Forum of Mathematics, Sigma (2025), **Vol. 13**:e6 1–14
doi:10.1017/fms.2024.156

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

A single source theorem for primitive points on curves

Maleeha Khawaja[1] and Samir Siksek[2]

[1]School of Mathematics and Statistics, Univseristy of Sheffield, Hicks Building, Sheffield, S3 7RH, United Kingdom;
E-mail: mkhawaja2@sheffield.ac.uk.
[2]Mathematics Institute, University of Warwick, Gibbet Hill Road, Coventry, CV4 7AL, United Kingdom;
E-mail: s.siksek@warwick.ac.uk (Corresponding author).

Received: 5 January 2024; **Revised:** 3 October 2024; **Accepted:** 15 December 2024

2020 Mathematical Subject Classification: *Primary* – 11G30; *Secondary* – 20B15, 11S20

Abstract

Let C be a curve defined over a number field K and write g for the genus of C and J for the Jacobian of C. Let $n \geq 2$. We say that an algebraic point $P \in C(\overline{K})$ has degree n if the extension $K(P)/K$ has degree n. By the Galois group of P we mean the Galois group of the Galois closure of $K(P)/K$ which we identify as a transitive subgroup of S_n. We say that P is primitive if its Galois group is primitive as a subgroup of S_n. We prove the following 'single source' theorem for primitive points. Suppose $g > (n-1)^2$ if $n \geq 3$ and $g \geq 3$ if $n = 2$. Suppose that either J is simple or that $J(K)$ is finite. Suppose C has infinitely many primitive degree n points. Then there is a degree n morphism $\varphi : C \to \mathbb{P}^1$ such that all but finitely many primitive degree n points correspond to fibres $\varphi^{-1}(\alpha)$ with $\alpha \in \mathbb{P}^1(K)$. We prove, moreover, under the same hypotheses, that if C has infinitely many degree n points with Galois group S_n or A_n, then C has only finitely many degree n points of any other primitive Galois group.

Contents

1 Introduction 1
2 Primitive group actions 3
3 Primitivity and Riemann–Roch dimension 4
4 Proof of Theorem 1.4 6
5 Proof of Theorem 1.1 6
6 Galois Theory and specializations 8
7 Proof of Theorem 1.2 11
References 13

1. Introduction

Low degree points on curves have long been a subject of intensive study, both from a theoretical point-of-view (e.g., [2], [31]) and algorithmically (e.g., [28]). Perhaps the most celebrated result in this subject is Merel's uniform boundedness theorem [23], which (thanks to a strengthening due to Oesterlé [10, Section 6]) asserts that the only degree n points on the modular curve $X_1(p)$ (with p prime) are cuspidal, for $n < 2\log_3(\sqrt{p}-1)$. A common theme in the subject is to seek a description of which curves can have infinitely many points of a certain degree. For example, a famous theorem of Harris and Silverman [16] asserts that if a curve C over a number field K, of genus ≥ 2, has infinitely many quadratic points,

then it is either hyperelliptic or bielliptic. The strongest results to date on infinite families of low degree points on curves are due to Smith and Vogt [29] and to Kadets and Vogt [20], whose works elucidate the geometric origin of such families provided the degree is small compared to the genus. By comparison, the question of which groups arise infinitely often as Galois groups of low degree points on a curve has received very little attention; the only results we are aware of concern degrees 3 or 4 (e.g., [4], [5], [11], [18], [19]). This paper is concerned with giving insights into this question for primitive groups. Before we go further, we recall the notion of a primitive permutation group. Let G be a group acting on a finite set Ω. We say the action is **primitive** if it is transitive and the only partitions of Ω that are G-stable are $\{\Omega\}$ and $\{\{\omega\} : \omega \in \Omega\}$. It is well-known that a 2-transitive group acts primitively (Lemma 2.1 below), and thus, S_n and A_n are primitive groups (with their natural action on $\{1, 2, \ldots, n\}$), for $n \geq 1$ and $n \geq 3$, respectively.

Let K be a perfect field and let $\overline{K}$ denote a fixed algebraic closure of K. Write $G_K = \mathrm{Gal}(\overline{K}/K)$ for the absolute Galois group of K. Let C be a curve defined over K (by which we mean a smooth projective and geometrically irreducible variety defined over K having dimension 1). By a degree n point on C/K we mean an algebraic point $P \in C(\overline{K})$ such that $[K(P) : K] = n$. Equivalently, the orbit of P under the action of G_K has size n. If the orbit of P is $\{P_1, \ldots, P_n\}$, then we define the **Galois group of** P, which we denote by $\mathrm{Gal}(P/K)$, to be the image of the natural permutation representation $G_K \to \mathrm{Sym}(\{P_1, \ldots, P_n\})$. Thus, we may identify $\mathrm{Gal}(P/K)$ (up to conjugation) as a transitive subgroup of the n-th symmetric group S_n. The Galois group of P is also the Galois group of the Galois closure of $K(P)/K$. Following [21], we say that the point P is **primitive** if $\mathrm{Gal}(P/K)$ acts primitively on $\{P_1, \ldots, P_n\}$; this means that the only partitions of the orbit $\Omega = \{P_1, \ldots, P_n\}$ preserved by $\mathrm{Gal}(P/K)$ are $\{\Omega\}$ and the singletons partition $\{\{P_1\}, \ldots, \{P_n\}\}$. We call a divisor D on C **rational** if it is supported on $C(\overline{K})$ and stable under the action of G_K. Henceforth, all divisors considered are assumed to be rational. An effective divisor D is said to be **reducible** if it admits a decomposition $D = D_1 + D_2$, where $D_1 > 0$, $D_2 > 0$ and both are rational; otherwise, we say that D is irreducible. Thus, an irreducible divisor consists of a single Galois orbit of algebraic points; an irreducible divisor of degree n is what many other authors (e.g., [3], [20], [29], [31]) call a degree n closed point. We call an irreducible divisor **primitive** if it is the Galois orbit of a primitive point.

Theorem 1.1. *Let K be a number field. Let C/K be a curve of genus g, and write J for the Jacobian of C. Let $n \geq 2$ and suppose*

$$\begin{cases} g > (n-1)^2 & \text{if } n \geq 3 \\ g \geq 3 & \text{if } n = 2. \end{cases} \tag{1.1}$$

Suppose that $A(K)$ is finite for every abelian subvariety A/K of J of dimension $\leq n/2$. If C has infinitely many primitive points of degree n, then there is a degree n morphism $\varphi : C \to \mathbb{P}^1$ defined over K such that all but finitely many primitive degree n divisors are fibres $\varphi^*(\alpha)$ with $\alpha \in \mathbb{P}^1(K)$.

We call Theorem 1.1 the "Single Source Theorem", since, with finitely many exceptions, all primitive degree n points come from a single source which is the morphism $\varphi : C \to \mathbb{P}^1$.

Theorem 1.2. *Let K be a number field. Let C/K be a curve of genus g, and write J for the Jacobian of C. Let $n \geq 2$ and suppose (1.1) holds. Suppose that $A(K)$ is finite for every abelian subvariety A/K of J of dimension $\leq n/2$. Suppose C has infinitely many degree n points with Galois group S_n or A_n. Then C has only finitely many degree n points with any primitive Galois group $\neq A_n, S_n$.*

The above results show that primitive points are severely constrained if their degree is sufficiently small compared to the genus. If the degree is large compared to the genus, then the behaviour is very different. Indeed, Derickx [9] has shown that if C is a smooth projective curve over a number field K of genus g with $C(K) \neq \emptyset$, then C has infinitely many primitive degree n points for every $n > 2g$. For the intermediate range $g + 1 \leq n \leq 2g$, the existence of a single primitive degree n point guarantees the existence of infinitely many [21, Theorem 12].

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

We point out that, in both Theorems 1.1 and 1.2, we may replace the assumption '$A(K)$ is finite for every abelian subvariety A/K of J of dimension $\leq n/2$' with the stronger (but more simply-stated) assumption that 'J is simple or $J(K)$ is finite'. Later on, we give versions of both theorems where this assumption is replaced by a weaker but more technical hypothesis (Theorems 5.1 and 7.1).

We mention two intermediate results that may be of independent interest.

Theorem 1.3. *Let K be a perfect field. Let $n \geq 2$. Let C be a curve of genus g defined over K. Suppose*

$$g > \frac{(n-1)(n-2)}{2}. \tag{1.2}$$

Let D be a primitive degree n divisor on C. Then $\ell(D) \leq 2$.

Here, $L(D)$ denotes the Riemann–Roch space associated to D, and $\ell(D)$ denotes its dimension. We believe that Theorem 1.3 is the first ever example of a relationship between the Galois group of a divisor and its Riemann–Roch dimension.

Theorem 1.4. *Let K be a perfect field. Let C/K be a curve of genus g. Let $n \geq 2$. Let D_1, D_2 be two primitive degree n divisors on C with $\ell(D_1) = \ell(D_2) = 2$. Suppose*

$$g > (n-1)^2. \tag{1.3}$$

Then D_1, D_2 are linearly equivalent.

The paper is structured as follows. In Section 2, we review some standard results on primitive group actions that are needed later in the paper. In Section 3, we prove Theorem 1.3: if $\ell(D) \geq 3$ and D is primitive, then we show that C is birational to a plane degree n curve which contradicts (1.2). In Section 4, we prove Theorem 1.4: if D_1, D_2 are inequivalent and primitive, then we show that C is birational to an (n,n)-curve on $\mathbb{P}^1 \times \mathbb{P}^1$ contradicting (1.3). In Section 5, we show that Theorem 1.1 follows from Theorems 1.3, 1.4 and a famous theorem of Faltings on rational points lying on subvarieties of abelian varieties. The next two sections (Section 6 and Section 7) are devoted to deducing Theorem 1.2 from Theorem 1.1. Indeed, Theorem 1.1 allows us to focus on the fibres of a single degree n morphism $\varphi : C \to \mathbb{P}^1$ defined over K. We show that this morphism has 'generic Galois group' A_n or S_n, and to prove Theorem 1.2, it will be enough to show that only finitely many fibres have primitive Galois groups $\neq A_n, S_n$. The map φ is not in general a Galois cover, and we will need to consider the 'geometrically connected Galois closure' $\tilde{C} \to \mathbb{P}^1$, which is defined over an extension L of K. We show, using the simplicity of A_n, that either $L = K$ or L/K is quadratic. The fibres $\varphi^*(\alpha)$, for $\alpha \in \mathbb{P}^1(L)$, which have any given Galois group H, give rise to L-points on some subcover D_H/L of $\tilde{C}$. The proof of Theorem 1.2 boils down to noting that all these D_H have genus ≥ 2, thanks to a theorem of Guralnick and Shareshian, and hence finitely many L-points by Faltings' theorem.

2. Primitive group actions

In this section, we review some properties of primitive group actions. This is standard material (e.g. [12]), and is included for the convenience of the reader. Let G be a group acting transitively on a finite set Ω. Let $\mathcal{P}$ be a partition of Ω. We say that $\mathcal{P}$ is G-stable if $\sigma(Y) \in \mathcal{P}$ for all $Y \in \mathcal{P}$ and all $\sigma \in G$. We say that the action of G on Ω is **primitive** if the only G-stable partitions of Ω are the trivial ones: $\{\Omega\}$ and $\{\{\omega\} : \omega \in \Omega\}$. Here, is an equivalent formulation: the action of G on Ω is imprimitive if and only if there is some $Y \subset \Omega$ such that $2 \leq \#Y < \#\Omega$, and for all $\sigma \in G$, either $\sigma(Y) = Y$ or $\sigma(Y) \cap Y = \emptyset$.

Lemma 2.1. *Suppose the action of G on Ω is 2-transitive. Then the action is primitive.*

Proof. Let Y be a subset of Ω with at least two elements and suppose that for all $\sigma \in G$, either $\sigma(Y) = Y$ or $\sigma(Y) \cap Y = \emptyset$. We want to show that $Y = \Omega$. Let $c \in \Omega$; we want to show that $c \in Y$. Let $a, b \in Y$ be distinct. We may suppose $c \neq a, b$. As G is 2-transitive on Ω, there is some $\sigma \in G$ such that $\sigma(a) = a$ and $\sigma(b) = c$. As $a \in Y \cap \sigma(Y)$, we have $Y = \sigma(Y)$ and so $c \in Y$. □

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

It follows from Lemma 2.1 that S_n is primitive for all n, and A_n is primitive for $n \geq 3$.

Lemma 2.2. *Suppose* $|\Omega| \geq 2$. *The action of* G *on* Ω *is primitive if and only if* $\mathrm{Stab}(\omega)$ *is maximal for any (and hence all)* $\omega \in \Omega$.

Proof. As the action is transitive, any two point stabilizers are conjugate, and thus, if one is maximal, then so are all of them. Let $\omega \in \Omega$. As $|\Omega| \geq 2$, the stabilizer $\mathrm{Stab}(\omega)$ is a proper subgroup of G. Suppose it is non-maximal, and let $\mathrm{Stab}(\omega) \subsetneq H \subsetneq G$ be a subgroup. Let $Y = H\omega$. Then

$$2 \leq \underbrace{[H : \mathrm{Stab}(\omega)]}_{\#Y} < [G : \mathrm{Stab}(\omega)] = \#\Omega. \tag{2.1}$$

Suppose $\sigma \in G$ and $Y \cap \sigma(Y) \neq \emptyset$. Then, there are h_1, $h_2 \in H$ such that $h_1\omega = \sigma h_2 \omega$, and so $h_1^{-1}\sigma h_2 \in \mathrm{Stab}(\omega) \subset H$, so $\sigma \in H$, and hence, $\sigma(Y) = (\sigma H)\omega = H\omega = Y$. Therefore, the action is imprimitive.

Conversely, suppose the action is imprimitive, so there is some $Y \subset \Omega$ satisfying $2 \leq \#Y < \#\Omega$, and for all $\sigma \in G$, either $\sigma(Y) \cap Y = \emptyset$ or $\sigma(Y) = Y$. Let $\omega \in Y$ and let

$$H = \{\tau \in G : \tau(Y) = Y\} = \{\tau \in G : \tau(Y) \cap Y \neq \emptyset\}.$$

If $\sigma \in \mathrm{Stab}(\omega)$, then $\omega \in Y \cap \sigma(Y)$ so $\sigma(Y) = Y$ and so $\sigma \in H$. Hence, $\mathrm{Stab}(\omega) \subseteq H$. Moreover, as H acts transitively on the elements of Y, we have $[H : \mathrm{Stab}(\omega)] = \#Y$, so (2.1) holds, and therefore, $\mathrm{Stab}(\omega)$ is non-maximal. □

Lemma 2.3. *Suppose* G *acts primitively on* Ω. *Let* N *be a normal subgroup of* G. *Then* N *acts either transitively or trivially on* Ω.

Proof. We may suppose $\#\Omega \geq 2$. Let $\omega \in \Omega$. By Lemma 2.2, the stabilizer $\mathrm{Stab}(\omega)$ is maximal. Let

$$H = N\,\mathrm{Stab}(\omega) = \{nk : n \in N,\ k \in \mathrm{Stab}(\omega)\}.$$

As N is normal, H is a subgroup of G, and since $\mathrm{Stab}(\omega)$ is maximal, $H = \mathrm{Stab}(\omega)$ or $H = G$. Suppose first that $H = G$. Then $\Omega = G\omega = H\omega = N\omega$, so N acts transitively. Suppose instead that $H = \mathrm{Stab}(\omega)$. Then $N \subseteq \mathrm{Stab}(\omega)$. As N is normal and all point stabilizers are conjugate, we see that N is contained in all point stabilizers and so acts trivially. □

3. Primitivity and Riemann–Roch dimension

In this section, we prove Theorem 1.3. We assume basic knowledge of divisors and linear series as in, for example, the standard text of Arbarello, Cornalba, Griffiths and Harris [1].

Lemma 3.1. *Let* K *be a perfect field and let* C/K *be a curve. Let* D *be an irreducible divisor and let* $f \in L(D)$ *be non-constant. Then* $\mathrm{div}_\infty(f) = D$, *where* $\mathrm{div}_\infty(f)$ *denotes the divisor of poles of* f.

Proof. As f is non-constant and belongs to $L(D)$, we have $0 < \mathrm{div}_\infty(f) \leq D$. However, D is irreducible; therefore, $\mathrm{div}_\infty(f) = D$. □

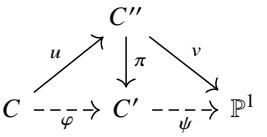
Lemma 3.2. *Let* K *be a perfect field and let* C/K *be a curve. Let* D *be a primitive divisor. Let* $f \in L(D)$ *be non-constant. Suppose there is a (possibly singular) curve* C'/K, *and rational maps* $\varphi : C \dashrightarrow C'$ *and* $\psi : C' \dashrightarrow \mathbb{P}^1$ *defined over* K *such that* $f = \psi \circ \varphi$. *Then* $\deg(\varphi) = 1$ *or* $\deg(\psi) = 1$.

Proof. Since D is primitive, it is irreducible, and thus, $\mathrm{div}_\infty(f) = D$ by Lemma 3.1.

Now let $\pi : C'' \to C'$ be the normalization of C'. The map π is birational, and we write $u = \pi^{-1} \circ \varphi$, and $v = \psi \circ \pi$. As C and C'' are proper, $u : C \to C''$ and $v : C'' \to \mathbb{P}^1$ are morphisms defined over K.

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

Consider the following commutative diagram:



We note that $f = \psi \circ \varphi = v \circ u$. In particular, $D = f^*(\infty) = u^*(v^*(\infty))$.

Write $r = \deg(u)$ and $s = \deg(v)$. Write $v^*(\infty) = Q_1 + \cdots + Q_s$. Note that

$$\{u^{-1}(Q_i) : i \in \{1, \ldots, s\}\}$$

is a partition of the points in D, into s subsets of size r, that is Galois-stable. As D is primitive, either $r = 1$ or $s = 1$. However, $r = \deg(\varphi)$ and $s = \deg(\psi)$, completing the proof. □

Proof of Theorem 1.3. Suppose $\ell(D) \geq 3$. Then there are $f, g \in K(C)$ such that $1, f, g$ are linearly independent elements of $L(D)$. Let V be the subspace of $L(D)$ spanned by $1, f, g$, and consider the corresponding linear system:

$$\{D + \operatorname{div}(h) \ : \ h \in V\}. \tag{3.1}$$

We claim that (3.1) is base-point free. Indeed, let D_0 be the base locus of (3.1). Thus, D_0 is a K-rational divisor and $D_0 \leq D$. Since D is irreducible, either $D_0 = 0$ or $D_0 = D$. If $D_0 = D$, then all elements of the linear system (3.1) are equal to D, which makes all $h \in V$ constant, giving a contradiction. Thus, $D_0 = 0$, establishing our claim. We let

$$\varphi : C \xrightarrow{|V|} \mathbb{P}^2, \qquad \varphi = [f : g : 1],$$

and let C' be the image of C in $\mathbb{P}^2$ under φ, which is a geometrically irreducible curve defined over K, but may be singular. We claim that $[0 : 1 : 0] \notin C'$. Suppose $[0 : 1 : 0] \in C'$; thus, there is some point $P \in C$ such that $(f/g)(P) = (1/g)(P) = 0$. However, by Lemma 3.1, we have $\operatorname{div}_\infty(f) = \operatorname{div}_\infty(g) = D$. Since $(1/g)(P) = 0$, we have $\operatorname{ord}_P(D) > 0$. But then $\operatorname{ord}_P(f) = -\operatorname{ord}_P(D) = \operatorname{ord}_P(g)$, contradicting $(f/g)(P) = 0$ and establishing our claim.

Write

$$\psi : C' \to \mathbb{P}^1, \qquad \psi[x : y : z] = [x : z].$$

We may interpret this as projection of the curve C' from the point $[0 : 1 : 0]$ to the line $\ell = \{[x : 0 : z] \ : \ [x : z] \in \mathbb{P}^1\}$. For a suitably general point $[a : b] \in \mathbb{P}^1$, the pull-back $\psi^*[a : b]$ is the intersection of C' with the line connecting $[0 : 1 : 0]$ with $[a : 0 : b]$. Thus, $\deg(\psi)$ is the degree of C' as a plane curve.

We also denote by φ the morphism $C \to C'$. Then $\psi \circ \varphi = f$. Applying Lemma 3.2 to $\psi \circ \varphi = f$ gives $\deg(\varphi) = 1$ or $\deg(\psi) = 1$. However, if $\deg(\psi) = 1$, then C' is a line which contradicts the linear independence of $1, f, g$. Thus, $\deg(\varphi) = 1$, and so $\deg(\psi) = \deg(f) = \deg(D) = n$ since $\operatorname{div}_\infty(f) = D$. In particular, the plane curve C' has degree n. As $\deg(\varphi) = 1$, the map $\varphi : C \to C'$ is birational. Hence, the geometric genus of C' is g. Since C' has degree n, its arithmetic genus is $(n-1)(n-2)/2$. As the geometric genus is bounded by the arithmetic genus, we have that $g \leq (n-1)(n-2)/2$. This contradicts (1.2). □

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

4. Proof of Theorem 1.4

As $\ell(D_i) = 2$, we may choose non-constant $f_i \in L(D_i)$. Then $\mathrm{div}_\infty(f_i) = D_i$ by Lemma 3.1, and in particular, $\deg(f_i) = n$. Let

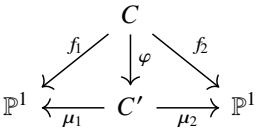
$$\varphi \ : \ C \to \mathbb{P}^1 \times \mathbb{P}^1, \qquad \varphi = (f_1, f_2),$$

and let $C' = \varphi(C)$. Then C'/K is an irreducible but possibly singular curve lying on $\mathbb{P}^1 \times \mathbb{P}^1$; we also denote the map $C \to C'$ by φ. Let $\pi_1, \pi_2 : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ denote projection onto the first and second factor, respectively. Let $\mu_i = \pi_i|_{C'} : C' \to \mathbb{P}^1$. Then $f_i = \mu_i \circ \varphi$. By Lemma 3.2, there are two possibilities:

(I) either $\deg(\varphi) = 1$ and $\deg(\mu_1) = \deg(\mu_2) = n$;
(II) or $\deg(\varphi) = n$ and $\deg(\mu_1) = \deg(\mu_2) = 1$.

Suppose that (I) holds. Then φ is a birational map, and so C and C' have the same geometric genus g. Moreover, C' is a curve of bidegree (n, n) on $\mathbb{P}^1 \times \mathbb{P}^1$ and therefore has arithmetic genus $(n-1)^2$ (see [17, Exercise III.5.6]). Thus, $g \le (n-1)^2$ giving a contradiction.

Therefore, (II) holds. Thus, μ_1, μ_2 are birational, and we have a commutative diagram of morphisms



Write $\mu = \mu_2 \circ \mu_1^{-1}$. Then $\mu : \mathbb{P}^1 \to \mathbb{P}^1$ is an automorphism satisfying $f_2 = \mu \circ f_1$. Thus, $f_2^* = f_1^* \circ \mu^* = f_1^* \circ \mu^{-1}$. Let $\alpha = \mu^{-1}(0)$. Then

$$\mathrm{div}(f_2) = f_2^*(0) - f_2^*(\infty) = f_2^*(0) - D_2, \qquad \mathrm{div}(f_1 - \alpha) = f_1^*(\alpha) - f_1^*(\infty) = f_2^*(0) - D_1.$$

Hence, $D_2 - D_1 = \mathrm{div}((f_1 - \alpha)/f_2)$ establishing the theorem.

5. Proof of Theorem 1.1

Let C be a smooth projective and absolutely irreducible curve over a number field K, with genus $g \ge 2$, and write J for its Jacobian. Let $n \ge 1$. We denote the n-th symmetric power of C by $C^{(n)}$; this is defined as the quotient $C^{(n)} = C^n/S_n$, where S_n is the n-th symmetric group acting naturally on the n-th Cartesian power C^n of C. Recall that $C^{(n)}(K)$ can be identified with the set of effective degree n divisors on C. Let D_0 be a fixed rational divisor of degree n, and let

$$\iota : C^{(n)} \to J, \qquad D \mapsto [D - D_0] \tag{5.1}$$

be the corresponding Abel–Jacobi map. Write $W_n(C) = W_n^0(C)$ for the image of $C^{(n)}$ under ι; this is the degree n Brill–Noether locus [1, Section IV.3].

We now state a stronger, but more technical, version of Theorem 1.1.

Theorem 5.1. *Let $n \ge 2$ and suppose (1.1) holds. Suppose $W_n(C)$ does not contain the translate of an abelian subvariety A/K of J of positive rank. If C has infinitely many primitive points of degree n, then there is a degree n morphism $\varphi : C \to \mathbb{P}^1$ defined over K such that all but finitely many primitive degree n divisors are fibres $\varphi^*(\alpha)$ with $\alpha \in \mathbb{P}^1(K)$.*

We point out that Derickx [8] has developed a powerful computational method that is often capable of ruling out the existence of translates of abelian varieties within $W_n(C)$, even when J has abelian subvarieties of small dimension.

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

We shall need the following theorem of Debarre and Fahlaoui [7, Corolllary 3.6].

Theorem 5.2 (Debarre and Fahlaoui). *Suppose $n \leq g-1$. Let A be an abelian subvariety of J with a translate contained in $W_n(C)$. Then* $\dim(A) \leq n/2$.

Thanks to the theorem of Debarre and Fahlaoui, Theorem 5.1 immediately implies Theorem 1.1. It is therefore enough to prove Theorem 5.1.

We shall also need the following famous theorem of Faltings [13] which establishes the Mordell–Lang conjecture for subvarieties of Abelian varieties.

Theorem 5.3 (Faltings). *Let B be an abelian variety defined over a number field K, and let $V \subset B$ be a subvariety defined over K. Then there is a finite number of abelian subvarieties $B_1, \ldots, B_r$ of B, defined over K, and a finite number of points $x_1, \ldots, x_r \in V(K)$ such that the translates $x_i + B_i$ are contained in V, and, moreover, such that*

$$V(K) = \bigcup_{i=1}^{r} x_i + B_i(K).$$

For the proof of Theorem 5.1, we shall need the following proposition.

Proposition 5.4. *Let $n \leq g-1$. Suppose that $W_n(C)$ does not contain the translate of an abelian subvariety A/K of J of positive rank. Then there are a finite number of divisors $D_1, D_2, \ldots, D_m \in C^{(n)}(\mathbb{Q})$ such that*

$$C^{(n)}(K) = \bigcup_{i=1}^{m} |D_i|.$$

Here, $|D|$ denotes the complete linear system corresponding to D:

$$|D| \;=\; \{D + \operatorname{div}(f) \;:\; f \in L(D)\}.$$

Proposition 5.4 is an elementary and straightforward consequence of the aforementioned theorem of Faltings; versions of the proposition have appeared elsewhere [2, Theorem 4.2], [14, Proposition 2], [16, Theorem 2], [21, Proposition 18]. For the convenience of the reader, we give the proof.

Proof of Proposition 5.4. Recall our assumption that $n \leq g-1$. The Brill–Noether locus $W_n(C)$ has dimension n as it is birational to $C^{(n)}$ (see, for example, [24, Theorem 5.1]) and is therefore a proper subvariety of J. We apply Faltings' theorem to deduce that

$$W_n(C)(K) = \bigcup_{i=1}^{r} x_i + B_i(K),$$

where $x_i \in W_n(K)$, and B_i/K are abelian subvarities of J such that the translates $x_i + B_i$ are contained in $W_n(C)$. Thus, $B_i(K)$ is finite by the assumption. Thus, $W_n(C)(K)$ is finite.

We note that $\iota(C^{(n)}(K))$ is a subset of $W_n(K)$ and hence must be finite. Choose $D_1, \ldots, D_m \in C^{(n)}(K)$ such that $\iota(C^{(n)}(K)) = \{\iota(D_1), \ldots, \iota(D_m)\}$. Now let $D \in C^{(n)}(K)$. Then $[D - D_0] = \iota(D) = \iota(D_i) = [D_i - D]$ for some i, and therefore, $D \sim D_i$, giving $D \in |D_i|$. □

Proof of Theorem 5.1. Write $C^{(n)}_{\mathrm{prim}}(K)$ for the subset of $C^{(n)}(K)$ consisting of primitive divisors. We apply Proposition 5.4. Hence,

$$C^{(n)}_{\mathrm{prim}}(K) \;\subseteq\; \bigcup_{j=1}^{m} |D_j| \tag{5.2}$$

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

for some effective degree n divisors $D_1, \dots, D_m$. We may delete any $|D_j|$ from (5.2) that does not contain any primitive divisor. Recall that $D' \in |D|$ if and only if $|D'| = |D|$. Hence, we may suppose that $D_1, \dots, D_m$ are primitive. We now apply Theorem 1.3. This tells us that $\ell(D_i) = 1$ or 2 for $i = 1, \dots, m$. Moreover, Theorem 1.4 tells us that $\ell(D) = 2$ for at most one divisor D among $D_1, \dots, D_m$. If $\ell(D) = 1$, then $|D| = \{D\}$. Since $C^{(n)}_{\text{prim}}(K)$ is infinite, we deduce, after permuting the D_i, that

$$C^{(n)}_{\text{prim}}(K) \ \subseteq \ \{D_1, \dots, D_{m-1}\} \cup |D_m|,$$

where $\ell(D_m) = 2$. Let $\varphi \in L(D_m)$ be a non-constant function, which we regard as a morphism $\varphi : C \to \mathbb{P}^1$ satisfying $\varphi^*(\infty) = D_m$. If $D \in |D_m|$, and $D \neq D_m$, then $D = D_m + \text{div}(\varphi - \alpha)$ for some $\alpha \in K$, and so $D = \varphi^*(\alpha)$. This completes the proof. □

6. Galois Theory and specializations

Let K be a number field. Let $\varphi : C \to \mathbb{P}^1$ be a morphism of curves defined over K. Note that $K(C) \cap \overline{K} = K$, as C is geometrically connected. We write $\text{Ram}(\varphi) \subset C$ for the set of ramification points of C. The **set of branch values** for φ is

$$\text{BV}(\varphi) \ = \ \{\varphi(P) \ : \ P \in \text{Ram}(\varphi)\} \ \subset \ \mathbb{P}^1.$$

Let $\mathbb{K}$ be the Galois closure of the function field extension $K(C)/K(\mathbb{P}^1)$ induced by φ. Write $n = \deg(\varphi)$. Then we may naturally identify $G' := \text{Gal}(\mathbb{K}/K(\mathbb{P}^1))$ with a transitive subgroup of S_n. In what follows, when we speak of subgroups of G' being transitive or primitive, it is with respect to the action on $\{1, 2, \dots, n\}$.

Lemma 6.1. *Let $\alpha \in \mathbb{P}^1(K)$, and consider α as a place of $\mathbb{P}^1$. Let $\mathcal{P}$ be a place of $\mathbb{K}$ above α. Then $K(\mathcal{P})/K$ is a Galois extension with Galois group isomorphic to the decomposition group*

$$G'_{\mathcal{P}} = \{\sigma \in G' \ : \ \sigma(\mathcal{P}) = \mathcal{P}\}.$$

Proof. For this, see [30, Theorem III.8.2]. However, we will sketch some of the ideas in the proof of Lemma 6.2. □

Let $L = \mathbb{K} \cap \overline{K}$, which is a finite Galois extension of K. Let $G = \text{Gal}(\mathbb{K}/L(\mathbb{P}^1))$. Then we obtain an exact sequence of Galois groups

$$1 \to \underbrace{\text{Gal}(\mathbb{K}/L(\mathbb{P}^1))}_{G} \to \underbrace{\text{Gal}(\mathbb{K}/K(\mathbb{P}^1))}_{G'} \to \underbrace{\text{Gal}(L(\mathbb{P}^1)/K(\mathbb{P}^1))}_{\cong \text{Gal}(L/K)} \to 1. \tag{6.1}$$

We note that $\mathbb{K}/L(\mathbb{P}^1)$ is regular in the sense that $\mathbb{K} \cap \overline{L} = L$. Therefore, $\mathbb{K} = L(\tilde{C})$, where $\tilde{C}$ is a (geometrically connected) curve defined over L. The inclusions $L(\mathbb{P}^1) \subseteq L(C) \subseteq L(\tilde{C})$ correspond to morphisms

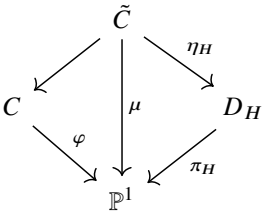
$$\tilde{C} \to C \xrightarrow{\varphi} \mathbb{P}^1,$$

and we write $\mu : \tilde{C} \to \mathbb{P}^1$ for the composition which is defined over L. We may naturally identify G with automorphisms of the cover μ.

Now let H be a subgroup of G. Write $\mathbb{K}^H$ for the subfield of $\mathbb{K}$ fixed by H. The function field extension $\mathbb{K}^H/L(\mathbb{P}^1)$ corresponds to a morphism of curves $\pi_H : D_H \to \mathbb{P}^1$ defined over L, where $L(D_H) = \mathbb{K}^H$.

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

Note that we have the following commutative diagram of morphisms:



(6.2)

We note that $\mathrm{BV}(\mu) = \mathrm{BV}(\varphi)$ (see, for example, [30, Corollary III.8.4]). It follows that $\mathrm{BV}(\pi_H) \subseteq \mathrm{BV}(\varphi)$.

We shall use (6.2) to study fibres of the map φ with certain Galois group. The curve D_H is important to us because of the following standard result.

Lemma 6.2. *Let $\mathcal{P} \in \tilde{C}$ be an algebraic point with $\mu(\mathcal{P}) \in \mathbb{P}^1(L) - \mathrm{BV}(\varphi)$. Write*

$$G_{\mathcal{P}} := \{\sigma \in G \ : \ \sigma(\mathcal{P}) = \mathcal{P}\}$$

for the decomposition group of $\mathcal{P}$. Let H be a subgroup of G, and suppose $G_{\mathcal{P}} \subseteq H$. Then $\eta_H(\mathcal{P}) \in D_H(L)$.

Proof. The lemma is implicit in most proofs of Hilbert's Irreducibility Theorem (e.g., [27, Proposition 3.3.1]), but we give a proof as it helps make ideas precise. Note that $\mathcal{P}$ is unramified in μ. Since $\mathbb{K}/L(\mathbb{P}^1)$ is a Galois extension, the extension $L(\mathcal{P})/L$ is Galois, and its Galois group can be identified with $G_{\mathcal{P}}$ in a natural way; see, for example, [30, Theorem 3.8.2]. We shall in fact need some of the details of this identification, which we now sketch. Write

$$\mathcal{O}_{\mathcal{P}} = \{f \in \mathbb{K} \ : \ \mathrm{ord}_{\mathcal{P}}(f) \geq 0\}, \qquad \mathfrak{m}_{\mathcal{P}} = \{f \in \mathbb{K} \ : \ \mathrm{ord}_{\mathcal{P}}(f) > 0\}, \tag{6.3}$$

for the valuation ring of $\mathcal{P}$ and its maximal ideal. Then $L(\mathcal{P})$ may be identified with $\mathcal{O}_{\mathcal{P}}/\mathfrak{m}_{\mathcal{P}}$ via the well-defined map

$$\mathcal{O}_{\mathcal{P}}/\mathfrak{m}_{\mathcal{P}} \to L(\mathcal{P}), \qquad f + \mathfrak{m}_{\mathcal{P}} \mapsto f(\mathcal{P}).$$

Let $\sigma \in G_{\mathcal{P}}$, and let $f \in \mathbb{K}$. Then

$$\mathrm{ord}_{\mathcal{P}}(\sigma(f)) = \mathrm{ord}_{\sigma^{-1}(\mathcal{P})}(f) = \mathrm{ord}_{\mathcal{P}}(f).$$

It follows that $\sigma(\mathcal{O}_{\mathcal{P}}) = \mathcal{O}_{\mathcal{P}}$ and $\sigma(\mathfrak{m}_{\mathcal{P}}) = \mathfrak{m}_{\mathcal{P}}$. Hence, $\sigma \in G_{\mathcal{P}}$ induces a well-defined automorphism of $\mathcal{O}_{\mathcal{P}}/\mathfrak{m}_{\mathcal{P}} = L(\mathcal{P})$ given by $\sigma(f + \mathfrak{m}_{\mathcal{P}}) = \sigma(f) + \mathfrak{m}_{\mathcal{P}}$. Since $L \subseteq L(\mathbb{P}^1)$ which is fixed by G, the automorphism on $L(\mathcal{P})$ induced by σ fixes L. We have now constructed a homomorphism $G_{\mathcal{P}} \to \mathrm{Aut}(L(\mathcal{P})/L)$. It turns out [30, Theorem III.8.2], since $\mathbb{K}/L(\mathbb{P}^1)$ is Galois, that $L(\mathcal{P})/L$ is Galois, and that the homomorphism constructed is in fact an isomorphism $G_{\mathcal{P}} \xrightarrow{\sim} \mathrm{Gal}(L(\mathcal{P})/L)$.

Now write $R = \eta_H(\mathcal{P})$. We would like to show that $\eta_H(R) \in D_H(L)$. It is enough to show that $g(R) \in L$ for all $g \in \mathcal{O}_R$. However, $g(R) = f(\mathcal{P})$, where $f = \eta_H^*(g) \in \mathcal{O}_{\mathcal{P}}$. Thus, we need to show that $f(\mathcal{P}) \in L$. This is equivalent to showing that $\sigma(f(\mathcal{P})) = f(\mathcal{P})$ for all $\sigma \in \mathrm{Gal}(L(\mathcal{P})/L)$, which is equivalent to showing that $\sigma(f + \mathfrak{m}_{\mathcal{P}}) = f + \mathfrak{m}_{\mathcal{P}}$ for all $\sigma \in G_{\mathcal{P}}$. However, by the construction of the function field of D_H, we see that $\sigma(f) = f$ for all $\sigma \in H \supseteq G_{\mathcal{P}}$. This completes the proof. □

Lemma 6.3. *Let $P \in C/K$ be a primitive degree n point, with $\varphi(P) = \alpha \in \mathbb{P}^1(K) - \mathrm{BV}(\varphi)$, and suppose $P \notin C(L)$. Let $P_1 = P, P_2, \ldots, P_n$ be the Galois orbit of P, and let*

$$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Sym}(\{P_1, \ldots, P_n\})$$

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

be the permutation representation obtained from the Galois action of $\mathrm{Gal}(\overline{K}/K)$ *on the orbit. Let* $I = \rho(\mathrm{Gal}(\overline{K}/K))$ *and* $J = \rho(\mathrm{Gal}(\overline{K}/L))$*; these are the Galois groups of* P *over* K *and* L*, respectively. Then the following hold.*

(i) *J is a nontrivial normal subgroup of I and is a transitive subgroup of* $\mathrm{Sym}(\{P_1, \dots, P_n\}) \cong S_n$.
(ii) *Let $\mathcal{P} \in \tilde{C}$ be above P. Then $G_{\mathcal{P}} \subseteq G$ is conjugate to J when both are regarded as subgroups of S_n.*
(iii) *There is some transitive subgroup H of G, conjugate to J in S_n, such that $R \in D_H(L)$ where $R = \eta_H(\mathcal{P})$.*

Proof. By assumption, $\rho(\mathrm{Gal}(\overline{K}/K))$ is a primitive subgroup of $\mathrm{Sym}(\{P_1, \dots, P_n\}) \cong S_n$. Since L/K is Galois, $J = \rho(\mathrm{Gal}(\overline{K}/L))$ is a normal subgroup of $\rho(\mathrm{Gal}(\overline{K}/K))$. By Lemma 2.3, the group $J \subset \mathrm{Sym}(\{P_1, \dots, P_n\})$ is either trivial or transitive. However, since $P \notin C(L)$, the group J is nontrivial and therefore transitive. This proves (i).

Recall that $\varphi(P) = \alpha \in \mathbb{P}^1(K) - \mathrm{BV}(\varphi)$. Since P has precisely n conjugates, and $\deg(\varphi) = n$, we see that the fibre $\varphi^*(\alpha)$ consists of $P_1, \dots, P_n$, each with multiplicity 1. By composing φ with a suitable automorphism of $\mathbb{P}^1$, we may suppose that $\alpha \in \mathbb{A}^1(K) = K$. We shall find it convenient to think of φ as an element of $K(C)$, and with this identification, we have $K(\mathbb{P}^1) = K(\varphi) \subseteq K(C)$. The extension $K(C)/K(\varphi)$ has degree n.

Write

$$\mathcal{O}_P = \{h \in K(C) \ : \ \mathrm{ord}_P(h) \geq 0\}, \qquad \mathfrak{m}_P = \{h \in K(C) \ : \ \mathrm{ord}_P(h) \geq 1\},$$

for the valuation ring of P and its maximal ideal. Then the residue field $\mathcal{O}_D/\mathfrak{m}_D$ can be identified with $K(P)$, where the identification is given by $g + \mathfrak{m}_D \mapsto g(P)$. Now fix $\theta \in K(P)$ such that $K(P) = K(\theta)$. Note that $[K(\theta) : K] = n$ since P has degree n. Then there is some $g \in \mathcal{O}_P$ such that $g(P) = \theta$. As $g \in K(C)$ and $K(C)$ has degree n over $K(\varphi)$, there is a polynomial $F(U, V) \in K[U, V]$,

$$F(U, V) = \sum_{i=1}^{m} a_i(V) U^i, \qquad a_i(V) \in K[V] \tag{6.4}$$

of degree $m \mid n$, such that $\gcd(a_0(V), \dots, a_m(V)) = 1$, and $F(g, \varphi) = 0$. Now, $F(\theta, \alpha) = F(g(P), \varphi(P)) = 0$, and so θ is a root of the polynomial $F(U, \alpha) \in K[U]$; this polynomial is nonzero as $\gcd(a_0(V), \dots, a_m(V)) = 1$. As θ has degree n over K, it follows that $m = n$, and that $F(U, V)$ is irreducible over $K(V)$. In particular, $F(U, V) = 0$ is a (possibly singular) plane model for C/K, and the map φ is given by $(u, v) \mapsto v$. As C is absolutely irreducible, $F(U, V)$ is irreducible over $\overline{K}$. Let $g_1 = g, g_2, \dots, g_n$ be the roots of $F(U, \varphi) = 0$ in $\mathbb{K}$; then $\mathbb{K} = K(\varphi)(g_1, \dots, g_n)$. In particular, $G' = \mathrm{Gal}(\mathbb{K}/K(C))$ may be identified as a transitive subgroup of $\mathrm{Sym}(g_1, \dots, g_n) \cong S_n$.

Let $\theta_1 = \theta, \theta_2, \dots, \theta_n$ be the roots of $F(U, \alpha) = 0$, which are distinct since $K(\theta)/K$ has degree n. We see that the affine plane model $F(U, V) = 0$ for C has n distinct points $(\theta_1, \alpha), \dots, (\theta_n, \alpha)$ above $\alpha \in \mathbb{P}^1$. However, the smooth model C has precisely n points $P_1, \dots, P_n$ above $\alpha \in \mathbb{P}^1$. After relabeling, we may identify $P_i = (\theta_i, \alpha)$. Next, we consider the action of $\mathrm{Gal}(\overline{K}/L)$ on $P_1, \dots, P_n$, and recall that $\alpha \in K \subseteq L$. It follows that J is conjugate to $\mathrm{Gal}(L(\theta_1, \dots, \theta_n)/L)$ when we consider J as a subgroup of $\mathrm{Sym}(\{P_1, \dots, P_n\}) \cong S_n$ and $\mathrm{Gal}(L(\theta_1, \dots, \theta_n)/L)$ as a subgroup of $\mathrm{Sym}(\{\theta_1, \dots, \theta_n\}) \cong S_n$.

Let $\mathcal{P}$ be a point of $\tilde{C}$ above P. Thus,

$$g_1(\mathcal{P}) = g(P) = \theta, \qquad \mu(\mathcal{P}) = \varphi(P) = \alpha \in K \subseteq L.$$

As in the proof of Lemma 6.2, the extension $L(\mathcal{P})/L$ is Galois. Since $\theta = g_1(\mathcal{P}) \in L(\mathcal{P})$, we see that $\theta_1, \dots, \theta_n \in L(\mathcal{P})$. In particular, for each i, there is an automorphism $\sigma \in L(\mathcal{P})/L$ such that $\sigma(\theta) = \theta_i$. Recalling the natural identification of $\mathrm{Gal}(L(\mathcal{P})/L)$ with $G_{\mathcal{P}}$, we see that there is an automorphism $\sigma' \in G_{\mathcal{P}}$ such that $\sigma'(g_1)(\mathcal{P}) = \sigma(\theta) = \theta_i$. However, $\sigma'(g_1)$ is a root of $F(U, \varphi)$ and is equal to one of the g_j. Thus, $g_i(\mathcal{P}) = \theta_i$, after suitably reordering $g_1, \dots, g_n$. Since $g_1, \dots, g_n$ generate $\mathbb{K}$, we

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

conclude that $L(\mathcal{P}) = L(\theta_1, \dots, \theta_n)$ and that $G_{\mathcal{P}}$ is conjugate to $\mathrm{Gal}(L(\theta_1, \dots, \theta_n)/L)$, which is in turn conjugate to J. This proves (ii).

Finally, letting $H = G_{\mathcal{P}}$, we deduce (iii) from Lemma 6.2. □

Of course, if $\mathrm{genus}(D_H) \geq 2$, then by Faltings' theorem, there are only finitely many $R \in D_H(L)$. The monodromy data for the morphism φ gives lower bounds for the genus of D_H. We shall make use of lower bounds due to Guralnick and Shareshian [15]. Fix an embedding $L \subset \overline{L} \subset \mathbb{C}$. Then φ induces an étale covering $C(\mathbb{C}) - \varphi^{-1}(\mathrm{BV}(\varphi)) \to \mathbb{P}^1(C) - \mathrm{BV}(\varphi)$ of Riemann surfaces. Since $\mathbb{K}/L(\mathbb{P}^1)$ is regular (i.e. $\mathbb{K} \cap \overline{L} = L$), we can identify $G = \mathrm{Gal}(\mathbb{K}/L(\mathbb{P}^1))$ with the image of the monodromy representation [25, Chapter 4] of this covering. Moreover, monodromy attaches (e.g., [25, Corollary 4.10]) elements

$$\sigma_1, \sigma_2, \dots, \sigma_r \in G - \{1\} \tag{6.5}$$

to the branch values $\mathrm{BV}(\varphi) = \{\beta_1, \beta_2, \dots, \beta_r\}$, satisfying

$$G = \langle \sigma_1, \dots, \sigma_r \rangle, \qquad \sigma_1 \sigma_2 \cdots \sigma_r = 1. \tag{6.6}$$

In this context, G is known as the monodromy group.

Theorem 6.4 (Guralnick and Shareshian). *Let $n \geq 5$. Let $\varphi : C \to \mathbb{P}^1$ be a morphism with monodromy group $G = A_n$ or S_n. Suppose, $\#\mathrm{BV}(\varphi) \geq 5$. Let $H \neq A_n$ be a maximal transitive subgroup of G. Then D_H has genus ≥ 3.*

Proof. For $n \geq 7$, this is a special case of Theorem 1.1.2 of [15], and for $n = 5, 6$ a special case of Corollary A.3.3 of the same paper. □

We note that Monderer and Neftin [26, Theorem 1.2] prove a stronger version of Theorem 6.4 that does not require the assumption of at least 5 branch points, but at the expense of assuming that $n > 3.5 \times 10^6$.

Remark. In the present context, the Riemann–Hurwitz formula, maybe restated (e.g., [22, Proposition 4.20]) as

$$\mathrm{genus}(D_H) = 1 - [G : H] + \frac{1}{2} \sum_{i=1}^{r} \mathrm{ind}(\sigma_i, G/H). \tag{6.7}$$

We explain the notation. Given a group G acting on a finite set Ω, and an element $g \in G$, we define the **index of** g to be $\mathrm{ind}(g, \Omega) := \#\Omega - \#\mathrm{Orb}(g, \Omega)$, where $\mathrm{Orb}(g, \Omega)$ is the set of orbits of g acting on Ω. We define the **minimal index of** G **acting on** Ω by

$$\mathrm{ind}(G, \Omega) := \min\{\mathrm{ind}(g, \Omega) \ : \ g \in G, \ g \neq 1\}.$$

Note that a large minimal index for the action of G on the coset space G/H, together with a sufficiently large number of branch points r, forces the genus of D_H to be large thanks to (6.7). A recent paper of Burness and Guralnick [6, Theorem 7] gives lower bounds for the minimal index for primitive actions, and in forthcoming work, we will use this to deduce a version of Theorem 6.4 for G other than A_n, S_n.

7. Proof of Theorem 1.2

In this section, we prove Theorem 1.2, which we now restate in a stronger but more technical form.

Theorem 7.1. *Let K be a number field. Let C/K be a curve of genus g, and write J for the Jacobian of C. Let $n \geq 2$ and suppose (1.1) holds. Suppose $W_n(C)$ does not contain the translate of an abelian subvariety A/K of J of positive rank. Suppose C has infinitely many degree n points with Galois group S_n or A_n. Then C has only finitely many degree n points with any primitive Galois group $\neq A_n, S_n$.*

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

We note that Theorem 1.2 follows from Theorem 7.1 thanks to the theorem of Debarre and Fahlaoui. It therefore remains to prove Theorem 7.1. We note that S_n has no proper primitive subgroups $\neq A_n$ for $n \leq 4$. Thus, we may suppose that $n \geq 5$.

Let K be a number field and let C/K be a curve of genus g. Let $n \geq 5$ and suppose $g > (n-1)^2$. Suppose $A(K)$ is finite for any abelian subvariety A/K of J having a translate contained in $W_n(C)$. Suppose C has infinitely many degree n points with Galois group A_n or S_n. By Theorem 5.1, there is a degree n morphism $\varphi : C \to \mathbb{P}^1$ such that all but finitely many primitive degree n divisors are fibres $\varphi^*(\alpha)$ with $\alpha \in \mathbb{P}^1(K)$. Thus, to prove Theorem 1.2, we need to show that there are at most finitely many $\alpha \in \mathbb{P}^1(K) - \mathrm{BV}(\varphi)$ such that the Galois group of the fibre $\varphi^*(\alpha)$ is primitive but not A_n, S_n.

As in Section 6, we write $\mathbb{K}$ for the Galois closure of the function field extension $K(C)/K(\mathbb{P}^1)$ induced by φ, and we let $G' = \mathrm{Gal}(\mathbb{K}/K(\mathbb{P}^1))$. As φ has degree n, we may identify G' as a subgroup of S_n.

Lemma 7.2. *$G' = A_n$ or S_n.*

Proof. There infinitely many fibres $\varphi^*(\alpha)$ with $\alpha \in \mathbb{P}^1(K) - \mathrm{BV}(\varphi)$ that have Galois group A_n or S_n. Choose such an α, let $P \in \varphi^*(\alpha)$; thus, the Galois group of the Galois closure of the extension $K(P)/K$ has Galois group S_n or A_n. Moreover, $P \in C$ is a degree n point, and we regard it as a degree n place of $K(C)$. We let $\mathcal{P}$ be a place of $\mathbb{K}$ above P. By Lemma 6.1, the extension $K(\mathcal{P})/K$ is Galois, and its Galois group is isomorphic to the decomposition group $G'_{\mathcal{P}} \subseteq G'$. However, $K(P) \subseteq K(\mathcal{P})$ and the Galois group of the Galois closure of $K(P)/K$ is either A_n or S_n. It follows that $G' = A_n$ or S_n. □

Lemma 7.3. *Let $r = \#\mathrm{BV}(\varphi)$. Then $r \geq 2n+1$.*

Proof. Write $\mathrm{BV}(\varphi) = \{\beta_1, \ldots, \beta_r\}$. We make use of the Riemann–Hurwitz formula applied to φ. Thus,

$$2g - 2 \;=\; -2n + \sum_{i=1}^{r} \sum_{P \in \varphi^*(\beta_i)} e(P) - 1 \;\leq\; -2n + r(n-1).$$

However, $g \geq (n-1)^2 + 1$. Putting these together gives

$$r \;\geq\; 2(n-1) + \frac{2n}{n-1} \;>\; 2n.$$

□

As in Section 6, let $L = \mathbb{K} \cap \overline{K}$, and recall that L/K is a finite Galois extension. Let $G = \mathrm{Gal}(\mathbb{K}/L(\mathbb{P}^1))$.

Lemma 7.4.

(a) *Suppose $G' = A_n$. Then $L = K$ and $G = A_n$.*
(b) *Suppose $G' = S_n$. Then*
  (i) *either $L = K$ and $G = S_n$,*
  (ii) *or L/K is quadratic and $G = A_n$.*

Proof. As φ is ramified, the extension $\mathbb{K}/L(\mathbb{P}^1)$ is non-trivial. Therefore, by the exactness of (6.1), the group G is a nontrivial normal subgroup of G'. As $n \geq 5$, the only nontrivial normal subgroup of A_n is A_n, and the only nontrivial normal subgroups of S_n are S_n and A_n. The lemma follows. □

We now complete the proof of Theorem 7.1. As observed at the beginning of the section, we need to show that there are at most finitely many $\alpha \in \mathbb{P}^1(K) - \mathrm{BV}(\varphi)$ such that the Galois group of the fibre $\varphi^*(\alpha)$ is primitive but not A_n, S_n. It is therefore enough, for each primitive subgroup $I \subset G'$, with $I \neq A_n$, S_n, to show that there are finitely many $\alpha \in \mathbb{P}^1(K) - \mathrm{BV}(\varphi)$ such that the fibre $\varphi^*(\alpha)$ has Galois group I. Fix a primitive subgroup $I \subset G'$, $I \neq A_n$, S_n, and suppose there are infinitely many $\alpha \in \mathbb{P}^1(K) - \mathrm{BV}(\varphi)$ such that the fibre $\varphi^*(\alpha)$ has Galois group I. Since $C(L)$ is finite by Faltings' theorem, only finitely many of these fibres contain a point of $C(L)$. Thus, for infinitely many of the fibres, there is a primitive degree n point $P \in C - C(L)$ whose Galois group is I. There are finitely many

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

possibilities for the groups J, H in Lemma 6.3. As $I \neq A_n, S_n$, by the lemma, $H \neq A_n, S_n$ is a transitive subgroup of G. If $H \subset A_n$, then let H' be a maximal subgroup of A_n containing H. If $H \not\subset A_n$, then in this case, $G = S_n$, and we let H' be a maximal subgroup of S_n containing H, and note that $H' \neq A_n$. As $H \subseteq H'$, we have $\mathbb{K}^{H'} \subseteq \mathbb{K}^H$, and so the map $\pi_H : D_H \to \mathbb{P}^1$ factors via the map $\pi_{H'} : D'_H \to \mathbb{P}^1$. In particular, by Theorem 6.4 (applied with H' in place of H), the curve $D_{H'}$ has genus ≥ 2, and therefore, so does the curve D_H. Therefore, $D_H(L)$ is finite. This gives a contradiction and completes the proof.

Acknowledgements. We are grateful to Gareth Tracey for useful discussions and for drawing our attention to the work of Burness and Guralnick [6] on minimal indices. We thank Martin Derickx for useful remarks on a previous version of this paper. We are indebted to the referees for many pertinent comments, corrections and improvements, which have substantially enhanced the paper, and for drawing our attention to the paper of Guralnick and Shareshian [15].

Competing interest. The authors have no competing interest to declare.

Funding statement. Khawaja is supported by an EPSRC studentship from the University of Sheffield (EP/T517835/1). Siksek is supported by the EPSRC grant *Moduli of Elliptic Curves and Classical Diophantine Problems* (EP/S031537/1).

Data availability statement. There is no data associated to this paper.

References

[1] E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of Algebraic Curves. Vol.* I (Springer-Verlag, New York, 1985).
[2] A. Bourdon, O. Ejder, Y. Liu, F. Odumodu and B. Viray, 'On the level of modular curves that give rise to isolated j-invariants', *Adv. Math.* **357** (2019), 106824, 33.
[3] M. Bright and S. Siksek, 'Functions, reciprocity and the obstruction to divisors on curves', *J. Lond. Math. Soc. (2)* **77**(3) (2008), 789–807.
[4] P. Bruin, M. Derickx and M. Stoll, 'Elliptic curves with a point of order 13 defined over cyclic cubic fields', *Funct. Approx. Comment. Math.* **65**(2) (2021), 191–197.
[5] P. Bruin and F. Najman, 'Fields of definition of elliptic curves with prescribed torsion', *Acta Arith.* **181**(1) (2017), 85–95.
[6] T. C. Burness and R. M. Guralnick, 'Fixed point ratios for finite primitive groups and applications', *Adv. Math.* **411** (2022), Paper No. 108778, 90.
[7] O. Debarre and R. Fahlaoui, 'Abelian varieties in $W^r_d(C)$ and points of bounded degree on algebraic curves', *Compos. Math.* **88**(3) (1993), 235–249.
[8] M. Derickx, 'A-gonalities and algebraic points on curves', to appear.
[9] M. Derickx, 'Large degree primitive points on curves', Preprint, 2024, https://arxiv.org/abs/2409.05796.
[10] M. Derickx, S. Kamienny, W. Stein and M. Stoll, 'Torsion points on elliptic curves over number fields of small degree', *Algebra Number Theory* **17**(2) (2023), 267–308.
[11] M. Derickx and F. Najman, 'Torsion of elliptic curves over cyclic cubic fields', *Math. Comp.* **88**(319) (2019), 2443–2459.
[12] J. D. Dixon and B. Mortimer, *Permutation Groups* (Graduate Texts in Mathematics) vol. 163 (Springer-Verlag, New York, 1996).
[13] G. Faltings, 'The general case of S. Lang's conjecture', in *Barsotti Symposium in Algebraic Geometry* (Abano Terme, 1991) (Perspect. Math) vol. 15 (Academic Press, San Diego, CA, 1994), 175–182.
[14] G. Frey, 'Curves with infinitely many points of fixed degree', *Israel J. Math.* **85**(1–3) (1994), 79–83.
[15] R. M. Guralnick and J. Shareshian, 'Symmetric and alternating groups as monodromy groups of Riemann surfaces. I. Generic covers and covers with many branch points', *Mem. Amer. Math. Soc.* **189**(886) (2007), vi+128. With an appendix by Guralnick and R. Stafford.
[16] J. Harris and J. Silverman, 'Bielliptic curves and symmetric products', *Proc. Amer. Math. Soc.* **112**(2) (1991), 347–356.
[17] R. Hartshorne, *Algebraic Geometry* (Graduate Texts in Mathematics) no. 52 (Springer-Verlag, New York-Heidelberg, 1977).
[18] D. Jeon, 'Families of elliptic curves over cyclic cubic number fields with prescribed torsion', *Math. Comp.* **85**(299) (2016), 1485–1502.
[19] D. Jeon, C. H. Kim and Y. Lee, 'Families of elliptic curves with prescribed torsion subgroups over dihedral quartic fields', *J. Number Theory* **147** (2015), 342–363.
[20] B. Kadets and I. Vogt, 'Subspace configurations and low degree points on curves', Preprint, 2022. https://arxiv.org/abs/2208.01067.
[21] M. Khawaja and S. Siksek, 'Primitive algebraic points on curves', *Res. Number Theory* **10**(3) (2024), Paper No. 57.
[22] D. Lombardo, E. Lorenzo García, C. Ritzenthaler and J. Sijsling, 'Decomposing Jacobians via Galois covers', *Exp. Math.* **32**(1) (2023), 218–240.
[23] L. Merel, 'Bornes pour la torsion des courbes elliptiques sur les corps de nombres', *Invent. Math.* **124**(1–3) (1996), 437–449.
[24] J. S. Milne, 'Jacobian varieties', in *Arithmetic Geometry (Storrs, Conn., 1984)* (Springer, New York, 1986), 167–212.

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press

[25] R. Miranda, *Algebraic Curves and Riemann Surfaces* (Graduate Studies in Mathematics) vol. 5 (American Mathematical Society, Providence, RI, 1995).
[26] T. Monderer and D. Neftin, 'Symmetric Galois groups under specialization', *Israel J. Math.* **248**(1) (2022), 201–227.
[27] J.-P. Serre, *Topics in Galois Theory* (Research Notes in Mathematics) vol. 1, second edn. (A K Peters, Ltd., Wellesley, MA, 2008). With notes by Henri Darmon.
[28] S. Siksek, 'Chabauty for symmetric powers of curves', *Algebra Number Theory* **3**(2) (2009), 209–236.
[29] G. Smith and I. Vogt, 'Low degree points on curves', *Int. Math. Res. Not. IMRN* **1** (2022), 422–445.
[30] H. Stichtenoth, *Algebraic Function Fields and Codes* (Graduate Texts in Mathematics) vol. 254, second edn. (Springer-Verlag, Berlin, 2009).
[31] B. Viray and I. Vogt, 'Isolated and parameterized points on curves', Preprint, 2024, https://arxiv.org/abs/2406.14353.

https://doi.org/10.1017/fms.2024.156 Published online by Cambridge University Press