation of Theorem 4.1, for a point P on $\mathcal{F}$, the associated character satisfies $\chi_{P'} = \chi_P^{-1}$. Thus to determine the contribution of $\mathcal{F}$ towards V_{tame}^{ab} it suffices to determine the equivalences classes of rqZ modulo rq as (X, Y, Z) ranges over the integral points on $\hat{\mathcal{F}}$ not lying on L.

Let $Z(X, Y) = (qh + Dx)(r - Y) - rDX$. Note $Z(X, Y)$ is an integer if X and Y are, and $(X, Y, \frac{1}{rq}Z(X, Y))$ is a point on $\hat{\mathcal{F}}$. Suppose X and Y are integers. Then $Z(X, Y) \equiv -(qh + Dx)Y \mod r$. As Y takes values strictly between 0 and r, we see $Z(X, Y) \equiv 0 \mod r$ if and only if $-(qh + Dx) \equiv 0 \mod r$ and furthermore if $-(qh + Dx) \not\equiv 0 \mod r$ then the equivalence class $Z(X, Y) \mod r$ only depends on Y.

Let us now study $Z(X, Y) = (qh+Dx)(r-Y)-rDX$ modulo q. If $q|D$, then $Z(X, Y) \equiv 0 \mod q$ always holds. Suppose $q \nmid D$, then $Z(X, Y) \equiv Dx(r - Y) - rDX \mod q$. As rD is invertible modulo q, we see for fixed Y value and X ranged over this line on $\hat{\mathcal{F}}$ that the quantity $Z(X, Y) \mod q$ runs over all equivalences classes if $r \nmid x$ and all non-zero classes if $r|x$.

The line L contains integral points in $\hat{\mathcal{F}}$ if and only if $r|x + q$. These points contribute towards V_{tame}^{toric} if and only if they belong to $\Delta(\mathbb{Z})$, equivalently, $x + q \neq x_{n+1}$. The equation of the line L connecting $(0, r, 0)$ to $(x + q, 0, h - D)$ is given by $\frac{-rX}{x+q} = Y - r = \frac{rZ}{D-h}$. Thus we see that if (X, Y, Z) is an integral point on L, then $Z(X, Y) = q(Y - r)(D - h)$ is always divisible by q and $Z(X, Y) \equiv qY(D - h) \equiv 0 \mod r$ if and only if $h - D \equiv 0 \mod r$.

Applying the Chinese Remainder Theorem and Theorem 4.1 concludes the proof. □

Corollary 4.5 *Suppose C/F is a Δ_v-regular curve determined by the affine chart $y^r = f(x)$, with potentially good reduction and Newton polytope Δ_v of the form given in Theorem 4.4. Then as $\mathbb{Q}(\zeta_r)_\lambda[I_F]$-modules,*

$$V_\lambda(J(C))^{I_{wild}} \cong V_\lambda(J(C)) \cong \bigoplus_{s=1}^{t}\bigoplus_{j=1}^{q_s-1}(\chi_{q_s}^{jD_s}\otimes\chi_{s,j}^{\delta_s})\oplus(\chi_s^{\delta_s})^{\oplus\gamma_s+\gamma_{s+1}-1}$$

where the $\chi_{s,j}$, χ_s (resp. χ_{q_s}) are primitive characters of order r (resp. q_s).

In particular, if $r\neq\ell$ and no q_s equals ℓ, then

$$\rho_\lambda|_{I_F} = \bigoplus_{s=1}^{t}\bigoplus_{j=1}^{q_s-1}(\chi_{q_s}^{jD_s}\otimes\chi_{s,j}^{\delta_s})\oplus(\chi_s^{\delta_s})^{\oplus\gamma_s+\gamma_{s+1}-1}$$

where by abuse of notation, we use the same symbols to denote the reductions of $\chi_{s,j}$, χ_s, χ_{q_s}.

Proof Theorem 4.4 gives us the isomorphism

$$V_\ell(J(C))^{I_{wild}} \cong V_\ell(J(C)) \cong V_{tame}^{ab}\oplus V_{tame}^{toric}\otimes \mathrm{Sp}(2)$$

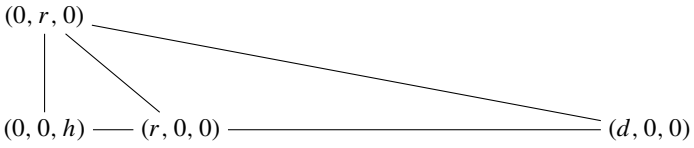
where $V_{tame}^{toric} = 0$ as C/F has potentially good reduction and

$$V_{tame}^{ab} \cong_{\bar{\mathbb{Q}}_\ell} \bigoplus_{s=1}^{t}(\mathbb{Q}_\ell[C_{q_s}]^{D_s}\ominus\mathbb{Q}_\ell)\otimes(\mathbb{Q}_\ell[C_r]^{\delta_s}\ominus\mathbb{Q}_\ell)\oplus(\mathbb{Q}_\ell[C_r]^{\delta_s}\ominus\mathbb{Q}_\ell)^{\oplus\gamma_s+\gamma_{s+1}-1}$$

(note $\gamma_1 = 0$ and $\gamma_s = 1$ for $2\leq s\leq t$). As V_{tame}^{ab} is a rational representation (see Remark 4.2), the corresponding $E\otimes_{\mathbb{Q}}\mathbb{Q}_\ell$ representation $V_\ell(J(C))$ of I_F, may be realised over E, so we may apply Proposition 2.2 to see that the entries of the matrix representations of I_F on any two V_λ, $V_{\lambda'}$ with λ, $\lambda'|\ell$ differ by applying an element of $\mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})$. Sorting the characters appearing in $\rho_\ell|_{I_F}$ accordingly gives the required result.

The eigenvalues of $\rho_{\lambda^\infty}(\sigma)$ on T_λ are the same as those on $V_\lambda = T_\lambda\otimes\mathbb{Q}_\ell$, thus the result for $\rho_\lambda|_{I_F}$ follows by reducing $\rho_{\lambda^\infty}(\sigma)$ modulo λ and noting $\rho_\lambda|_{I_F}$ is semisimple as ℓ does not divide the order of $\rho_\lambda(I_F)$. □

Proposition 4.6 *Suppose C/F is a Δ_v-regular curve, d, h positive integers, $p\nmid r\ell h$, $\ell\nmid rh$, with Newton polytope Δ_v of the form:*



Then $\rho_\lambda\colon I_F\to Aut(J(C)[\lambda])$ factors through I_F^{tame}. The r-th power of a generator τ of $\rho_\lambda(I_F)$ is a transvection. Furthermore, if $r\nmid h$ then τ has exactly $r-2$ non-trivial eigenvalues all of which are primitive r-th roots of unity, else all of its eigenvalues are trivial.

Proof Let v' be the extension of v to $F^{1/r}{:=}F(\pi^{1/r})$, normalised so that $v'(\pi) = r$. The curve C has semistable reduction reduction over $F^{1/r}$ and is $\Delta_{v'}-$regular, as can be seen from the Newton polygon: all points of $\Delta(\mathbb{Z})$ have integer value under v'.

Theorem 3.13 of [11] provides us with a (proper, flat) regular model $\mathcal{C}/\mathcal{O}_{F^{1/r}}^{nr}$ of $C\times(F^{1/r})^{nr}$ with strict normal crossings. In the notation of this theorem, the inner v'-edge L has

slopes $s_1^L = h, s_2^L = 0$, and the denominator of every v'-edge and v'-face equals one. The theorem thus shows the special fibre of $\mathcal{C}$ consists of exactly two irreducible components with positive genus linked by r chains of $\mathbb{P}^1$'s of length $h-1$. Furthermore, all components have multiplicity one. In particular the special fibre $\mathcal{C}_{\bar{k}_{v'}}$ is geometrically reduced. The dual graph of $\mathcal{C}_{\bar{k}_{v'}}$ is thus given by two vertices joined by r arcs each consisting of h edges. Proposition 9.6.10 of [4] now applies to show $|\Phi(\bar{k}_{v'})| = rh^{r-1}$.

Applying Theorem 4.1, we obtain an isomorphism of tame $I_{F^{1/r}}$-modules $V_\ell(J(C)) \cong \mathbb{Q}_\ell^{\oplus 2(g-r+1)} \oplus \mathbb{Q}_\ell^{\oplus r-1} \otimes \mathrm{Sp}(2)$. Thus, by Proposition 2.2 applied to an appropriate subgroup of $I_{F^{1/r}}$ (see Remark 4.3), we see that for each λ, the group $\rho_{\lambda^\infty}(I_{F^{1/r}})$ contains a transvection. As ℓ does not divide $|\Phi(\bar{k}_{v'})| = rh^{r-1}$, it follows from [31, Lemmas 1 & 2] that $2g - \dim_{\mathbb{F}_\ell} J(C)[\ell]^{I_{F^{1/r}}} = r-1$, thus we see each $\rho_\lambda(I_{F^{1/r}})$ also contains a transvection.

Theorem 4.1 applies to show that as tame I_F-modules $V_\ell(J(C)) \cong V_{tame}^{ab} \oplus V_{tame}^{toric} \otimes \mathrm{Sp}(2)$ where $V_{tame}^{ab} \cong (\mathbb{Q}_\ell[C_r]^h \ominus \mathbb{Q}_\ell)^{\oplus r-2}$ and $V_{tame}^{toric} \cong \mathbb{Q}_\ell^{\oplus r-1}$. If $r|h$, then the claim follows immediately. Thus suppose $r \nmid h$.

Recall that the action of I_F on $V_\ell(J(C))$ factors through $I_F^{tame} \cong \prod_{p' \neq p} \mathbb{Z}_{p'}$ [26, pp. 410]. Furthermore, the action of I_F^{tame} on V_{tame}^{ab} factors through a group isomorphic to $\mathbb{Z}_r$ and its action on $V_{tame}^{toric} \otimes \mathrm{Sp}(2)$ through a group isomorphic to $\mathbb{Z}_\ell$. In particular, we can find a subgroup I of I_F^{tame} which acts faithfully (and rationally) on V_{tame}^{ab}, rationally on $V_{tame}^{toric} \otimes \mathrm{Sp}(2)$ and whose image $\rho_{\lambda^\infty}(I)$ in $\rho_{\lambda^\infty}(I_F)$ is dense (see Remarks 4.2, 4.3). Thus Proposition 2.2 applies to the $(E \otimes \mathbb{Q}_\ell)[I]$-module $V_\ell(J(C))$, and moreover there exist generators $\tau \in \rho_{\lambda^\infty}(I_F)$ and $\tau' \in \rho_{\lambda^\infty}(I)$ with the same eigenvalues.

It follows that the non-trivial eigenvalues of τ are primitive r-th roots of unity and are $r-2$ in number. As the eigenvalues of τ on T_λ are equal to those on V_λ, we see the reduction modulo λ also has exactly $r-2$ non-trivial eigenvalues which are all primitive r-th roots of unity. Observing that $\rho_\lambda(I_F)^r = \rho_\lambda(I_{F^{1/r}})$ completes the proof. □

Remark 4.7 Suppose $C'\colon y^r = g(x)$ defines a Δ_v-regular superelliptic curve with $g(x) \in F[x]$ monic and degree coprime to r. Let $h(x) \in F[x]$ be both coprime to g modulo π and separable modulo π. Let $C\colon y^r = g(x)h(x)$, then C defines a Δ_v-regular superelliptic curve. Furthermore, by considering the Newton polytopes of C and C', we see that as I_F-modules,

$$H^1_{\acute{e}t}(C_{\overline{F}}, \mathbb{Q}_\ell)^{I_{wild}} \cong H^1_{\acute{e}t}(C'_{\overline{F}}, \mathbb{Q}_\ell)^{I_{wild}} \oplus \mathbb{Q}_\ell^{\oplus m}$$

for some appropriate value of m. The analogous statement carries through for $V_\lambda(J(C))$ and $V_\lambda(J(C'))$.

The restriction and reduction of a polynomial, along with their relation to Δ_v-regularity, are defined on pages 2533 and 2534 of [11].

Remark 4.8 Suppose the Newton polytope of the superelliptic curve $C\colon y^r = f(x)$ with $f(0) \neq 0$, is of the form required in either Theorem 4.4 or Proposition 4.6. To check C is Δ_v-regular, it suffices to check $\overline{f|_L}$ is squarefree modulo π for each horizontal v-edge L of Δ.

Indeed, if L is a non-horizontal v-edge of Δ, then $\overline{(y^r - f)|_L}$ is of the form $X + a$ or $X^r + a$ where $\pi \nmid a$ and so is square free as $r \neq p$. Likewise, for a v-face $\mathcal{F}$, either $\overline{(y^r - f)|_\mathcal{F}} = Y + G(X)$ or $\overline{(y^r - f)|_\mathcal{F}} = Y^r + G(X)$ where $G(X)$ is some function of X. As we work in $\mathbb{G}_m^2$, taking the partial derivative with respect to Y shows the associated scheme $X_\mathcal{F}$ (see Definition 3.7 [11]) is smooth in both cases.

The point in the Newton polygon corresponding to y^r does not belong to $\bar{L}(\mathbb{Z})_\mathbb{Z}$ for any horizontal v-edge of Δ. Thus $\overline{(f - y^r)|_L} = \overline{f|_L}$.

Definition 4.9 We shall say that a polynomial $f \in F[x]$ has *v-degree* $(q_1, \ldots, q_t)$ and *height* $(h_1, \ldots, h_t)$, if

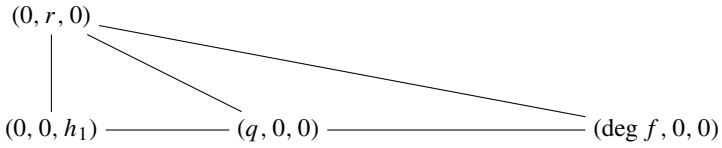
- f has no repeated roots over $F[x]$;
- there exists some $a \in \mathcal{O}_F$ such that $f(x-a)$ can be factored into monic polynomials g, h over an algebraic closure such that $g(x) \equiv x^{\deg(g)} \mod \pi$, h is separable modulo π, $h(0) \neq 0 \mod \pi$, $r | \deg(g) \iff h = 1$; and
- either $C\colon y^r = f(x-a)$ defines a superelliptic curve satisfying the hypotheses of Proposition 4.6, or $C\colon y^r = g(x)$ defines a superelliptic curve satisfying Theorem 4.4 with $q_1, \ldots, q_t$ and $h_1, \ldots, h_t$ as given.

In particular this means $p, \ell, q_1, \ldots, q_t$ are not equal to r, unless $t = 1$ and C satisfies Proposition 4.6.

If $h_s = h_{s+1} + 1$ and $h_t = 1$, then we shorten the above and simply say $f \in F[x]$ has v-degree $(q_1, \ldots, q_t)$.

Remark 4.10 Let $f \in F[x]$ have v-degree $(q_1, \ldots, q_t)$ and height $(h_1, \ldots, h_t)$ with $h_s - h_{s+1}$ coprime to q_s, where we take $h_{t+1} = 0$, as in Theorem 4.4. Suppose that $\frac{h_j - h_{j+1}}{q_j} \neq \frac{h_k - h_{k+1}}{q_k}$ for $j \neq k$. Then $C\colon y^r = f(x-a)$ is Δ_v-regular. Indeed, let $f_a(x) := f(x-a)$, then for every horizontal line L in the Newton polytope, $\overline{f_a|_L}$ is either linear or $\overline{f_a|_L} = h$ and hence squarefree modulo π in either case.

Example 4.11 Let p, q, r be distinct primes, and $h_1 \in \mathbb{N}_{>0}$ not divisible by q. Let $f \in F[x]$ have v-degree q and height h_1. For example, if $v(p) = 1$, we can take $h(x) \in F[x]$ monic, separable modulo π with $v(h(0)) = 0$ and $f(x) = (x^q - p^{h_1})h(x)$. The above implies $C\colon y^r = f(x)$ is Δ_v-regular and has Newton polygon



and as I_F-modules,

$$V_\ell(J(C)) \cong_{\bar{\mathbb{Q}}_\ell} \mathbb{Q}_\ell^{\oplus m} \oplus (\mathbb{Q}_\ell[C_q]^{h_1} \ominus \mathbb{Q}_\ell) \otimes (\mathbb{Q}_\ell[C_r]^{h_1} \ominus \mathbb{Q}_\ell)$$

with wild inertia acting trivially and m some integer divisible by $r-1$. This in turn carries over to give

$$V_\lambda \cong_{\bar{\mathbb{Q}}_\ell} \mathbb{Q}(\zeta_r)_\lambda^{\oplus \frac{m}{r-1}} \oplus \bigoplus_{j=1}^{q-1} \chi_q^{jh_1} \otimes \chi_j^{h_1}$$

where the χ_j are primitive characters of order r and χ_q is a primitive character of order q.

The representation modulo λ then satisfies

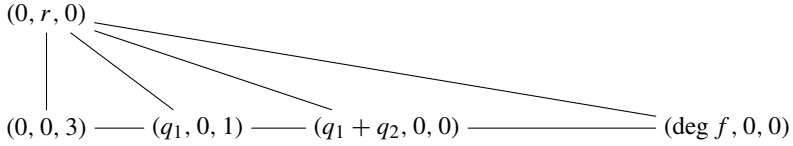
$$(\rho_\lambda)_{I_F} = \mathbb{F}_{\ell^i}^{\oplus \frac{m}{r-1}} \oplus \bigoplus_{j=1}^{q-1} \chi_q^{jh_1} \otimes \chi_j^{h_1}$$

where again by abuse of notation, we use the same symbols to denote the reductions of χ_j, χ_q.

In particular, if $q = 2$ and $h_1 = 1$, that is, f has v-degree 2, then $\rho_\ell(I_F)$ is generated by a semisimple element τ with exactly $r-1$ non-trivial eigenvalues which are all distinct and have common order equal to $2r$.

Furthermore, the restriction τ_λ of τ to $J[\lambda]$ has exactly one non-trivial eigenvalue when $J[\lambda]$ is viewed as a vector space over $\mathbb{F}_{\ell^i}$.

Example 4.12 Let $p \neq q_1, q_2$ be primes not equal to r, with $q_1 \leq q_2$ and $q_1 + q_2 \not\equiv 0 \mod r$. Let $f \in F[x]$ have v-degree (q_1, q_2) and height $(3, 1)$. For example, if $v(p) = 1$, we may take $h(x) \in F[x]$ monic, separable mod π with $v(h(0)) = 0$ and then set $f(x) = (x^{q_1} - p)(x^{q_2} - p^2)h(x)$. The above implies $C\colon y^r = f(x)$ is Δ_v-regular with Newton polygon



and as I_F-modules,

$$V_\ell(J(C)) \cong_{\bar{\mathbb{Q}}_\ell} \mathbb{Q}_\ell^{\oplus m} \oplus (\mathbb{Q}_\ell[C_{q_1}]^2 \ominus \mathbb{Q}_\ell) \otimes (\mathbb{Q}_\ell[C_r]^3 \ominus \mathbb{Q}_\ell) \oplus (\mathbb{Q}_\ell[C_{q_2}] \ominus \mathbb{Q}_\ell) \otimes (\mathbb{Q}_\ell[C_r]^{q_1+2q_2} \ominus \mathbb{Q}_\ell)$$

with wild inertia acting trivially and m being some integer divisible by $r-1$. This in turn carries over to give

$$V_\lambda \cong_{\bar{\mathbb{Q}}_\ell} \mathbb{Q}(\zeta_r)_\lambda^{\oplus \frac{m}{r-1}} \oplus \bigoplus_{j=1}^{q_1-1} \chi_{q_1}^{2j} \otimes \chi_j^3 \oplus \bigoplus_{k=1}^{q_2-1} \chi_{q_2}^k \otimes \chi_k^{q_1+2q_2}$$

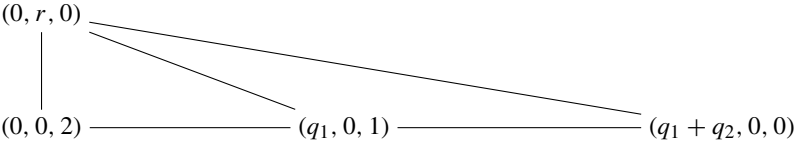
where the χ_j, χ_k are primitive characters of order r and the χ_{q_s} are primitive characters of order q_s.

The representation modulo λ then satisfies

$$(\rho_\lambda)_{I_F} = \mathbb{F}_{\ell^i}^{\oplus \frac{m}{r-1}} \oplus \bigoplus_{j=1}^{q_1-1} \chi_{q_1}^{2j} \otimes \chi_j^3 \oplus \bigoplus_{k=1}^{q_2-1} \chi_{q_2}^k \otimes \chi_k^{q_1+2q_2}$$

where again by abuse of notation, we use the same symbols to denote the reductions of χ_j, χ_k, χ_{q_s}.

Example 4.13 Let p, q_1, q_2, r be distinct primes with $q_1 < q_2$ and $q_1 + q_2 \equiv 0 \mod r$. Let f have π-degree (q_1, q_2). For example, if $v(p) = 1$, we may take $f(x) = (x^{q_1} - p)(x^{q_2} - p)$. The above implies $C\colon y^r = f(x)$ is Δ_v-regular and has Newton polygon



and as I_F-modules,

$$V_\ell(J(C)) \cong_{\bar{\mathbb{Q}}_\ell} (\mathbb{Q}_\ell[C_{q_1}] \ominus \mathbb{Q}_\ell) \otimes (\mathbb{Q}_\ell[C_r]^2 \ominus \mathbb{Q}_\ell) \oplus (\mathbb{Q}_\ell[C_{q_2}] \ominus \mathbb{Q}_\ell) \otimes (\mathbb{Q}_\ell[C_r]^{q_1+2q_2} \ominus \mathbb{Q}_\ell)$$

with wild inertia acting trivially and m some integer divisible by $r-1$. This in turn carries over to give

$$V_\lambda \cong_{\bar{\mathbb{Q}}_\ell} \bigoplus_{j=1}^{q_1-1} \chi_{q_1}^j \otimes \chi_j^2 \oplus \bigoplus_{k=1}^{q_2-1} \chi_{q_2}^k \otimes \chi_k^{q_1+2q_2}$$

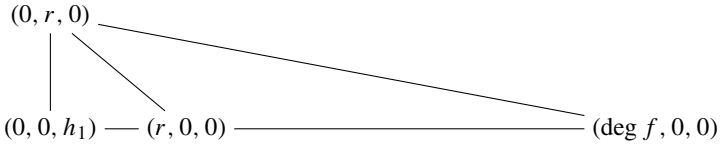
where the χ_j, χ_k are primitive characters of order r and the χ_{q_s} are primitive characters of order q_s.

The representation modulo λ then satisfies

$$(\rho_\lambda)_{I_F} = \bigoplus_{j=1}^{q_1-1} \chi_{q_1}^j \otimes \chi_j^2 \oplus \bigoplus_{k=1}^{q_2-1} \chi_{q_2}^k \otimes \chi_k^{q_1+2q_2}$$

where again by abuse of notation, we use the same symbols to denote the reductions of $\chi_j, \chi_k, \chi_{q_s}$.

Example 4.14 Let $p \neq r$ be primes, and $h_1 \in \mathbb{N}_{>0}$ not divisible by r. Let $f \in F[x]$ have p-degree r and height h_1. For example, if $v(p) = 1$, we can take $h(x) \in F[x]$ monic, separable mod π with $v(h(0)) = 0$ and set $f(x) = (x^r - p^{h_1})h(x)$. The above implies $C\colon y^r = f(x)$ is Δ_v-regular and has Newton polygon



and as I_F-modules,

$$V_\ell(J(C)) \cong_{\bar{\mathbb{Q}}_\ell} \mathbb{Q}_\ell^{\oplus m} \oplus (\mathbb{Q}_\ell[C_r]^{h_1} \ominus \mathbb{Q}_\ell)^{\oplus r-2} \oplus \mathrm{Sp}(2) \otimes \mathbb{Q}_\ell^{\oplus r-1}$$

with wild inertia acting trivially and m some integer divisible by $r-1$.

Furthermore the action of $\rho_{\lambda\infty}(I_F)$ and $\rho_\lambda(I_F)$ is as given by Proposition 4.6.

A theorem of Silverberg [34, Thm 4.1] shows $\mathbb{Q}(\zeta_r)$ must be contained in the ℓ-torsion field of J for any odd prime ℓ. As a consequence, the criterion of Néron-Ogg-Shafarevich tells us that if $F/\mathbb{Q}_r$ is a finite extension and J/F has good reduction then F must contain primitive r-th roots of unity. The below lemma not only shows we may find superelliptic curves $J/\mathbb{Q}_r(\zeta_r)$ with good reduction, but also tells us how to produce them.

Lemma 4.15 *Let F be a finite extension of $\mathbb{Q}_r(\zeta_r)$ and π a uniformiser in $\mathbb{Q}_r(\zeta_r)$. Set*

$$f(x) = x^{rs} + a_{rs-1}x^{rs-1} + \cdots + a_1 x + a_0 \in F[x].$$

If either

(i) $a_0 - \left(\frac{1}{\pi}\right)^r \in \mathcal{O}_F$, $a_{rs-1} \in \mathcal{O}_F^*$ *and* $a_j \in \mathcal{O}_F$ *for* $1 \leq j \leq rs-2$, *or*
(i) $a_0 \equiv b\pi^{r(s-1)} \mod \pi^{rs}$, *where* $b \equiv 1 \mod \pi^r$, $a_{rs-1} \equiv u\pi \mod \pi^2$ *with* $u \in \mathcal{O}_F^*$, *and* $a_j \equiv 0 \mod \pi^{rs-j}$ *for* $1 \leq j \leq rs-2$,

then C/F has good reduction. In particular I_F acts trivially on $J[\ell]$ for $\ell \neq r$.

Proof The second assertion follows from the first by taking $x = \pi X$ and $y = \pi^s Y$. It thus suffices to prove the first assertion, which we shall now do.

The substitution $y \mapsto Y + \frac{1}{\pi}$, provides us with the model

$$\left(Y + \frac{1}{\pi}\right)^r - \left(\frac{1}{\pi}\right)^r = f(x) - \left(\frac{1}{\pi}\right)^r. \tag{4.16}$$

The leading coefficient on the left hand side is non-zero modulo π. Likewise the coefficient of Y is a unit, since by the binomial expansion this equals $\frac{r}{\pi^{r-1}}$ and $\mathbb{Q}_r(\zeta_r)/\mathbb{Q}_r$ is a totally ramified extension of degree $r-1$. As the binomial coefficient $\binom{r}{i}$ is divisible by r for $1 \leq i \leq r-1$, we see the coefficient of Y^i is zero modulo π for $2 \leq i \leq r-1$.

It follows the left hand side of (4.16) taken modulo π is congruent to $Y^r + uY$ reduced modulo π where u is a unit in $\mathbb{Z}_r[\zeta_r]$. Our assumptions on the coefficients of $f(x)$ allow us to reduce our affine model (4.16) modulo π. As the partial derivative with respect to Y is non-zero modulo π, we find all points on this chart are smooth.

Making the substitution $V = 1/x$, $W = Y/x^s$ in (4.16) we obtain a chart containing the points at infinity:

$$\left(W + \frac{1}{\pi}V^s\right)^r - \left(\frac{1}{\pi}\right)^r V^{rs} = V^{rs}\left(f(1/V) - \left(\frac{1}{\pi}\right)^r\right).$$

Any point at infinity has $V = 0$, so the above simplifies to $W^r = 1$ giving r distinct points. The partial derivative with respect to V at $V = 0$ is a unit since the coefficient of V on the right hand side is $a_{rs-1} \in \mathcal{O}_F^*$. It follows that our curve has good reduction. Hence, by the criterion of Néron-Ogg-Shafarevich I_F acts trivially on $J[\ell]$ for $\ell \neq r$. □

5 Image of inertia

Let ℓ be a prime, m a positive integer and r a prime. Let K be a number field. For primes $\mathfrak{p}, \mathfrak{p}_j$ in K we let p, p_j denote the rational primes below. Let V denote a finite dimensional vector space over $\overline{\mathbb{F}}_\ell$.

We allow subscripts on representations to denote restrictions to subgroups.

The following definition along with Proposition 5.5 were inspired by [1, Proposition 3.1].

Definition 5.1 Let $p, q_1, \ldots, q_t$ be primes distinct from ℓ. We say $\rho\colon G_K \to \mathrm{GL}(V)$ has $\mathfrak{p}$-*system* $(q_1, \ldots, q_t)$ if neither ℓ nor p divide $|\rho(I_\mathfrak{p})|$ and

$$\rho_{I_\mathfrak{p}} \cong_{\overline{\mathbb{F}}_\ell} \psi \oplus \bigoplus_{s=1}^{t} \bigoplus_{j=1}^{q_s-1} \chi_{s,j} \otimes \chi_{q_s}^{j},$$

where the $\chi_{s,j}$ are either trivial characters or have order dividing some m so that the residue field $k_\mathfrak{p}$ satisfies $|k_\mathfrak{p}| \equiv 1 \mod m$, the χ_{q_s} are primitive characters of order q_s and ψ is some $\overline{\mathbb{F}}_\ell$-representation of $I_\mathfrak{p}$. When it is necessary to be explicit about m, we will say the $\mathfrak{p}$-system is *twisted by* m.

If furthermore, the subvector space of V corresponding to $\bigoplus_{j=1}^{q_s-1} \chi_{s,j} \otimes \chi_{q_s}^{j}$ is an irreducible $D_\mathfrak{p}$ module for every s, then we say the $\mathfrak{p}$-system $(q_1, \ldots, q_t)$ is *irreducible*.

We say a $\mathfrak{p}$-system is *strict* if ψ is zero or is a direct sum of copies of the trivial representation.

If the restriction may be written in the form

$$\rho_{I_\mathfrak{p}} \cong_{\overline{\mathbb{F}}_\ell} \psi \oplus \bigoplus_{s=1}^{t} \chi_s \otimes (\overline{\mathbb{F}}_\ell[C_{q_s}] \ominus \overline{\mathbb{F}}_\ell)$$

where the χ_s are characters of order dividing m, we say the $\mathfrak{p}$-system $(q_1, \ldots, q_t)$ is *tidy*.

Remark 5.2 By definition of a $\mathfrak{p}$-system, $p \nmid \#\rho(I_\mathfrak{p})$ and thus $I_\mathfrak{p}$ acts tamely, so $\rho(I_\mathfrak{p})$ is cyclic.

Remark 5.3 Suppose $f \in \mathbb{Q}(\zeta_r)[x]$ has $\mathfrak{p}$-degree $(q_1, \ldots, q_t)$ and $\mathfrak{p}$ is a prime of potentially good reduction for the jacobian $J/\mathbb{Q}(\zeta_r)$ of the superelliptic curve $y^r = f(x)$. Then the representation $\rho_\lambda \colon G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}\,(J[\lambda])$ has $\mathfrak{p}$-system $(q_1, \ldots, q_t)$ twisted by r. Indeed by Corollary 4.5, the only condition to check is that $|k_\mathfrak{p}| \equiv 1 \mod r$ (the D_s in the statement of Corollary 4.5 is always one by definition of such polynomials). This condition is implied by the well-known result that the inertia degree of $\mathfrak{p}$ over p is equal to the order of p modulo r.

Remark 5.4 Let f and $\mathfrak{p}$ be as in the previous remark. If f has $\mathfrak{p}$-degree q $(\neq r)$ and height h coprime to q, then by Example 4.11 the $\mathfrak{p}$-system associated to ρ_λ is strict and twisted by r.

Likewise, if $r \mid \deg f = q_1 + q_2$ where q_1, q_2 $(\neq r)$ are prime and f has $\mathfrak{p}$-degree (q_1, q_2), then by Example 4.13 the $\mathfrak{p}$-system associated to ρ_λ is strict.

5.1 Irreducibility

In this subsection we relate the decomposition of $V_{D_\mathfrak{p}}$ into irreducible subspaces to their corresponding $\mathfrak{p}$-systems. We then use this to give a criterion for irreducibility and will use it also in the next subsection to help prove results about primitivity.

Recall that if $I \lhd D$ are finite groups and V is a D-module, and $W \subseteq V_I$ is an I-submodule, then φW, where $\varphi \in D$, is also an I-submodule. Moreover, if χ is the character corresponding to W, then the character corresponding to φW is ${}^\varphi\chi$, where ${}^\varphi\chi(\tau) := \chi(\varphi^{-1}\tau\varphi)$ for $\tau \in I$.

Proposition 5.5 *Suppose $\rho \colon G_K \to GL(V)$ has a $\mathfrak{p}$-system $(q_1, \ldots, q_t)$ and the size of the residue field $|k_\mathfrak{p}|$ is a primitive root modulo each q_s.*

Then the $\mathfrak{p}$-system is irreducible and tidy. In particular, the socle of V, when viewed as a $D_\mathfrak{p}$-module, contains $\bigoplus_s W_s$, where each W_s is an irreducible $D_\mathfrak{p}$-module of dimension $q_s - 1$.

Proof By assumption the inertia group $I_\mathfrak{p}$ acts tamely and so $\rho(I_\mathfrak{p})$ is cyclic. It follows that the action of $D_\mathfrak{p}$ factors through the finite group $D = \rho(D_\mathfrak{p}) = \langle \tau, \varphi \rangle$, where $\rho(I_\mathfrak{p}) = \langle \tau \rangle \lhd D$ is the inertia subgroup and φ is a lift of Frobenius.

Let $\chi_{s,j} \otimes \chi_{q_s}^j$ be one of the characters appearing in $\rho_{I_\mathfrak{p}}$. Using that $\varphi\tau\varphi^{-1} = \tau^{|k_\mathfrak{p}|}$ [26, 7.5.3], we have

$${}^{\varphi^{-1}}\left(\chi_{s,j} \otimes \chi_{q_s}^j\right) = \left(\chi_{s,j} \otimes \chi_{q_s}^j\right)^{|k_\mathfrak{p}|} = \chi_{s,j} \otimes \chi_{q_s}^{j|k_\mathfrak{p}|}.$$

Set W_s to be the orbit of $\chi_{s,j} \otimes \chi_{q_s}^j$ under D. Clearly this is an irreducible $\overline{\mathbb{F}}_\ell[D]$-submodule of V. Furthermore, its dimension is $q_s - 1$ since $|k_\mathfrak{p}|$ is a primitive root modulo q_s. Finally, as the action of D on $\chi_{s,j} \otimes \chi_{q_s}^j$ fixes $\chi_{s,j}$ the $\mathfrak{p}$-system is tidy. □

Proposition 5.6 *Suppose there are odd primes $q_1 < q_2 < q_3$ coprime to $m\ell$ such that $q_3 - 1 \leq \dim(V) = q_1 + q_2 - 2$. Suppose also there are primes $\mathfrak{p}_1, \mathfrak{p}_2$ with residue characteristics different from ℓ such that $|k_{\mathfrak{p}_1}|$ is a primitive root modulo both q_1, q_2 and $|k_{\mathfrak{p}_2}|$ is a primitive root modulo q_3.*

Suppose $\rho\colon G_K \to \mathrm{GL}(V)$ has a (strict) $\mathfrak{p}_1$-system (q_1, q_2) and a strict $\mathfrak{p}_2$-system (q_3). Then V is irreducible.

Proof Proposition 5.5 tells us the socle of $\rho_{D_{\mathfrak{p}_1}}$ contains a direct sum of irreducible submodules of dimensions $q_1 - 1$ and $q_2 - 1$. Hence either ρ is irreducible or its semisimplification is a direct sum of exactly two modules with dimensions $q_1 - 1$ and $q_2 - 1$.

Likewise the socle of $\rho_{D_{\mathfrak{p}_2}}$ contains an irreducible submodule of dimension at least $q_3 - 1$. As $q_2 - 1 < q_3 - 1$, we see V is irreducible. □

5.2 Primitivity

Recall that V denotes a finite dimensional vector space over $\overline{\mathbb{F}}_\ell$. We shall say that a group G acts imprimitively on V if it preserves a decomposition $V = \bigoplus_{j=1}^{k} V_j$ with $k > 1$ *and* permutes the subspaces V_j transitively.

In this subsection we give criteria to prove that a group does not act imprimitively. To help the reader navigate themselves through this subsection, let us explain the basic idea of how to deal with this case.

Suppose the absolute Galois group G_K of some field K acts transitively on an imprimitivity decomposition $V = \bigoplus_{j=1}^{k} V_j$, then we obtain a homomorphism $G_K \to S_k$ and thus some finite extension L/K. If $L = K$, then G_K acts trivially, but also transitively by assumption, so $k = 1$.

If K is known to have no unramified extensions, then one can achieve this by showing the action of G_K on the imprimitivity decomposition is unramified. See Lemma 5.12.

If K has unramified extensions, then in favourable circumstances, one might be able to obtain information on these unramified extensions. For example, if it has odd class number, or maybe even obtain information on a maximal unramified extension (if such an extension exists). See Lemmas 5.15 and 5.16.

On the other hand, the description of the action of the decomposition groups $D_{\mathfrak{p}}$ on V given in Proposition 5.5 can be used to gain information on the cycle types of elements in the image of $G_K \to S_k$.

Combining these two pieces of information allows one to give criteria for primitivity. See Proposition 5.13 and Theorem 5.18.

Lemma 5.7 [1, Lemma 4.15] *Let $V = \bigoplus_{j=1}^{k} V_j$ be a finite dimensional vector space over $\overline{\mathbb{F}}_\ell$. Suppose $\tau \in \mathrm{GL}(V)$ permutes the subspaces V_j cyclically. If the eigenvalues of τ^k on V_1 are $\alpha_1, \ldots, \alpha_d$ (with multiplicity), then the eigenvalues of τ on V (with multiplicity) are*

$$\zeta_k^s \alpha_t^{1/k}$$

for $t = 1, \ldots, d$ and $s = 0, \ldots, k-1$.

In particular, if τ has order k, then each k-th root of 1 is an eigenvalue of τ and has multiplicity $d = \dim V_j$.

Lemma 5.8 *Let $V = \bigoplus_{j=1}^{k} V_j$, $k > 1$ be a finite dimensional vector space over $\overline{\mathbb{F}}_\ell$. Suppose $\tau \in \mathrm{GL}(V)$ satisfies $(\tau - 1)^2 = 0$ and preserves the above decomposition. If τ does not fix the subspaces V_j, then $\ell = 2$.*

In particular, if $G \leq \mathrm{GL}(V)$ *both preserves an imprimitivity decomposition* $V = \bigoplus_{j=1}^{k} V_j$ *with* $\dim V_j = 1$ *and contains a non-identity element* τ *satisfying* $(\tau-1)^2 = 0$, *then* $\ell = 2$.

Proof The first assertion is [1, Lemma 4.16]. We now prove the second. All the eigenvalues of an element $\tau \in \mathrm{GL}(V)$ satisfying $(\tau-1)^2 = 0$ are equal to 1, thus if τ were to fix the V_j, then τ would be the identity element. Applying the first assertion now proves the result. □

Corollary 5.9 *Suppose* $\rho\colon G_K \to GL(V)$ *be a representation whose image preserves an imprimitivity decomposition* $V = \bigoplus_{j=1}^{k} V_j$.

Suppose $\rho(I_{\mathfrak{p}})$ *is generated by an element which has at most* $2r-1$ *non-trivial eigenvalues all being* r*-th roots of unity, and whose* r*-th power is a transvection. Then* $\rho(I_{\mathfrak{p}})$ *fixes each* V_j.

Proof Let τ be a generator of $\rho(I_{\mathfrak{p}})$. By the preceding lemma τ^r fixes each V_j. As τ has at most $2r-1$ non-trivial eigenvalues, Lemma 5.7 implies that either τ fixes each V_j or each V_j has dimension one. The latter possibility is ruled out by Lemma 5.8. □

Proposition 5.10 *Suppose* $\ell > 2$. *Let* $\rho\colon G_K \to GL(V)$ *be a representation whose image both preserves an imprimitivity decomposition* $V = \bigoplus_{j=1}^{k} V_j$ *and contains a transvection. Let* $q_1, \ldots, q_t$ *be distinct primes different from* ℓ *and coprime to* m.

Suppose ρ *has a strict* $\mathfrak{p}$*-system* $(q_1, \ldots, q_t)$ *twisted by* m. *Then* $\rho(I_{\mathfrak{p}})$ *fixes each* V_j.

Proof Let τ be a generator of $\rho(I_{\mathfrak{p}})$. As m is coprime to $q_1, \ldots, q_s$ which are distinct, no subset of the eigenvalues of τ is fixed by multiplication by a non-trivial m-th root of 1. Thus by Lemma 5.7 there are no cycles of length dividing m in the action of τ on $\{V_1, \ldots, V_k\}$.

For ease, we may now suppose each χ_s is trivial. All non-trivial eigenvalues of τ have prime order and multiplicity 1, thus if τ does not fix the V_j then by Lemma 5.7 the dimension of each V_j is one (take all $\alpha_t = 1$). But this possibility is ruled out by Lemma 5.8. □

Recall that we write $n = \frac{2g}{r-1}$ where g is the dimension of our jacobian $J/\mathbb{Q}(\zeta_r)$. We also only require $n \geq 10$ for our main results, but everything in this section holds for $n \geq 3$.

Proposition 5.11 *Let* $\lambda|\ell \neq r$ *be a prime of semistable reduction for* $J/\mathbb{Q}(\zeta_r)$, *with* $\ell > \max(\frac{n}{2}, 3)$.

Let λ' *be some Galois conjugate of* λ. *If* $\rho_\lambda\colon G_{\mathbb{Q}(\zeta_r)} \to Aut(J[\lambda])$ *preserves an imprimitivity decomposition* $J[\lambda] = \bigoplus_{j=1}^{k} V_j$ *and contains a transvection, then* $\rho_\lambda(I_{\lambda'})$ *fixes each* V_j.

Proof As $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ contains a transvection and $\ell > 2$, there are at most $\frac{n}{2}$ subspaces in the imprimitivity decomposition. We may view $J[\lambda] \subseteq J[\ell]$ as an $\mathbb{F}_\ell$-vector space. The imprimitivity decomposition $V_1, \ldots, V_k$ of $J[\lambda]$ (viewed with the structure of an $\mathbb{F}_{\ell^i}$-vector space) induces an imprimitivity decomposition $W_1, \ldots, W_k$ of $J[\lambda]$ as an $\mathbb{F}_\ell$-vector space. It therefore suffices to show $I_{\lambda'}$ fixes each W_j. The argument used in [1, Prop.4.12] now carries over verbatim to achieve this. □

Let G be a group acting on a vector space V. Suppose G preserves an imprimitivity decomposition $V = \bigoplus_{j=1}^{k} V_j$. This corresponds to an action of G on the set $\{V_1, \ldots, V_k\}$, which in turn gives us a natural homomorphism $G \to S_k$.

Lemma 5.12 *Let $\ell > \max(\frac{n}{2}, 3)$ be a prime of semistable reduction for $J/\mathbb{Q}(\zeta_r)$.*

Suppose $\rho_\lambda : G_{\mathbb{Q}(\zeta_r)} \to Aut(J[\lambda])$ preserves an imprimitivity decomposition $V = \bigoplus_{j=1}^k V_j$, its image contains a transvection, and for any place $\mathfrak{p}$ of residue characteristic different to ℓ either $J/\mathbb{Q}(\zeta_r)$ is semistable at $\mathfrak{p}$, ρ_λ has a strict $\mathfrak{p}$-system, or $\rho_\lambda(I_\mathfrak{p})$ is as in Corollary 5.9. Then the induced homomorphism $\theta : G_{\mathbb{Q}(\zeta_r)} \to S_k$ is unramified.

In particular, if $\mathbb{Q}(\zeta_r)$ has no unramified extensions contained in $\mathbb{Q}(\zeta_r)(J[\lambda])$, then $k = 1$.

Proof It suffices to show $\rho_\lambda(I_v)$ fixes each V_j for each place v of $\mathbb{Q}(\zeta_r)$. For $v|l$, this is achieved by Proposition 5.11. If v is a place of semistable reduction for $J/\mathbb{Q}(\zeta_r)$, then Grothendieck's semistable reduction theorem implies that for any $\tau \in \rho(I_v)$, we have $(\tau - 1)^2 = 1$ [14, Proposition 3.5] [4, Page 184, Thm 6]. By Lemma 5.8, such a τ stabilises each V_j. Finally, if ρ_λ has a strict v-system (or $\rho_\lambda(I_v)$ is as in Corollary 5.9), then by Proposition 5.10 (resp. Corollary 5.9), $\rho_\lambda(I_v)$ preserves each V_j. □

Proposition 5.13 *Let K be a field with odd class number. Suppose $\rho : G_K \to GL(V)$ preserves an imprimitivity decomposition $V = \bigoplus_{j=1}^k V_j$ and the induced homomorphism $\theta : G_K \to S_k$ is unramified. The following hold:*

1. *If ρ has an irreducible $\mathfrak{p}$-system (q_1, q_2) where $q_1 + q_2 - 2 = \dim V$, then either k is even or $k = 1$.*
2. *If ρ has an irreducible $\mathfrak{p}$-system (q) where $q - 1 = \dim V$, then k is odd.*

In particular if ρ has an irreducible $\mathfrak{p}_1$-system (q_1, q_2) and an irreducible $\mathfrak{p}_2$-system (q_3) where $q_1 + q_2 - 2 = q_3 - 1 = \dim V$, then $k = 1$.

Proof The action of $D_{\mathfrak{p}_s}$ factors through the finite group $D_s = \rho(D_{\mathfrak{p}_s}) = \langle \tau_s, \varphi_s \rangle$, where $I_s = \rho(I_{\mathfrak{p}_s}) = \langle \tau_s \rangle \lhd D_s$ is the inertia subgroup and φ_s is a lift of Frobenius. Let σ_s be the image of a Frobenius element at $\mathfrak{p}_s$ under θ.

We first prove 1. Let us assume $k > 1$. By assumption V is the sum of two irreducible $\overline{\mathbb{F}}_\ell[D_1]$-modules. As I_1 fixes each V_j and there are exactly two irreducible D_1-submodules, φ_1 has exactly two orbits on the V_j. This implies σ_1 is product of two cycles, the sum of whose lengths is k. If k is odd, then exactly one of these cycles has even length. This implies σ_1 is an odd permutation, and so the image of θ does not land in A_k. This gives rise to an unramified degree 2 extension of K, contrary to assumption.

We now prove 2. As I_2 fixes each V_j, and V is an irreducible $\overline{\mathbb{F}}_\ell[D_2]$-module, φ_2 must permute the V_j transitively. Consequently the permutation σ_2 is a k-cycle. In particular σ_2 is an odd permutation if k is even. This again gives us an unramified degree 2 extension of K contrary to assumption. □

Lemma 5.14 *Suppose $\rho : G_K \to GL(V)$ preserves an imprimitivity decomposition $V = \bigoplus_{j=1}^k V_j$ and has an irreducible $\mathfrak{p}$-system (q), where $q - 1 > \frac{1}{2} \dim V$.*

Suppose the induced homomorphism $\theta : G_K \to S_k$ is unramified and let σ be the image of a Frobenius element at $\mathfrak{p}$. Let L/K be the extension cut out by θ.

The following hold:

- *if σ has order 2, then $k = 2$ or 3 and K has an unramified (Galois) extension of degree 2 inert at $\mathfrak{p}$;*
- *if σ has order 3, L/K is soluble and K has odd class number then $k = 3$ or 4 and K has an unramified Galois extension of degree 3 inert at $\mathfrak{p}$.*

Proof By assumption V is an $\overline{\mathbb{F}}_\ell[D_\mathfrak{p}]$-module with an irreducible submodule of dimension $q - 1$. Moreover, the action of $D_\mathfrak{p}$ factors through the finite group $D = \rho(D_\mathfrak{p}) = \langle \tau, \varphi \rangle$,

where $\rho(I_\mathfrak{p}) = \langle\tau\rangle \lhd D$ is the inertia subgroup and φ is a lift of Frobenius. Let $a \in \{2, 3\}$ denote the order of σ.

As the orbits of the V_j under φ are D-modules, one of these orbits must contain the forementioned irreducible module of dimension $q - 1 > \frac{1}{2}\dim V$. Since the V_j have equal dimension, σ has a cycle of length greater than $k/2$. Having prime order, the cycles in the decomposition of σ all have the same length. This implies σ is an a-cycle and $k < 2a$.

In the case $a = 2$, we see $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of S_3. As S_3 has a normal subgroup of order 3 with quotient isomorphic to C_2, the statement follows for $a = 2$.

Suppose we are in the second case, i.e., $a = 3$. As L/K is a soluble extension and 2 does not divide the class number of K, we may rule out $k = 5$ since A_5 does not have a proper subgroup which is both transitive on 5 points and contains an element of order 3. We deduce $k = 3$ or 4 and $\mathrm{Gal}(L/K)$ is isomorphic to a subgroup of A_4 (again using K has odd class number). As A_4 has a normal subgroup of order 4 with quotient isomorphic to C_3, the final statement follows. □

Lemma 5.15 *Let $L/\mathbb{Q}(\zeta_{23})$ be a non-trivial unramified Galois extension. Then either* $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{23})) \cong C_3$ *or* A_4.

Proof The root discriminant of $\mathbb{Q}(\zeta_{23})$ is equal to 19.94 to two decimal places. As $L/\mathbb{Q}(\zeta_{23})$ is an unramified extension, it has equal root discriminant to $\mathbb{Q}(\zeta_{23})$ [38, Lemma 11.22]. Table 1 in [9] shows any totally imaginary number field of absolute degree greater than or equal $462 = 21 \times 22$ has root discriminant at least 19.98. This shows us such an L satisfies $[L : \mathbb{Q}(\zeta_{23})] < 21$.

The class number of $\mathbb{Q}(\zeta_{23})$ is 3 [38, Tables, Sect. 3]. Thus any abelian quotient of $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{23}))$ must have order dividing 3. This with the above bound implies $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{23})) \cong C_3$ or A_4. □

Lemma 5.16 *Let $L/\mathbb{Q}(\zeta_{31})$ be a non-trivial unramified Galois extension. Then assuming GRH either* $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{31})) \cong C_3$, $C_3 \times C_3$, *or* C_9.

Proof The root discriminant of $\mathbb{Q}(\zeta_{31})$ is equal to 27.65 to two decimal places. As $L/\mathbb{Q}(\zeta_{31})$ is an unramified extension, it has equal root discriminant to $\mathbb{Q}(\zeta_{31})$ [38, Lemma 11.22]. The bounds given in Table 1 of [27] show, upon assumption of GRH, any totally imaginary number field of absolute degree greater than or equal $720 = 24 \times 30$ has root discriminant at least 27.98. This shows us such an L satisfies $[L : \mathbb{Q}(\zeta_{31})] < 24$.

The class number of $\mathbb{Q}(\zeta_{31})$ is 9 [38, Tables, Sect. 3]. Thus any abelian quotient of $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{31}))$ must have order dividing 9. This with the above bound implies $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{31})) \cong C_3$, $C_3 \times C_3$, C_9, A_4 or $C_7 \rtimes C_3$.

The compositum of two unramified Galois extensions is an unramified Galois extension. Thus if $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{31})) \cong A_4$ (resp. $C_7 \rtimes C_3$) then there would be an unramified Galois extension of $\mathbb{Q}(\zeta_{31})$ of degree 36 (resp. 63). But these contradict the above bound. We deduce $\mathrm{Gal}(L/\mathbb{Q}(\zeta_{31})) \cong C_3$, $C_3 \times C_3$, or C_9. □

The following lemma shows we may always find a prime q fulfilling the hypothesis of Theorem 5.18.

Lemma 5.17 *For $m \geq 6$ there is a prime $m + 1 < q < 2m$ congruent to 2 modulo 3.*

Proof For $m \geq 21$ this follows from section 4 of [22]. The remaining values of m can easily be checked by hand. □

Theorem 5.18 *Let $r \in \{23, 31\}$. If $r = 31$ assume GRH. Suppose $\rho\colon G_K \to GL(V)$ preserves an imprimitivity decomposition $V = \bigoplus_{j=1}^{k} V_j$ and the induced homomorphism $\theta\colon G_{\mathbb{Q}(\zeta_r)} \to S_k$ is unramified. Let $L/\mathbb{Q}(\zeta_r)$ be the extension cut out by θ.*

Let p, q be primes distinct from r and ℓ, with $|k_{\mathfrak{p}}|$ a primitive root modulo q. If ρ has a $\mathfrak{p}$-system (q), where $q - 1 > \frac{1}{2}\dim V$ and $q \equiv 2 \mod 3$, then $k = 1$.

Proof If $L = \mathbb{Q}(\zeta_r)$, then we are done, so suppose not. By Proposition 5.5, the $\mathfrak{p}$-system (q) is irreducible, and in particular, V has an irreducible $D = \rho(D_{\mathfrak{p}})$ submodule of dimension $q - 1 > \frac{1}{2}\dim V$.

By Lemmas 5.15 and 5.16, either $\mathrm{Gal}(L/\mathbb{Q}(\zeta_r)) \cong C_3, C_3 \times C_3, C_9$ or A_4. It follows from Lemma 5.14 that σ, the image of the Frobenius element at $\mathfrak{p}$, has order dividing 9. Furthermore, if σ has order 3 then $k = 3$ or 4, and if σ has order 9 then $\mathrm{Gal}(L/\mathbb{Q}(\zeta_r)) \cong C_9$ giving $k = 9$ since $\mathrm{Gal}(L/\mathbb{Q}(\zeta_r))$ acts transitively.

Let us rule out the case where σ is trivial. Here, every V_j is a D-module, and some V_j must have an irreducible constituent of dimension at least $q - 1$, forcing $k = 1$. Hence we may suppose the order of σ is 3 or 9.

Let $\varphi \in D$ be a lift of Frobenius and τ be a generator of the tame inertia group $\rho(I_{\mathfrak{p}})$, so that $D = \langle \tau, \varphi \rangle$. Let $U_1, \ldots, U_t$ be the orbits of φ^3 on the V_j. Then each U_j is a $\langle \tau, \varphi^3 \rangle$-module, and as 3 divides the order of σ, either $t = 3$ or 4 by the above. The dimension of each U_j is less than or equal to $\frac{1}{3}\dim V$. We deduce $|k_{\mathfrak{p}}|^3$ is not a primitive root modulo q, else following the proof of Proposition 5.5, we would be able to produce an irreducible $\langle \tau, \varphi^3 \rangle$-submodule of V with dimension $q - 1 > \frac{1}{2}\dim V$. It follows that the cubing map does not induce an automorphism on $(\mathbb{Z}/q\mathbb{Z})^*$. Thus $q \equiv 1 \mod 3$, completing the proof. □

5.3 Subfield subgroups and classical subgroups

The following lemma will come in handy when ruling out the possible containment of $G_\lambda = \rho_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})})$ in certain maximal subgroups.

We note the only importance of the conditions of this lemma is that there exists an element in G_λ which has exactly one eigenvalue of order $2r$ and the rest equal to 1.

Lemma 5.19 *Suppose $f(x) \in \mathbb{Q}(\zeta_r)[x]$ has $\mathfrak{p}$-degree 2 for some prime $\mathfrak{p}$ with residue characteristic distinct from r, ℓ. Then*

- *the image of* $\det\colon G_\lambda \to \mathbb{F}_{\ell^i}^*$ *is not contained in a proper subfield of $\mathbb{F}_{\ell^i}$;*
- *G_λ is not contained in a subfield subgroup;*
- *G_λ does not preserve a symplectic pairing up to scalars.*

Proof By Example 4.11, $I_{\mathfrak{p}}$ acts tamely on $J[\lambda]$ and furthermore,

$$(\rho_\lambda)_{I_{\mathfrak{p}}} = (\varepsilon \otimes \chi_r) \oplus \mathbb{F}_{\ell^i}^{\oplus n-1}$$

where ε, χ_r are characters of orders 2 and r respectively. Note also that as $p \neq r, \ell$ we have the containment $\rho_\lambda(I_{\mathfrak{p}}) \leq G_\lambda$.

Let τ be a generator of $\rho_\lambda(I_{\mathfrak{p}})$. Then $\det(\tau^2) = \chi_r(\tau^2)$ which is a primitive r-th root. But $\mathbb{F}_{\ell^i}$ is the smallest extension of $\mathbb{F}_\ell$ containing a primitive r-th root, whence the first statement. As τ^2 is not a scalar, the second statement follows.

We now show the third statement. Suppose τ^r is similar to an element of $\mathrm{GSp}_n(\mathbb{F}_{\ell^i})$. As the similitude character $\chi_\sharp\colon \mathrm{GSp}_n(\mathbb{F}_{\ell^i}) \to \mathbb{F}_{\ell^i}^*$ is a homomorphism and τ^r has order two,

we find $\chi_\sharp(\tau^r) = \pm 1$. Using [18, Lemma 2.4.5], we evaluate $\chi_\sharp(\tau^r)^{n/2} = \det(\tau^r) = -1$. Thus $\chi_\sharp(\tau^r) = -1$.

The only eigenvalues of τ^r are plus and minus one, thus Lemma 3.4 combined with $\chi_\sharp(\tau^r) = -1$ implies they are equal in number. Since $n > 2$, this contradicts the description of $(\rho_\lambda)_{I_\mathfrak{p}}$ given above. □

6 The endomorphism character

6.1 Algebraic Hecke characters

Here we collect a few facts about algebraic Hecke characters which we shall need later in this section. Everything in this subsection is well-known and one may consult [29], [8], or [30] for more details. The reader should, however, be aware that none of these references contain all the details we require and the conventions and (mathematical) language changes in each of them.

Let E be a number field and fix an algebraic closure $\bar{E}$. Let K be a number field in $\bar{E}$ containing all conjugates of E. Let $\lambda|\ell$ be a prime above ℓ in E. Choose a valuation v_λ of $\bar{E}$ which extends the λ-adic valuation of E. The completion $\bar{E}_\lambda$ of $\bar{E}$ with respect to v_λ is then an algebraic closure of E_λ. Let k_λ denote the residue field of $\bar{E}_\lambda$.

Let Γ denote the set of embeddings $K \hookrightarrow \bar{E}$. Every element σ of Γ extends by linearity to a homomorphism $K_\ell^* = (K \otimes \mathbb{Q}_\ell)^* \to \bar{E}_\lambda$, by abuse of notation we denote this homomorphism again by σ. This extension is trivial on all but one of the K_v^*'s in the decomposition $K_\ell^* = \prod_{v|l} K_v^*$, to be precise, the one corresponding to $v_\lambda \circ \sigma$. We denote by $\Gamma(v)$ the elements $\sigma \in \Gamma$ such that $v_\lambda \circ \sigma$ is equivalent to v. By the above we have for any embedding $\sigma \in \Gamma(v)$ a canonical embedding $\sigma_v \colon K_v^* \hookrightarrow \bar{E}_\lambda$.

We write $\mathbb{A}_K^\times$ for the ideles of K and identify K^* with its diagonal embedding in $\mathbb{A}_K^\times$ and likewise K_ℓ^* with its image in $\mathbb{A}_K^\times$.

A Hecke character with values in E is a continuous homomorphism $\chi : \mathbb{A}_K^\times \to E^*$ trivial on K^*. All such characters may be written as $\chi = \chi^\infty \chi_\infty^{-1}$, a product of its restriction to the finite places $\chi^\infty \colon \prod_{v\nmid\infty} K_v^* \to E^*$ and its restriction to the infinite places $\chi_\infty^{-1} \colon K_\infty^* = \prod_{v|\infty} K_v^* \to E^*$.

An algebraic Hecke character with values in E is a Hecke character χ taking values in E such that the restriction of χ to $K_\infty^{*,0}$, the connected component of 1 in K_∞^*, is given by an algebraic homomorphism. That is, there exists $T = \sum_{\sigma\in\Gamma} n_\sigma \sigma$ such that $\chi_\infty = T$ on $K_\infty^{*,0}$. We call $\sum_\sigma n_\sigma \sigma$ the *infinity type* of χ.

Let us now construct the λ-adic avatar of χ. Let $\alpha \in \mathbb{A}_K^\times$, write α_∞ for the components of α in K_∞^*. Define $\tilde{\chi} : \mathbb{A}_K^\times \to E^*$ by $\tilde{\chi}(\alpha) = \chi(\alpha) T(\alpha_\infty)$. Note $\tilde{\chi}|_{K^*} = T$ since $\chi|_{K^*}$ is trivial. As elements of Γ may be extended to homomorphisms $K_\ell^* \to \bar{E}_\lambda^*$, the infinity type T may also be extended to a homomorphism $T_\lambda \colon K_\ell^* = (K \otimes \mathbb{Q}_\ell)^* \to E_\lambda^*$. Let $\alpha_\ell = (\alpha_v)_{v|\ell} \in K_\ell^* = \prod_{v|\ell} K_v^*$. The character $\chi_\lambda \colon \mathbb{A}_K^\times \to E_\lambda^*$ defined by

$$\chi_\lambda(\alpha) = \tilde{\chi}(\alpha) T_\lambda(\alpha_\ell^{-1})$$

is continuous and trivial on K^* (here we view $\tilde{\chi}(\alpha) \in E^* \hookrightarrow E_\lambda^*$ under the obvious embedding). We call χ_λ the λ-*adic avatar* of χ.

Clearly, χ_λ may be viewed as a character on $C_K = \mathbb{A}_K^\times / K^*$, the idele class group of K, furthermore as E_λ is totally disconnected, the connected component C_K^0 of C_K is sent to 1 under χ_λ. Class field theory allows us to view χ_λ as a homomorphism $G_K^{ab} \cong C_K / C_K^0 \to E_\lambda^*$

via the Artin map. In particular for all but finitely many $\mathfrak{p}$, the image of the arithmetic Frobenius is $\chi_\lambda(\mathrm{Frob}_\mathfrak{p}) = \tilde{\chi}(\pi_\mathfrak{p})T_\lambda(1) = \chi(\pi_\mathfrak{p})$, where $\pi_\mathfrak{p} \in \mathbb{A}_K^\times$ is a uniformiser at $\mathfrak{p}$ and 1 in every other component (here equality is viewed under the embedding $E^* \hookrightarrow E_\lambda^*$).

The profinite completion $\hat{\mathcal{O}}_K$ of $\mathcal{O}_K$, the ring of integers of K, may be decomposed as a product $\prod_{v\nmid\infty} \mathcal{O}_v$, where $\mathcal{O}_v$ is the subring of elements in K_v having non-negative valuation. Owing to the fact that χ is continuous and $\hat{\mathcal{O}}_K^* \subseteq \mathbb{A}_K^\times$ is profinite, $\chi(\mathcal{O}_v^*) = 1$ for all but finitely many v. When $\chi(\mathcal{O}_v^*) \neq 1$, there is some subgroup $1 + \mathfrak{p}_v^{m_v} \subseteq \mathcal{O}_v^*$ whose image under χ is trivial. We say χ is unramified at v if $\chi(\mathcal{O}_v^*) = 1$, and ramified otherwise. Let $\mathfrak{m} = \prod \mathfrak{p}_v^{m_v}$ where the product is taken over the ramified primes of χ.

For $\mathfrak{p} \nmid \mathfrak{m}$ define $\chi(\mathfrak{p}) = \chi(\pi_\mathfrak{p})$, where $\pi_\mathfrak{p} \in \mathbb{A}_K^\times$ is a uniformiser at $\mathfrak{p}$ and 1's elsewhere. Note this is independent of the choice of uniformiser as χ is unramified at $\mathfrak{p}$. This allows us to extend χ^∞ to a group homomorphism from ideals of K coprime to $\mathfrak{m}$ to $\bar{\mathbb{Q}}^*$. Let (α) be an ideal of K coprime to $\mathfrak{m}$, and suppose α is totally positive, then

$$\chi^\infty((\alpha)) = \chi_\infty(\alpha) = T(\alpha) = \prod_\sigma \sigma(\alpha)^{n_\sigma}$$

as χ is trivial on K^* and $\alpha_\infty \in K_\infty^{*,0}$. We may extend T to a map of ideals satisfying

$$(\chi(\mathfrak{p})) = T(\mathfrak{p}).$$

The above relation gives us a method to determine T, the infinity type of χ, by factorising $(\chi(\mathfrak{p}))$.

In the introduction we briefly mentioned that knowledge of the infinity type helps determine the mod ℓ image of Galois. Let us indicate how here. Continue to let $\mathfrak{m}$ be as above. We define U_v as the connected component of K_v^* if $v|\infty$, and otherwise as $\mathcal{O}_v^*$ if $v \nmid \mathfrak{m}$ and the subgroup $1 + \mathfrak{p}_v^{m_v} \subseteq \mathcal{O}_v^*$ if $v|\mathfrak{m}$. Finally, we write $U_\mathfrak{m} = \prod_v U_v$. By construction of $U_\mathfrak{m}$, we have $\tilde{\chi}(\alpha) = 1$ for all $\alpha \in U_\mathfrak{m}$, which leads to the equality

$$\chi_\lambda(\alpha) = T_\lambda(\alpha_\ell^{-1}) = \prod_\sigma \sigma_v(\alpha_\ell^{-1})^{n_\sigma} \quad \text{for } \alpha \in U_\mathfrak{m}.$$

The image of χ_λ is compact, and thus lands in $\mathcal{O}_{E_\lambda}^*$, the maximal compact subgroup of E_λ^*. This allows to reduce modulo λ. Local Class Field Theory associates $\mathcal{O}_v^*$ to the inertia group of the maximal abelian extension of K_v^* and $1 + \mathfrak{p}_v$ to its wild inertia subgroup. The multiplicative subgroup k_v^* of the residue field of K_v thus corresponds to the tame inertia group. Passing to the residue field, the $\sigma \in \Gamma(v)$ induce embeddings $k_v \to k_\lambda$, which we denote by $\bar{\sigma}$. For $v \nmid \mathfrak{m}$, the above provides us with following description of $\bar{\chi}_\lambda$ on the inertia groups

$$\bar{\chi}_\lambda(\alpha) = \begin{cases} 1 & \text{for } \alpha \in U_v,\ v \nmid \ell, \\ \prod_{\sigma\in\Gamma(v)} \bar{\sigma}(\bar{\alpha}_\ell^{-1})^{n_\sigma} & \text{for } \alpha \in U_v,\ v|\ell \end{cases}$$

where $\bar{\alpha}_\ell$ denotes the reduction of α_ℓ modulo $\mathfrak{p}_v$.

Using Class Field Theory, the characters $\bar{\alpha}_\ell \mapsto \bar{\sigma}(\bar{\alpha}_\ell^{-1})$ may be viewed as characters on the inertia group I_v. From this viewpoint they turn out to be fundamental characters of level $[k_v : \mathbb{F}_\ell]$, see [30, Prop 3].

One may rewrite the above equation by letting $\theta(\bar{\alpha}_\ell) = \bar{\sigma}(\bar{\alpha}_\ell^{-1})$ for some $\sigma \in \Gamma(v)$ and then for any $\tau \in \Gamma(v)$ writing

$$\theta(\bar{\alpha}_\ell)^{\ell^{m_\tau}} = \bar{\tau}(\bar{\alpha}_\ell^{-1})$$

for some appropriate integer m_τ. This provides us with the following description (for $v \nmid \mathfrak{m}$):

$$\bar{\chi}_\lambda(\alpha) = \begin{cases} 1 & \text{for } \alpha \in U_v,\ v \nmid \ell, \\ \prod_{\sigma \in \Gamma(v)} \theta(\bar{\alpha}_\ell)^{n_\sigma \ell^{m_\sigma}} & \text{for } \alpha \in U_v,\ v|\ell \end{cases} \tag{6.1}$$

where θ is some fundamental character of level $[k_v : \mathbb{F}_\ell]$.

A fundamental character of level $[k_v : \mathbb{F}_\ell]$ differs by an automorphism of k_v from any other fundamental character of the same level. As all the automorphisms of k_v are given by raising its elements to some power of p, we see that the image of U_v is independent of θ.

6.2 The endomorphism character

In this subsection let us consider a g-dimensional abelian variety A/K. Suppose we have an embedding $E \hookrightarrow \mathrm{End}_K^0(A)$. Then, as in Sect. 2, we may attach a system of λ-adic representations to A. These representations form a strictly compatible system (ρ_λ) with exceptional set S equal to the set of places of K where A has bad reduction, see Section II of [28] for more details.

As explained in Sect. 2, taking the determinant of these representations leads to the existence of an algebraic Hecke character Ω such that $\Omega_\lambda = \det \circ \rho_{\lambda^\infty}$ for each λ. We call Ω the *endomorphism character*.

Fité has recently determined the infinity types of the Ω_λ up to a suitable equivalence when K/E and $E/\mathbb{Q}$ are Galois extensions, that is, viewing Ω_λ as a map on ideals, he determines the integers n_σ appearing in the factorisation

$$\Omega_\lambda((\alpha)) = \prod_{\sigma : K \hookrightarrow \bar{E}} \sigma(\alpha)^{n_\sigma}$$

up to a certain equivalence, where $\alpha \in K$. Note that for this product to belong to E, we must be able to rewrite the above as

$$\Omega_\lambda((\alpha)) = \prod_{\tau : E \hookrightarrow \bar{E}} \tau(N_E^K(\alpha))^{n_\tau}$$

for some integers n_τ. We now describe the aforementioned equivalence. The Galois group $\mathrm{Gal}(E/\mathbb{Q})$ acts on the tuple $(n_\tau)_\tau$ by $h \cdot (n_\tau)_\tau = (n_{\tau \circ h^{-1}})_\tau$ for $h \in \mathrm{Gal}(E/\mathbb{Q})$. Two such tuples are then called equivalent if they belong to the same orbit under this action.

The endomorphism algebra $\mathrm{End}_K^0(A)$ acts on the regular differentials of A, and by restriction so does E. Enlarging K by a finite extension, we may assume there exists a basis $\omega_1, \ldots, \omega_g$ of $\Omega^1(A)$ satisfying

$$\alpha \cdot \omega_i = \psi_i(\alpha)\omega_i$$

for all i and $\alpha \in E$, where the ψ_i are embeddings of E into $\bar{E}$. Let m_τ denote the multiplicity of τ in $\{\psi_1, \ldots \psi_g\}$.

Theorem 6.2 [13, Prop. 14] *The tuple $(n_{\tau^{-1}})_\tau$ is equivalent to $(m_{\bar{\tau}})_\tau$ the complex conjugate of the tuple given by the action of E on $\Omega^1(A)$.*

The above coupled with the content in Sect. 6.1 provides us with valuable information about a given Ω_λ. Namely, it gives a description of the images of Frobenius elements outside the places belonging to $S \cup S_\ell$, (S_ℓ being the set of primes above ℓ in K) as well as the image of inertia at primes above ℓ, where $\lambda|\ell$. The following proposition places restrictions on $\Omega_\lambda(I_\mathfrak{p})$ for $\mathfrak{p} \in S$, $\mathfrak{p} \nmid \ell$.

Proposition 6.3 *Let $\mathfrak{p} \nmid \ell$ be a prime of $\mathcal{O}_K$. Then $\Omega_\lambda(I_\mathfrak{p})$ is contained in the subgroup of E^* generated by roots of unity. Furthermore, if $\mathfrak{p}$ is a prime of semistable reduction then $\Omega_\lambda(I_\mathfrak{p}) = 1$.*

Proof If $\mathfrak{p}$ is a prime of semistable reduction then [14, Proposition 3.5] [4, Page 184, Thm 6] implies the inertia group $I_\mathfrak{p}$ acts unipotently and therefore $\Omega_\lambda(I_\mathfrak{p}) = \det \circ \rho_{\lambda\infty}(I_\mathfrak{p}) = 1$.

By the semistable reduction theorem [14] any prime $\mathfrak{p}$ is a prime of potential semistable reduction for A/K. Let $\tau \in I_\mathfrak{p}$. Then, as A acquires semistable reduction over some finite extension, there exists $n \in \mathbb{N}$ such that $\det \circ \rho_{\lambda\infty}(\tau^n) = 1$. Since $\det \circ \rho_{\lambda\infty} : I_\mathfrak{p} \to E^*$ is a homomorphism, we obtain $\Omega_\lambda(\tau) = \det \circ \rho_{\lambda\infty}(\tau)$ is a root of unity in E. □

6.3 Image of the endomorphism character

Let us resume our study of superelliptic jacobians. We decompose

$$\Omega^1(J) = \bigoplus_{j=1}^{r-1} \Omega^1_j(J)$$

into the eigenspaces of $[\zeta_r]^*$ where we write $\Omega^1_j(J)$ for the eigenspace of ζ_r^j. In the following we write $\lfloor x \rfloor_<$ for the greatest integer strictly less than x.

Lemma 6.4 *The dimension of $\Omega^1_j(J)$ equals $\left\lfloor \frac{(r-j)d}{r} \right\rfloor_<$ where d is the degree of f.*

Proof See Remarks 4.2, 4.4 and 4.5 of [41] (note that although Zarhin works over an algebraic closure of the ground field, his calculation suffices as differentials behave well with with respect to base change [21, Lemma 5.2.26], alternatively one can work directly over the base field using Baker's Theorem, see for example [11, Theorem 2.2]). □

From the discussion in Sect. 6.2, there is a unique infinity type associated to Ω, which is determined up to equivalence by Theorem 6.2. As we are working with the λ-adic avatars of Ω, it is not important to determine the exact infinity type of Ω. Instead, for convenience we shall fix a representative of the equivalence class and by abuse of language refer to it as the infinity type of Ω. Thus, let us say

$$\sum_{j=1}^{r-1} \psi_j^{-1} \left\lfloor \frac{(r-j)d}{r} \right\rfloor_<$$

is the infinity type of Ω, where $\psi_j : \mathbb{Q}(\zeta_r) \hookrightarrow \bar{\mathbb{Q}}$ is the embedding sending ζ_r to ζ_r^j. We denote the reduction of Ω_λ modulo λ by $\bar{\Omega}_\lambda$.

Suppose Ω is unramified at the finite place v of $\mathbb{Q}(\zeta_r)$. By Proposition 6.3 this is the case if $J/\mathbb{Q}(\zeta_r)$ has semistable reduction at v. If $v \nmid \ell$, then the restriction of $\bar{\Omega}_\lambda$ to the inertia group I_v is trivial. In the case $v \mid \ell$ the infinity type describes the restriction of $\bar{\Omega}_\lambda$ to I_v, see the discussion at the end of Sect. 6.1. Let us now give this description.

Let $\psi_j : \mathbb{Q}(\zeta_r) \hookrightarrow \bar{\mathbb{Q}}$ be an embedding which sends v to λ. This embedding ψ induces a homomorphism $\theta : k_v \to k_\lambda$ which via Class Field Theory may be viewed as a fundamental character of level equal to $[k_\lambda : \mathbb{F}_\ell]$. Any embedding $\psi_j : \mathbb{Q}(\zeta_r) \hookrightarrow \bar{\mathbb{Q}}$ which sends v to λ may be written as $\psi_\ell^{m(\theta,j)} \circ \psi$ for some integer $m(\theta, j)$. The fundamental character induced

by ψ_j then equals $\theta^{\ell^{m(\theta,j)}}$. We obtain

$$\bar{\Omega}_\lambda|_{I_v} = \prod_j \theta^{\ell^{m(\theta,j)}\left\lfloor \frac{(r-j)d}{r}\right\rfloor_<}$$

where j runs over all embeddings $\psi_j : \mathbb{Q}(\zeta_r) \to \bar{\mathbb{Q}}$ which send v to λ.

Note that the choice of θ does not matter since we shall only use information about the image of I_v. Indeed, taking a different fundamental character amounts to composing θ with an automorphism of k_v, that is, raising it to a p-th power. As the image of I_v has order prime to p, this is thus also an automorphism of the image of I_v.

In the following we shall say $J/\mathbb{Q}(\zeta_r)$ has semistable reduction at the rational prime ℓ, to signify J has semistable reduction at every prime above ℓ in $\mathbb{Q}(\zeta_r)$.

Example 6.5 Let $\ell \equiv 1 \mod r$ be a prime of semistable reduction for J. Then ℓ is totally split in $\mathbb{Q}(\zeta_r)$. Let λ, λ' be primes above ℓ in $\mathbb{Q}(\zeta_r)$ and let $1 \le j \le r-1$ be such that $\psi_j(\lambda') = \lambda$. Then, as the unique fundamental character of level one is the mod ℓ cyclotomic character χ_ℓ, we have

$$\bar{\Omega}_\lambda|_{I_{\lambda'}} = \chi_\ell^{\left\lfloor \frac{(r-j)d}{r}\right\rfloor_<}.$$

Let $\ell \equiv -1 \mod r$ be a prime of good reduction. We have $[k_\lambda : \mathbb{F}_\ell] = 2$ for a prime λ above ℓ in $\mathbb{Q}(\zeta_r)$. Let λ' be a prime above ℓ in $\mathbb{Q}(\zeta_r)$ and let $1 \le j \le r-1$ be such that $\psi_j(\lambda') = \lambda$. Then

$$\bar{\Omega}_\lambda|_{I_{\lambda'}} = \theta^{\left\lfloor \frac{(r-j)d}{r}\right\rfloor_< + \ell\left\lfloor \frac{jd}{r}\right\rfloor_<}$$

where θ is some fundamental character of level 2.

Example 6.6 Let $r = 7$, and $\ell \equiv 2 \mod 7$ be a prime of semistable reduction for J. There are two primes $\lambda, \bar{\lambda}$ above ℓ in $\mathbb{Q}(\zeta_7)$. The decomposition group of each of these is given by $\{\psi_1, \psi_2, \psi_4\}$ and the map ψ_{-1} sends λ to $\bar{\lambda}$. The above description then tells us

$$\bar{\Omega}_\lambda|_{I_\lambda} = \theta^{\left\lfloor \frac{6d}{r}\right\rfloor_< + \ell\left\lfloor \frac{5d}{r}\right\rfloor_< + \ell^2\left\lfloor \frac{3d}{r}\right\rfloor_<}$$
$$\bar{\Omega}_\lambda|_{I_{\bar{\lambda}}} = (\theta')^{\left\lfloor \frac{d}{r}\right\rfloor_< + \ell\left\lfloor \frac{2d}{r}\right\rfloor_< + \ell^2\left\lfloor \frac{4d}{r}\right\rfloor_<}$$

where θ and θ' are fundamental characters of level 3.

Similarly for $\ell \equiv 4 \mod 7$, there are two primes $\lambda, \bar{\lambda}$ above ℓ in $\mathbb{Q}(\zeta_7)$ which are permuted by ψ_{-1}. Carrying out the above computation again, we find

$$\bar{\Omega}_\lambda|_{I_\lambda} = \theta^{\left\lfloor \frac{6d}{r}\right\rfloor_< + \ell\left\lfloor \frac{3d}{r}\right\rfloor_< + \ell^2\left\lfloor \frac{5d}{r}\right\rfloor_<}$$
$$\bar{\Omega}_\lambda|_{I_{\bar{\lambda}}} = (\theta')^{\left\lfloor \frac{d}{r}\right\rfloor_< + \ell\left\lfloor \frac{4d}{r}\right\rfloor_< + \ell^2\left\lfloor \frac{2d}{r}\right\rfloor_<}$$

for some fundamental characters θ, θ' of level 3.

In the following we write $m_j = \lfloor \frac{(r-j)d}{r} \rfloor_<$ and $n = \frac{2g}{r-1}$. We recall our notation $\rho_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})}) = G_\lambda$, which is viewed naturally as a subgroup of $\mathrm{GL}_n(\ell^i)$ when i the inertia degree of ℓ in $\mathbb{Q}(\zeta_r)$ is odd and as a subgroup of $\mathrm{GU}_n(\ell^{i/2})$ when i is even. The kernel of $\det_{J[\lambda]} : G_\lambda \to \mathbb{F}_{\ell^i}^*$ is denoted by S_λ. Finally, note G_λ is the kernel of the cyclotomic character on $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$.

Lemma 6.7 *Let $r = 3$. Then*

$$\det(G_\lambda) \leq \langle a^{m_1-m_2}, b\rangle$$

where b is an element of order 6, and if i is odd, a is a generator of $\mathbb{F}_\ell^*$, and if i is even then a is a generator of $(\mathbb{F}_{\ell^2}^*)^{\ell-1}$.

Proof Let $D = \langle a^{m_1-m_2}, b\rangle$. By the Chebotarev Density Theorem, it suffices to show the images of all but finitely many Frobenius elements of $G_{\mathbb{Q}(\zeta_{3\ell})}$ belong to D. Let $\mathfrak{P}$ be a prime in $\mathbb{Q}(\zeta_{3\ell})$ such that $J/\mathbb{Q}(\zeta_3)$ has semistable reduction at $\mathfrak{p}:=\mathfrak{P}\cap\mathbb{Z}[\zeta_3]$. Suppose $p \neq \ell$ is the rational prime below $\mathfrak{P}$, and let f be its order modulo ℓ. Then we have equality of Frobenius elements $\mathrm{Frob}_{\mathfrak{P}} = \mathrm{Frob}_{\mathfrak{p}}^f$.

Proposition 6.3 shows Ω_λ is unramified at $\mathfrak{p}$, so we may use the factorisation given by the infinity type, see Sect. 6.1. Furthermore, as $\mathbb{Z}[\zeta_3]$ has class number one,

$$\begin{aligned}\Omega_\lambda(\mathrm{Frob}_{\mathfrak{P}}) &= \Omega_\lambda(\mathrm{Frob}_{\mathfrak{p}})^f \\ &= (up^{m_2}\pi^{m_1-m_2})^f \text{ where } u \in \mathbb{Z}[\zeta_3]^* \text{ and } \pi \in \mathbb{Z}[\zeta_3] \\ &\equiv u^f \pi^{f(m_1-m_2)} \mod \lambda.\end{aligned}$$

As $\mathbb{Z}[\zeta_3]^* = \langle -\zeta_3\rangle$ has order 6, the result now follows when i is odd. Let us suppose i even. To finish the proof, we must show $\pi^f \mod \lambda$ belongs to $(\mathbb{F}_{\ell^2}^*)^{\ell-1}$. Note that $(\mathbb{F}_{\ell^2}^*)^{\ell-1}$ coincides with the kernel of the norm map $N_\ell^{\ell^2} : \mathbb{F}_{\ell^2}^* \to \mathbb{F}_\ell^*$. Since $N_\ell^{\ell^2}(\pi^f) = p^f \equiv 1 \mod \lambda$, the result follows. □

Remark 6.8 An easy calculation shows $m_1 - m_2 = \left\lceil \frac{g}{3} \right\rceil$.

Proposition 6.9 *Set $r = 3$. Let $\ell \equiv 1 \mod 3$ be a prime of semistable reduction for $J/\mathbb{Q}(\zeta_3)$. Then there is an element $\sigma \in G_\lambda$ such that $\det_{J[\lambda]}(\sigma) = a^{m_1-m_2}$ where $a \in \mathbb{F}_\ell^*$ is a generator.*

Furthermore, if f has $\mathfrak{p}$-degree 2, where p is a prime distinct from both 3 and ℓ then $\det(G_\lambda) = \langle a^{m_1-m_2}, b\rangle$ where b is an element of order 6.

In particular, if $S_\lambda \cong \mathrm{SL}_n(\ell)$ and f has $\mathfrak{p}$-degree 2, then

$$G_\lambda \cong \{\sigma \in \mathrm{GL}_n(\ell) | \det(\sigma) \in \langle a^{m_1-m_2}, b\rangle\}.$$

Proof To prove the first statement, we look for an element of $G_{\mathbb{Q}(\zeta_3)}$ whose image under χ_ℓ is trivial and image by $\bar{\Omega}_\lambda$ is a generator of $\mathbb{F}_\ell^*$ taken to the power of $m_1 - m_2$.

By Example 6.5 we have for $\psi_j(\lambda') = \lambda$,

$$\bar{\Omega}_\lambda|_{I_{\lambda'}} = \chi_\ell^{m_j}.$$

Let us denote by I (resp. I') an inertia group above $\psi_j^{-1}(\lambda)$ with $j = 1$ (resp. $j = 2$). Since $\chi_\ell : I, I' \to \mathbb{F}_\ell^*$ is surjective, we may take $\tau \in I$, $\sigma \in I'$ such that $\chi_\ell(\tau) = \chi_\ell(\sigma)^{-1}$ generates $\mathbb{F}_\ell^*$. By choice of τ and σ we have $\chi_\ell(\tau\sigma) = 1$, so $\tau\sigma \in G_\lambda$. The above formula gives

$$\bar{\Omega}_\lambda(\tau\sigma) = \chi_\ell(\tau)^{m_1-m_2}.$$

If f has $\mathfrak{p}$-degree 2, then by Example 4.11, the generator of $\rho_\lambda(I_{\mathfrak{p}})$ has a unique eigenvalue of order 6, with the others being equal to one. Taking the determinant of this element gives us b.

Let us show the final statement. Let G be the group we are trying to show G_λ is isomorphic to. Corollary 6.7 gives us $G_\lambda \leq G$. The above combined with the assumption $S_\lambda \cong \mathrm{SL}_n(\ell)$ shows G_λ contains a group isomorphic to G, and thus completes the proof. □

Proposition 6.10 *Set $r = 3$. Let $\ell \equiv 2 \mod 3$ be a prime of semistable reduction for $J/\mathbb{Q}(\zeta_3)$. Then there is an element $\sigma \in G_\lambda$ such that $\det_{J[\lambda]}(\sigma) = a^{m_1-m_2}$ where $a \in (\mathbb{F}_\ell^*)^{\ell-1}$ is a generator.*

Furthermore, if f has $\mathfrak{p}$-degree 2, where p is a prime distinct from both 3 and ℓ, then $\det(G_\lambda) = \langle a^{m_1-m_2}, b\rangle$ where b is an element of order 6.

In particular, if $S_\lambda \cong \mathrm{SU}_n(\ell)$ and f has $\mathfrak{p}$-degree 2, then

$$G_\lambda \cong \{\sigma \in \mathrm{GU}_n(\ell) | \det(\sigma) \in \langle a^{m_1-m_2}, b\rangle\}.$$

Proof Recall that as the residual degree $i = 2$ we have $G_\lambda \leq \mathrm{GU}_n(\ell)$. Given $\det\colon \mathrm{GU}_n(\ell) \to (\mathbb{F}_{\ell^2}^*)^{\ell-1}$ is surjective with kernel $\mathrm{SU}_n(\ell)$, we recognise $\det(G_\lambda)$ as being contained in $\bar{\Omega}_\lambda(G_{\mathbb{Q}(\zeta_r)}) \cap \mathbb{F}_{\ell^2}^{\ell-1}$. That is, the intersection of $\bar{\Omega}_\lambda(G_{\mathbb{Q}(\zeta_r)})$ with the kernel of the norm map $N_\ell^{\ell^2}\colon \mathbb{F}_{\ell^2}^* \to \mathbb{F}_\ell^*$.

There is a unique prime λ above ℓ in $\mathbb{Q}(\zeta_3)$. Example 6.5 shows

$$\bar{\Omega}_\lambda|_{I_\lambda} = \theta^{m_2+\ell m_1}$$

for an appropriate choice of a level 2 fundamental character θ (this choice does not concern us as they differ by an automorphism of $\mathbb{F}_{\ell^2}$).

As θ surjects onto $\mathbb{F}_{\ell^2}^*$ and hence onto the kernel of the norm map, we may choose $\tau \in I_\lambda$ such that $\theta(\tau)$ generates $(\mathbb{F}_{\ell^2}^*)^{\ell-1}$. Note such a τ must further be contained in $G_{\mathbb{Q}(\zeta_{r\ell})}$ since $\chi_\ell(\tau) = N_\ell^{\ell^2} \circ \theta(\tau) = 1$. The order of $\theta(\tau)$ is $\ell + 1$ and thus $\theta(\tau)^{m_2+\ell m_1} = \theta(\tau)^{m_2-m_1}$ which establishes the first claim.

If f has $\mathfrak{p}$-degree 2, then by Example 4.11, the generator of $I_\mathfrak{p}$ has a unique eigenvalue of order 6, the others being equal to one. Taking the determinant of this element gives us b.

Let us show the final statement. Let G be the group we are trying to show G_λ is isomorphic to. Corollary 6.7 gives us $G_\lambda \leq G$. The above combined with the assumption $S_\lambda \cong \mathrm{SU}_n(\ell)$ shows G_λ contains a group isomorphic to G, and thus completes the proof. □

The above gives us information on G_λ, which is important for our study of the image of the Galois representation $\rho_\ell\colon G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}(J[\ell])$, but if we are interested in the inverse Galois problem (for the classical groups) over $\mathbb{Q}(\zeta_r)$ then we should study $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$.

For i even, there is not much to be said once G_λ is determined, indeed $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is a fixed extension of G_λ not contained in $\mathrm{GU}_n(\ell^{i/2})$. However, when i is odd $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is, like G_λ, contained in $\mathrm{GL}_n(\ell^i)$. This plays to our advantage and allows us to realise $\mathrm{GL}_n(\ell)$ when $i = 1$.

Proposition 6.11 *Suppose $2r|d$. Let $\ell \equiv 1 \mod r$ be a prime of semistable reduction for $J/\mathbb{Q}(\zeta_r)$.*

If $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ contains $\mathrm{SL}_n(\ell)$, then $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)}) = \mathrm{GL}_n(\ell)$.

Proof It suffices to show $\bar{\Omega}_\lambda\colon G_{\mathbb{Q}(\zeta_r)} \to \mathbb{F}_\ell^*$ surjects. By Example 6.5 we have for $\psi_j(\lambda') = \lambda$

$$\bar{\Omega}_\lambda|_{I_{\lambda'}} = \chi_\ell^{m_j}.$$

As the mod ℓ cyclotomic character $\chi_\ell\colon G_{\mathbb{Q}(\zeta_r)} \to \mathbb{F}_\ell^*$ surjects, it suffices to find two values j, j' such that m_j and $m_{j'}$ are coprime.

Let us write $d = 2ra$. We evaluate $m_j = 2a(r-j) - 1$. In particular, for $j = \frac{r-1}{2}$ (resp. $j = \frac{r+1}{2}$) we have $m_j = a(r-1) - 1$ (resp. $m_j = a(r+1) - 1$). Let us now compute the greatest common divisor of these two quantities:

$$\gcd(a(r-1) - 1, a(r+1) - 1) = \gcd(a(r-1) - 1, 2a) = 1.$$

This proves $\det \circ \rho_\lambda = \bar{\Omega}_\lambda : G_{\mathbb{Q}(\zeta_r)} \to \mathbb{F}_\ell^*$ is surjective and thus completes the proof. □

Despite the above, we can still realise $\Delta \mathrm{U}_n(\ell)$ as a Galois extension of $\mathbb{Q}(\zeta_r)$ for many values of $\ell \equiv -1 \mod r$.

Proposition 6.12 *Suppose $2r|d$. Let $\ell \equiv -1 \mod r$, $\ell \neq 2$ be a prime of semistable reduction for $J/\mathbb{Q}(\zeta_r)$.*

Suppose there exists some $\delta|2r$ such that $\gcd(\frac{d}{r}, \frac{\ell+1}{\delta}) = \gcd(\delta, \frac{\ell+1}{\delta}) = 1$ and f has $\mathfrak{p}$-degree 2 for some prime of $\mathbb{Q}(\zeta_r)$ with residue characteristic $p \neq r, \ell$.

If $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ contains $\mathrm{SU}_n(\ell)$, then $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)}) = \Delta \mathrm{U}_n(\ell)$.

Proof By Theorem 3.10 $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is contained in a group isomorphic to $\Delta \mathrm{U}_n(\ell)$. Thus it suffices to show $\det \circ \rho_\lambda = \bar{\Omega}_\lambda : G_{\mathbb{Q}(\zeta_r)} \to \mathbb{F}_{\ell^2}^*$ is surjective. As $N_\ell^{\ell^2} \circ \bar{\Omega}_\lambda$ coincides with the cyclotomic character, it suffices to show $\bar{\Omega}_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})}) = (\mathbb{F}_{\ell^2}^*)^{\ell-1}$.

Let $\delta|2r$ be a positive integer satisfying $\gcd(\delta, \frac{\ell+1}{\delta}) = 1$. As f has $\mathfrak{p}$-degree 2, $\bar{\Omega}_\lambda(I_\mathfrak{p}) \leq (\mathbb{F}_{\ell^2}^*)^{\ell-1}$ has order $2r$. It thus suffices to show $\bar{\Omega}_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})})$ contains an element of order $\frac{\ell+1}{\delta}$.

Let λ, λ' be primes above ℓ in $\mathbb{Q}(\zeta_r)$ be such that $\psi_j(\lambda') = \lambda$. Example 6.5 shows

$$\Omega_\lambda|_{I_{\lambda'}} = \theta^{m_j + \ell m_{r-j}}$$

for an appropriate choice of a level 2 fundamental character θ (this choice does not concern us as they differ by an automorphism of $\mathbb{F}_{\ell^2}$).

As θ surjects onto $\mathbb{F}_{\ell^2}^*$ and hence onto the kernel of the norm map, it suffices to compute $\gcd(m_j + \ell m_{r-j}, \ell + 1)$ to determine the image of $I_{\lambda'}$ under $\bar{\Omega}_\lambda$ which lands in G_λ.

Due to the congruence $m_j + \ell m_{r-j} \equiv m_j - m_{r-j} \mod \ell + 1$, we compute

$$m_j - m_{r-j} = \left\lfloor \frac{(r-j)d}{r} \right\rfloor_< - \left\lfloor \frac{jd}{r} \right\rfloor_< = \frac{d(r-2j)}{r}.$$

This shows $\frac{d}{r}$ divides $m_j - m_{r-j}$ for all values of j. In fact, for $j = \frac{r-1}{2}$, we have $m_j - m_{r-j} = \frac{d}{r}$, so this is the best contribution we will get from an inertia group at a prime above ℓ.

The above shows $\bar{\Omega}_\lambda(G_{\mathbb{Q}(\zeta_{r\ell})})$ contains $(\mathbb{F}_{\ell^2}^*)^{\frac{d}{r}(\ell-1)}$. Now let $\tau \in \mathbb{F}_{\ell^2}^{\ell-1}$ be an element of order $\frac{\ell+1}{\delta}$. By assumption $\gcd(\frac{d}{r}, \frac{\ell+1}{\delta}) = 1$ and thus τ belongs to $(\mathbb{F}_{\ell^2}^*)^{\frac{d}{r}(\ell-1)}$, completing the proof. □

7 Galois images

In this section J denotes the jacobian of a superelliptic curve determined by the affine model $y^r = f(x)$ where $f \in \mathbb{Z}[\zeta_r][x]$ is a squarefree monic polynomial of degree $d \geq 12$ divisible by $2r$. Subsequently $n = \dim_{\mathbb{F}_{\ell^i}} J[\lambda] = \frac{2g}{r-1} = d - 2$.

We recall our convention to say $J/\mathbb{Q}(\zeta_r)$ is semistable at a rational prime ℓ, if $J/\mathbb{Q}(\zeta_r)$ is semistable at every prime above ℓ in $\mathbb{Q}(\zeta_r)$. Also recall that for a prime $\mathfrak{p}_j$ of $\mathbb{Q}(\zeta_r)$, we denote the rational prime below by p_j (likewise for $\mathfrak{p}$ and p).

The results proved thus far allow us to give a few different conditions for irreducibility and primitivity. In order to state Theorem 7.1 concisely with these different conditions available, we label certain hypotheses below.

(Irred I) There exist primes $q_1 < q_2 < q_3 < d$ such that $q_1 + q_2 = d$ and there are primes $\mathfrak{p}_1, \mathfrak{p}_2$ of $\mathbb{Q}(\zeta_r)$, such that $|k_{\mathfrak{p}_1}|$ (resp. $|k_{\mathfrak{p}_2}|$) is a primitive root modulo both q_1, q_2 (resp. modulo q_3). The set $S_{irr} = \{q_1, q_2, q_3, p_1, p_2\}$ has cardinality 5.

(Irred II) The number $d-1=q$ is prime and there is a prime $\mathfrak{p}$ of $\mathbb{Q}(\zeta_r)$, such that $|k_{\mathfrak{p}}|$ is a primitive root modulo q. Let $S_{irr}=\{q,p\}$.

(Prim I) Either $3\leq r\leq 23$ is prime or $r=31$. If $r=31$, assume GRH. If $r\in\{23,31\}$, assume there exists a prime $\frac{d}{2}<q_r<d$ congruent to 2 modulo 3, and let $\mathfrak{p}_r$ be a prime of $\mathbb{Q}(\zeta_r)$ such that $|k_{\mathfrak{p}_r}|$ is a primitive root modulo q_r. If $r\in\{23,31\}$, let $S_{prim}=\{q_r,p_r\}$, else $S_{prim}=\emptyset$.

(Prim II) Assume $\mathbb{Q}(\zeta_r)$ has *odd* class number and there exist primes $q_1<q_2<d$ such that $q_1+q_2=d$ and there is a prime $\mathfrak{p}_1$ of $\mathbb{Q}(\zeta_r)$, such that $|k_{\mathfrak{p}_1}|$ is a primitive root modulo both q_1,q_2. Let $S_{prim}=\{q_1,q_2,p_1\}$.

(A) Hypotheses (Irred I), (Prim I) both hold and $S_{irr}\cap S_{prim}\neq\{p_r\}$. If $q_r\in S_{irr}\cap S_{prim}$, then $q_3=q_r$ and $p_2=p_r$. Moreover, f has $\mathfrak{p}_1$-degree (q_1,q_2), $\mathfrak{p}_2$-degree q_3 and (if $S_{irr}\cap S_{prim}=\emptyset$) $\mathfrak{p}_r$-degree q_r.

(B) Hypothesis (Irred II) holds and either (Prim I) or (Prim II) holds. If (Prim I) holds, then f has $\mathfrak{p}$-degree q and if $r\in\{23,31\}$, then f has $\mathfrak{p}_r$-degree q_r (if, and only if, $q=q_r$, one may take $\mathfrak{p}=\mathfrak{p}_r$). If (Prim II) holds, then f has both $\mathfrak{p}_1$-degree (q_1,q_2), $\mathfrak{p}$-degree q and $\mathfrak{p}\neq\mathfrak{p}_1$.

The technical looking conditions in (A) amount to saying our choices for the p_i's should be distinct, though we may choose $p_r=p_2$ and $q_r=q_3$ if we wish to. Note the existence of a prime q_r satisfying the conditions of (Prim I) is guaranteed by Lemma 5.17.

Theorem 7.1 *Suppose either (A) or (B) holds true. Set* $\pi=1-\zeta_r$.

Let $f(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0\in\mathbb{Z}[\zeta_r][x]$ *satisfy* $a_0\equiv b\pi^{d-r} \mod \pi^r$ *where* $b\equiv 1 \mod \pi^r$, $a_{d-1}\equiv u\pi \mod \pi^2$ *with* $u\not\equiv 0 \mod \pi$, *and* $a_j\equiv 0 \mod \pi^{d-j}$ *for* $1\leq j\leq d-2$; *and have*

- $\mathfrak{p}_3$*-degree* 2;
- $\mathfrak{p}_4$*-degree* r *with* p_3, p_4 *distinct and not in* $S_{irr}\cup S_{prim}$.

Furthermore, suppose that for any place v *belonging to* S_{bad}, *the set of places dividing the discriminant of* f, *one of the following holds*

- $v=\pi$;
- f *has prime* v*-degree of any height;*
- f *has* v*-degree* (q_1',q_2') *of any height where* $q_1'+q_2'=d$ *and both* q_1' *and* q_2' *are primes; or*
- $J/\mathbb{Q}(\zeta_r)$ *has semistable reduction at* v.

Then for any prime λ *of semistable reduction for* $J/\mathbb{Q}(\zeta_r)$ *whose residue characteristic* $\ell>\frac{n}{2}$ *does not belong to* $S_{bad}\cup S_{irr}\cup S_{prim}$, *the group* $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ *contains* $\mathrm{SL}_n(\ell^i)$ *if* i *is odd and* $\mathrm{SU}_n(\ell^{i/2})$ *if* i *is even. In particular,* G_λ *is large.*

Proof By Proposition 4.6, $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ contains a transvection. As $r|d$, the dimension of the $\mathbb{F}_{\ell^i}$-vector space $J[\lambda]$ equals $d-2\geq 10$. Theorem 3.10 shows $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is contained in $\mathrm{GL}(\ell^i)$ if i is odd and $\Delta\mathrm{U}_n(\ell^{i/2})$ if i is even. We may therefore apply Theorems 3.16 and 3.17. Remark 5.4 will be used without comment in the following.

We first prove $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is irreducible and not contained in a subfield subgroup. If (A) is satisfied, then Proposition 5.6 shows $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ acts irreducibly on $J[\lambda]$, else this is achieved directly by Proposition 5.5. Lemma 5.19 implies $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is not contained in a subfield subgroup.

Suppose $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ preserves a decomposition $V=\bigoplus_{j=1}^k V_j$. Since $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ acts transitively on the V_j, it suffices to show the image of the induced homomorphism θ :

$G_{\mathbb{Q}(\zeta_r)} \to S_k$ is trivial to prove primitivity. Proposition 4.6 and Lemmas 4.15, 5.12 imply θ is everywhere unramified. If $3 \leq r \leq 19$, then $\mathbb{Q}(\zeta_r)$ has no unramified extensions (see for example [39, Appendix]) and so we are done. If $r = 23$ or 31, then noting $q_r - 1 > \frac{n}{2}$, we apply Theorem 5.18 to conclude. Else (by assumption) both (Irred II) and (Prim II) hold. Proposition 5.13 then applies giving $k = 1$.

We have now shown $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ contains $\mathrm{SU}_n(\ell^{i/2})$ if i is even. Thus we suppose i is odd in the following. In this case we need to show $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ is not contained in a classical group, in particular it is sufficient to show it does not preserve a symmetric or alternating form. The first cannot happen since $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ contains a transvection [15, Prop. 5.7] and the latter is ruled out by Lemma 5.19. We conclude $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})$ contains $\mathrm{SL}_n(\ell^i)$ when i is odd.

The final statement follows from the fact that $\rho_\lambda(G_{\mathbb{Q}(\zeta_r)})/G_\lambda$ is cyclic and the groups $\mathrm{SL}_n(\ell^i)$ and $\mathrm{SU}_n(\ell^{i/2})$ are perfect. □

Theorem 7.2 *Suppose the conditions of Theorem 7.1 are satisfied. Then the image of*

$$\rho_\ell : G_{\mathbb{Q}(\zeta_r)} \to \mathrm{Aut}(J[\ell])$$

is large provided $J/\mathbb{Q}(\zeta_r)$ is semistable at $\ell > \frac{n}{2}$ and ℓ is distinct from $r, q_1, q_2, q_3, p_1, p_2, p_3, p_4, p_r$.

Proof We may view $H = \rho_\ell(G_{\mathbb{Q}(\zeta_{r\ell})})$ as a subgroup of $C_{\mathrm{Sp}_{2g}(\ell)}(\zeta_r)$. Theorem 7.1 ensures that the projection onto each factor of $C_{\mathrm{Sp}_{2g}(\ell)}(\zeta_r)$ contains the commutator subgroup. As f has $\mathfrak{p}_3$-degree 2, Example 4.11 allows us to apply Theorem 3.22 to H, from which we deduce our representation has large image. □

Theorem 7.3 *Suppose the conditions of the Theorem 7.1 hold, and in addition $\ell \equiv 1 \mod r$. Then*

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_r)}) = \mathrm{GL}_n(\ell)$$

provided $J/\mathbb{Q}(\zeta_r)$ is semistable at $\ell > \frac{n}{2}$ and ℓ is distinct from $r, q_1, q_2, q_3, p_1, p_2, p_3, p_4, p_r$.

Proof This is a direct consequence of Theorem 7.1 and Proposition 6.11. □

Theorem 7.4 *Suppose the conditions of Theorem 7.1 hold and let $\ell \equiv -1 \mod r$ be a prime of semistable reduction for $J/\mathbb{Q}(\zeta_r)$ greater than $\frac{n}{2}$ and distinct from $r, q_1, q_2, q_3, p_1, p_2, p_3, p_4, p_r$. Suppose there exists some $\delta | 2r$ such that $\gcd(\frac{d}{r}, \frac{\ell+1}{\delta}) = \gcd(\delta, \frac{\ell+1}{\delta}) = 1$. Then*

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_r)}) = \Delta\mathrm{U}_n(\ell).$$

Proof This is a direct consequence of Theorem 7.1 and Proposition 6.12. □

In the below we let

$$\mathrm{GL}_n(\ell)^{\lceil \frac{g}{3} \rceil, 6} = \{\sigma \in \mathrm{GL}_n(\ell) | \det(\sigma) \in \langle a^{\lceil \frac{g}{3} \rceil}, b \rangle\}$$

where a generates $\mathbb{F}_\ell^*$ and $b \in \mathbb{F}_\ell^*$ has order 6. We also write

$$\mathrm{GU}_n(\ell)^{\lceil \frac{g}{3} \rceil, 6} = \{\sigma \in \mathrm{GU}_n(\ell) | \det(\sigma) \in \langle a^{\lceil \frac{g}{3} \rceil}, b \rangle\}$$

where a generates $(\mathbb{F}_{\ell^2}^*)^{\ell-1}$ and $b \in \mathbb{F}_{\ell^2}^*$ has order 6.

Theorem 7.5 *Let $r = 3$ and suppose the conditions of Theorem 7.1 are satisfied. Then for $\ell > \frac{n}{2}$ distinct from $q_1, q_2, q_3, p_1, p_2, p_3, p_4$ and semistable for $J/\mathbb{Q}(\zeta_3)$, the image of*

$$\rho_\ell \colon G_{\mathbb{Q}(\zeta_3)} \to Aut(J[\ell])$$

is for i odd:

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = GL_n(\ell)^{\lceil \frac{g}{3} \rceil, 6} \rtimes \langle \chi_\ell \rangle$$

and for i even:

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = GU_n(\ell)^{\lceil \frac{g}{3} \rceil, 6}.\langle \chi_\ell \rangle,$$

where χ_ℓ denotes the mod ℓ cyclotomic character. In particular the image of ρ_ℓ is as large as possible.

Proof This is a direct consequence of Theorem 7.1, Remark 6.8 and Propositions 6.9 and 6.10. □

7.1 Examples

We now use the above theorems to construct superelliptic curves

$$C \colon y^r = f(x) = x^d + a_{d-1}x^{d-1} + \cdots a_1 x + a_0$$

with $a_j \in \mathbb{Q}(\zeta_r)$, for which the mod ℓ representation attached to the jacobian of C is large for all but a finite explicit set of primes ℓ.

To do this we first find coefficients a_j which ensure for each $\mathfrak{p}_s$ as in Theorem 7.1 that the Newton polygons of $f \in \mathbb{Q}(\zeta_r)_{\mathfrak{p}_s}[x]$ will have the correct form. We then factorise the discriminant of f which allows us to verify the conditions stated in Theorem 7.1 on $v \in S_{bad}$.

7.1.1 $r = 3$, $\deg(f) = 12$

Theorem 7.1 allows us to take $a_{11} = \pi, a_3 = 7\pi^9, a_2 = 14\pi^{10}, a_0 = 406\pi^9$ and every other $a_j = 0$, up to a condition on the discriminant of f. Indeed, 7 is a primitive root modulo 11 and $406 = 2 \times 7 \times 29 \equiv 1 \mod 3^2$.

The discriminant of f is a product of primes above 2, 3, 7, 29 and the primes $\zeta_3 - 5$, $45\zeta_3 + 17$, $8139777131\zeta_3 + 30568866704$, $160690522581570205\zeta_3 - 330535909372465022$. The residue characteristics of these four last primes are 31, 1549, 751887821191463868553, and 188189419441256467739625500157072019 respectively.

It follows that for $\ell > 7$ not equal to 11, 29 or any of the previously mentioned primes that the image of the mod ℓ representation attached to the jacobian of

$$y^3 = x^{12} + \pi x^{11} + 7\pi^9 x^3 + 14\pi^{10}x^2 + 406\pi^9$$

is equal to

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{10}(\ell)^{2,6} \rtimes \langle \chi_\ell \rangle \text{ for } \ell \equiv 1 \mod 3, \text{ and}$$
$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GU}_{10}(\ell)^{2,6}.\langle \chi_\ell \rangle \text{ for } \ell \equiv 2 \mod 3.$$

Let $\lambda | \ell$ with ℓ as above. If $\ell \equiv 1 \mod 3$ we have

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{10}(\ell)$$

and if $\ell \equiv 5 \mod 12$, then

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \Delta \mathrm{U}_{10}(\ell).$$

7.1.2 $r = 3, \deg(f) = 18$

The prime 7 is also a primitive root modulo 17, and thus Theorem 7.1 allows us to take $a_{17} = \pi$, $a_3 = 7\pi^{15}$, $a_2 = 14\pi^{16}$, $a_0 = 406\pi^{15}$ and every other $a_j = 0$, up to a condition on the discriminant of f.

The discriminant of f is a product of primes above $2, 3, 7, 29$ and the primes $\zeta_3 - 3, 13\zeta_3 + 15, 79\zeta_3 + 72, 335\zeta_3 + 444, 1888757\zeta_3 + 3108290, 6313875129\zeta_3 - 22078748747, 22017526552863\zeta_3 - 3454026061453$, and $193191848791723\zeta_3 + 116736896365287$. The residue characteristics of the last eight primes are $13, 199, 5737, 160621, 7358065233619, 666738627970882050013, 57275088206154601855705791 7$ and $2839797658154615638538178159 7$ respectively.

It follows that for $\ell > 7$ not equal to $17, 29$ or any of the other previously mentioned primes that the image of the mod ℓ representation attached to the jacobian of

$$y^3 = x^{18} + \pi x^{17} + 7\pi^{15}x^3 + 14\pi^{16}x^2 + 406\pi^{15}$$

is equal to

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{16}(\ell)^{6,6} \rtimes \langle \chi_\ell \rangle \text{ for } \ell \equiv 1 \mod 3, \text{ and}$$
$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GU}_{16}(\ell)^{6,6}.\langle \chi_\ell \rangle \text{ for } \ell \equiv 2 \mod 3.$$

Let $\lambda|\ell$ with ℓ as above. If $\ell \equiv 1 \mod 3$ we have

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{16}(\ell)$$

and if $\ell \equiv 5, 29 \mod 36$, then

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \Delta \mathrm{U}_{16}(\ell).$$

7.1.3 $r = 3, \deg(f) = 24$

The primes dividing the discriminant of $f(x) = x^{24} + \pi x^{23} + 7\pi^{21}x^3 + 14\pi^{22}x^2 + 406\pi^{21}$ are those above $2, 3, 7, 29$ and $7\zeta_3 + 3, 7\zeta_3 - 3, 11\zeta_3 + 3, 233\zeta_3 + 291, 3454821\zeta_3 + 5114984$, and $9907002723533750692641706004827409961669051350764135528944 71\zeta_3 + 6761770527353202998031682033565248869962073599144218173933 63$. Moreover the last six primes divide the discriminant exactly once and have residue characteristics $37, 79, 97, 71167, 20427495324433$ and a 120 digit prime number respectively.

Thus for $\ell > 11$ not equal to $23, 29$ or any of the other previously mentioned primes, the image of the mod ℓ representation attached to the jacobian of

$$y^3 = x^{24} + \pi x^{23} + 7\pi^{21}x^3 + 14\pi^{22}x^2 + 406\pi^{21}$$

is equal to

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{22}(\ell)^{8,6} \rtimes \langle \chi_\ell \rangle \text{ for } \ell \equiv 1 \mod 3, \text{ and}$$
$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GU}_{22}(\ell)^{8,6}.\langle \chi_\ell \rangle \text{ for } \ell \equiv 2 \mod 3.$$

Let $\lambda|\ell$ with ℓ as above. If $\ell \equiv 1 \mod 3$ we have

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{22}(\ell)$$

and if $\ell \equiv 5 \mod 12$, then

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \Delta \mathrm{U}_{22}(\ell).$$

7.1.4 $r = 3, \deg(f) = 30$

The primes dividing the discriminant of $f(x) = x^{30} + \pi x^{29} + 19\pi^{27}x^3 + 38\pi^{28}x^2 + 190\pi^{27}$ are those above $2, 3, 5, 19$ and $7\zeta_3 + 3, 21\zeta_3 + 8, 23\zeta_3 + 57, 91969915\zeta_3 + 21624639, 1200258023\zeta_3 + 748167174, 3886224025627\zeta_3 - 3573324917796$, and $702018738854765774161209865355072484285 67\zeta_3 - 985230850519346120372676072667945083133 88$. Moreover the last seven primes divide the discriminant exactly once and have residue characteristics $37, 337, 2467, 6937274066251861, 1102379788888277803$, 417581292924127556825988 37 and an 83 digit prime number respectively.

Thus for $\ell > 13$ not equal to 19, 29 or any of the other previously mentioned primes, the image of the mod ℓ representation attached to the jacobian of

$$y^3 = x^{30} + \pi x^{29} + 19\pi^{27}x^3 + 38\pi^{28}x^2 + 190\pi^{27}$$

is equal to

$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{28}(\ell)^{10,6} \rtimes \langle \chi_\ell \rangle \text{ for } \ell \equiv 1 \mod 3, \text{ and}$$
$$\rho_\ell(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GU}_{28}(\ell)^{10,6}.\langle \chi_\ell \rangle \text{ for } \ell \equiv 2 \mod 3.$$

Let $\lambda|\ell$ with ℓ as above. If $\ell \equiv 1 \mod 3$ we have

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \mathrm{GL}_{28}(\ell)$$

and if ℓ satisfies both $\ell \equiv 5 \mod 12$ and $\ell \not\equiv -1 \mod 5$, then

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_3)}) = \Delta \mathrm{U}_{28}(\ell).$$

7.1.5 $r = 5, \deg(f) = 20$

Let $f(x) = x^{20} + 3\pi x^{19} + 41\pi^{15}x^5 + 82\pi^{18}x^2 + 3526\pi^{15}$. The norm of the discriminant of f is the product of powers of 2, 5, 41, 43 and a 265 digit prime. It follows from the theorems in the previous section that the jacobian attached to the superelliptic curve

$$y^5 = x^{20} + 3\pi x^{19} + 41\pi^{15}x^5 + 82\pi^{18}x^2 + 3526\pi^{15}$$

has large mod ℓ image for $\ell > 7$ and $\ell \neq 19, 41, 43$ or the 265 digit prime mentionned above.

In particular, if $\lambda|\ell$ with $\ell \equiv 1 \mod 5$, we have

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_5)}) = \mathrm{GL}_{18}(\ell)$$

and for $\ell \equiv 9 \mod 20$

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_5)}) = \Delta \mathrm{U}_{18}(\ell).$$

7.1.6 $r = 7, \deg(f) = 14$

Let $f(x) = x^{14} + \pi x^{13} + 2\pi^7 x^7 + 6\pi^{12} x^2 + 246\pi^7$. The norm of the discriminant of f is the product of powers of 2, 3, 7, 41 and the primes 701, 11039501386253916593179 along with a 211 digit prime. In particular, the discriminant of f is squarefree away from 2, 3, 7, 41.

It follows from the theorems in the previous section that the jacobian attached to the superelliptic curve

$$y^7 = x^{14} + \pi x^{13} + 2\pi^7 x^7 + 6\pi^{12} x^2 + 246\pi^7$$

has large mod ℓ image for $\ell > 7$ and $\ell \neq 13, 41, 701, 11039501386253916593179$ or the 211 digit prime dividing the norm of the discriminant of f.

In particular, if $\lambda | \ell$ with $\ell \equiv 1 \mod 7$, we have

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_7)}) = \mathrm{GL}_{12}(\ell)$$

and for $\ell \equiv 13 \mod 28$

$$\rho_\lambda(G_{\mathbb{Q}(\zeta_7)}) = \Delta\mathrm{U}_{12}(\ell).$$

Acknowledgements The author would like to thank his supervisor Tim Dokchitser for suggesting this project. He would further like to thank Tim Dokchitser and Scott Harper for many useful conversations. He also thanks Pedro Lemos, David Loeffler, Jeremy Rickard, David Zywina and the anonymous reviewer for their help and comments. The majority of this work was carried out during the author's PhD at the University of Bristol, which was supported by the Engineering and Physical Sciences Research Council, grant number EP/N509619/1. The author also made changes to the paper whilst in Université Clermont Auvergne supported by an early career fellowship from the London Mathematical Society, and during the time he transitioned from Universität Bayreuth to the Universitat de Barcelona, where he was supported by the Deutsche Forschungsgemeinschaft (DFG) project grant STO 299/18-2 (AOBJ: 686837) and by the Spanish Ministry of Science and Innovation via the grant "Abelian varieties, L-functions, and rational points" (code PID2022-137605NB-I00) respectively. He thanks these institutions and funding bodies for both their support and providing excellent working conditions.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

References

1. Anni, S., Dokchitser, V.: Constructing hyperelliptic curves with surjective Galois representations. Trans. Am. Math. Soc. **373**(2), 1477–1500 (2020)
2. Anni, S., Lemos, P., Siksek, S.: Residual representations of semistable principally polarized abelian varieties. Res. Number Theory **1**, 12 (2016)
3. Aschbacher, M.: On the maximal subgroups of the finite classical groups. Invent. Math. **76**(3), 469–514 (1984)
4. Bosch, S., Lütkebohmert, W., Raynaud, M.: Néron models. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). Results in Mathematics and Related Areas (3), vol. 21. Springer, Berlin (1990)
5. Burness, T.C., Giudici, M.: Classical groups, derangements and primes. Australian Mathematical Society Lecture Series, vol. 25. Cambridge University Press, Cambridge (2016)
6. Burness, T.C.: Fixed point ratios in actions of finite classical groups. II. J. Algebra **309**(1), 80–138 (2007)

7. Burness, T.C.: Fixed point ratios in actions of finite classical groups. IV. J. Algebra **314**(2), 749–788 (2007)
8. Chai, C-L.: Conrad, brian, oort, frans: complex multiplication and lifting problems. In: Mathematical Surveys and Monographs, vol. 195. American Mathematical Society, Providence (2014)
9. Diaz, F.D.: Tables minorant la racine n-ième du discriminant d'un corps de degré n, volume 6 of Publications Mathématiques d'Orsay 80. Mathematical Publications of Orsay 80. Université de Paris-Sud, Département de Mathématique, Orsay (1980)
10. Dieulefait, L.V.: Explicit determination of the images of the Galois representations attached to abelian surfaces with $\mathrm{End}(A) = \mathbb{Z}$. Exp. Math. **11**(4), 503–512 (2003)
11. Dokchitser, T.: Models of curves over discrete valuation rings. Duke Math. J. **170**(11), 2519–2574 (2021)
12. Dokchitser, T., Dokchitser, V., Maistret, C., Morgan, A.: Arithmetic of hyperelliptic curves over local fields. Math. Ann. **385**(3–4), 1213–1322 (2023)
13. Fité, F.: Ordinary primes for some varieties with extra endomorphisms. Publ. Mat. **68**(1), 27–40 (2024)
14. Grothendieck, A., Raynaud, M.: Modeles de Néron et monodromie. Springer, Berlin Heidelberg (1972)
15. Grove, L.C.: Classical groups and geometric algebra. Graduate Studies in Mathematics, vol. 39. American Mathematical Society, Providence (2002)
16. Guralnick, R.M., Saxl, J.: Generation of finite almost simple groups by conjugates. J. Algebra **268**(2), 519–571 (2003)
17. Henniart, G.: Représentations l-adiques abéliennes. In: Seminar on Number Theory, Paris 1980-81 (Paris, 1980/1981), volume 22 of Progr. Math., pages 107–126. Birkhäuser Boston, Boston, MA (1982)
18. Kleidman, P., Liebeck, M.: The subgroup structure of the finite classical groups. London Mathematical Society Lecture Note Series, vol. 129. Cambridge University Press, Cambridge (1990)
19. Lang, S.: Complex multiplication. Grundlehren der mathematischen Wissenschaften. Fundamental Principles of Mathematical Sciences, vol. 255. Springer, New York (1983)
20. Liebeck, M.W., Shalev, A.: Simple groups, permutation groups, and probability. J. Am. Math. Soc. **12**(2), 497–520 (1999)
21. Liu, Q.: Algebraic geometry and arithmetic curves, volume 6 of Oxford Graduate Texts in Mathematics. Oxford University Press, Oxford (2002). (Translated from the French by Reinie Erné, Oxford Science Publications)
22. Moree, P.: Bertrand's postulate for primes in arithmetical progressions. Comput. Math. Appl. **26**(5), 35–43 (1993)
23. Mumford, D.: Abelian varieties, volume 5 of Tata Institute of Fundamental Research Studies in Mathematics. Tata Institute of Fundamental Research, Bombay. Oxford University Press, London (1970)
24. Myron Masley J., Hugh L.: Montgomery. Cyclotomic fields with unique factorization. J. Reine Angew. Math., 286(287):248–256 (1976)
25. Neukirch, J.: Algebraic number theory, volume 322 of Grundlehren der mathematischen Wissenschaften. Fundamental Principles of Mathematical Sciences. Springer, Berlin (Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G, Harder) (1999)
26. Neukirch, J., Schmidt, A., Wingberg, K.: Cohomology of number fields, volume 323 of Grundlehren der mathematischen Wissenschaften. Fundamental Principles of Mathematical Sciences, second edition. Springer, Berlin (2008)
27. Odlyzko, A.: Discriminant bounds (1976). Available at http://www.dtc.umn.edu/~odlyzko/unpublished/index.html
28. Ribet, K.A.: Galois action on division points of Abelian varieties with real multiplications. Am. J. Math. **98**(3), 751–804 (1976)
29. Schappacher, N.: Periods of Hecke characters. Lecture Notes in Mathematics, vol. 1301. Springer, Berlin (1988)
30. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. **15**(4), 259–331 (1972)
31. Serre, J.-P., Tate, J.: Good reduction of abelian varieties. Ann. Math. **2**(88), 492–517 (1968)
32. Shimura, G.: Algebraic number fields and symplectic discontinuous groups. Ann. Math. **2**(86), 503–592 (1967)
33. Shimura, G.: Abelian varieties with complex multiplication and modular functions. Princeton Mathematical Series, vol. 46. Princeton University Press, Princeton, NJ (1998)
34. Silverberg, A.: Fields of definition for homomorphisms of abelian varieties. J. Pure Appl. Algebra **77**(3), 253–262 (1992)
35. Tate, J.: Number theoretic background. In: Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, volume XXXIII of Proc. Sympos. Pure Math., pages 3–26. Amer. Math. Soc., Providence, RI (1979)
36. Upton, M.G.: Galois representations attached to Picard curves. J. Algebra **322**(4), 1038–1059 (2009)

37. Wall, G.E.: On the conjugacy classes in the unitary, symplectic and orthogonal groups. J. Aust. Math. Soc. **3**, 1–62 (1963)
38. Washington, L.C.: Introduction to cyclotomic fields, volume 83 of Graduate Texts in Mathematics, second edition. Springer-Verlag, New York (1997)
39. Yamamura, K.: The determination of the imaginary abelian number fields with class number one. Math. Comp. **62**(206), 899–921 (1994)
40. Zalesskiĭ, A.E., Serežkin, V.N.: Linear groups generated by transvections. Izv. Akad. Nauk SSSR Ser. Mat. **40**(1), 26–49 (1976)
41. Zarhin, Y.G.: Endomorphism algebras of superelliptic Jacobians. In Geometric methods in algebra and number theory, volume 235 of Progr. Math., pages 339–362. Birkhäuser Boston, Boston, MA (2005)