Mathematische Annalen (2024) 389:1–62
https://doi.org/10.1007/s00208-023-02638-2

Mathematische Annalen

Unlikely intersections and the Chabauty–Kim method over number fields

Netan Dogra[1]

Received: 14 March 2022 / Revised: 24 December 2022 / Accepted: 29 April 2023 /
Published online: 24 May 2023

Abstract

The Chabauty–Kim method is a tool for finding the integral or rational points on varieties over number fields via certain transcendental p-adic analytic functions arising from certain Selmer schemes associated to the unipotent fundamental group of the variety. In this paper we establish several foundational results on the Chabauty–Kim method for curves over number fields. The two main ingredients in the proof of these results are an unlikely intersection result for zeroes of iterated integrals, and a careful analysis of the intersection of the Selmer scheme of the original curve with the unipotent Albanese variety of certain $\mathbb{Q}_p$-subvarieties of the restriction of scalars of the curve. The main theorem also gives a partial answer to a question of Siksek on Chabauty's method over number fields, and an explicit counterexample is given to the strong form of Siksek's question.

Contents

✉ Netan Dogra
netan.dogra@kcl.ac.uk

[1] King's College London, London, UK

1 Introduction

Let X be a hyperbolic curve over a number field K. Then, by a theorem of Siegel in the case X is affine [49] and by Faltings [20] in general, X has only finitely many integral points. Both these proofs are *ineffective*, in the sense that they do not give a way to determine the set of integral points. The Chabauty–Kim method seeks to give a method for determining this set of points, by constructing a set of p-adic points containing the integral points, which one can prove is finite and compute in practice. Before explaining the Chabauty–Kim method more precisely, we clarify what we mean by integral points. Let $\overline{X}$ be a smooth projective curve over K, with $X \subset \overline{X}$ and complement $D := \overline{X} - X$. We assume that X is hyperbolic, i.e. that $2g(\overline{X}) + \#D(\overline{K}) > 2$. Let $\overline{\mathcal{X}}$ be a regular model of $\overline{X}$ over $\mathcal{O}_{K,S}$, for S a finite set of primes, $\mathcal{D} \subset \overline{\mathcal{X}}$ a normal crossings divisor with generic fibre equal to D, and $\mathcal{X} := \overline{\mathcal{X}} - \mathcal{D}$. Then the theorems of Faltings and Siegel imply that $\mathcal{X}(\mathcal{O}_{K,S})$ is finite.

Let p be a prime which splits completely in K and which is a prime of good reduction for $\mathcal{X}$ (henceforth when we say that a rational prime is a prime of good reduction for $\mathcal{X}$, we will mean that for all $v|p$, v is not in S, $\overline{X}$ has good reduction at v and $\mathcal{D}$ is étale over $\mathcal{O}_{K_v}$). Then Kim's method produces nested subsets $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ and $\mathcal{X}(\mathcal{O}_{K_v})_{S,n}$ of $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) = \prod_{v|p} \mathcal{X}(\mathcal{O}_{K_v})$ and $\mathcal{X}(\mathcal{O}_{K_v})$ respectively, each containing the S-integral points of $\mathcal{X}$:

$$\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) \supset \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,1} \supset \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,2} \supset \cdots \supset \mathcal{X}(\mathcal{O}_{K,S}),$$
$$\mathcal{X}(\mathcal{O}_{K_v}) \supset \mathcal{X}(\mathcal{O}_{K_v})_{S,1} \supset \mathcal{X}(\mathcal{O}_{K_v})_{S,2} \supset \cdots \supset \mathcal{X}(\mathcal{O}_{K,S}).$$

When S is empty, these sets will be written simply as $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_n$ and $\mathcal{X}(\mathcal{O}_{K_v})_n$, and in the case $X = \overline{X}$ is projective, they will be written simply as $X(K \otimes \mathbb{Q}_p)_n$ and $X(K_v)_n$. A detailed description of $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ and $\mathcal{X}(\mathcal{O}_{K_v})_{S,n}$ is given in Sect. 3.1. A valuable feature of the Chabauty–Kim method is that the sets $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ and $\mathcal{X}(\mathcal{O}_{K_v})_{S,n}$ are often computable in practice, and can be used to determine $\mathcal{X}(\mathcal{O}_{K,S})$ (see e.g. [4, 6, 15, 16]).

In this paper we establish foundational results about the scope of the Chabauty–Kim method over number fields, by establishing when we should expect the sets $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ to be finite. The algorithmic side of the Chabauty–Kim method has also been developed in certain cases in depths one (see for example [50]) and two [3], and hence these results also suggest that the Chabauty–Kim method may be a practical method for the determination of rational points on hyperbolic curves of small genus over number fields.

1.1 Main results

The main result of this paper is that, essentially, the status of the Chabauty–Kim method over arbitrary number fields is the same as that over $\mathbb{Q}$. More precisely, we show that the Chabauty–Kim sets $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ are finite under the same sets of hypotheses as those needed over $\mathbb{Q}$. As we explain below, the proofs of these results are however quite different from their analogues over $\mathbb{Q}$.

Theorem 1.1 *Let K be a number field, and p a (rational) prime which splits completely in K, and S a finite set of primes disjoint from K. Then $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ is finite for all $n \gg 0$ in each of the following cases.*

(1) *$X = \mathbb{P}^1 - D$, where $D \subset \mathbb{P}^1_K$ is a closed subscheme with $\#D(\overline{K}) > 2$.*
(2) *X/K is a smooth projective curve of genus $g > 1$, and the conjecture of Jannsen, or the conjecture of Bloch–Kato, hold for all the product varieties X^n.*

In each of the following cases, there exists a finite extension $L|K$, such that for all rational primes p which split completely in L, there is a prime v of K above p such that $\mathcal{X}(\mathcal{O}_{K_v})_{S,n}$ is finite for all $n \gg 0$.

(3) *$X = E - O$, where E/K is an elliptic curve with complex multiplication.*
(4) *X/K is a smooth projective curve of genus $g > 1$ whose Jacobian is geometrically simple and has complex multiplication.*

Remark 1.1 The last two cases of Theorem 1.1 involve two conditions on the primes involved, which were erroneously not included in a previous version of this paper. The first, that of restricting to a positive proportion of primes, already occurs in the original work of Kim and Coates–Kim, since they require p to split completely in the CM field by which the Jacobian has complex multiplication. It also occurs in our work because we pass to a finite extension of K, and require p to split completely in that. The condition of only working with one prime above p seems difficult to remove without a deeper understanding of localisation maps in Galois cohomology.

Remark 1.2 When $K = \mathbb{Q}$, Theorem 1.1 is already known: cases (1), (2) and (3) are due to Kim [35–37]. Case (4) is due to Coates and Kim [13]. As in Ellenberg and Hast [19] this implies finiteness of $X(K_v)_n$ for any curve X which geometrically dominates a hyperbolic curve with geometrically simple CM Jacobian (since we prove finiteness over all number fields, we can just pass to a finite extension over which the cover is defined, and note that for a cover $X \to Y$, finiteness of $Y(K_v)_n$ implies finiteness of $X(K_v)_n$). In particular, it implies finiteness of $X(K)$ for all hyperelliptic curves X and number fields K.

When K is totally real, case (1) was proved independently by Hadian [26] and Kim [38].

Remark 1.3 As explained below, the main input into the proof of Theorem 1.1 is an unlikely intersection result (Proposition 4.1) for Kim's unipotent Albanese morphism. The idea of relating unlikely intersections to the Chabauty–Kim method also appears in the thesis of Daniel Hast [30, §5], where he shows that, when K has a real place, case (2) (assuming Bloch–Kato) and case (4) of the above theorem are implied by a sufficiently strong unlikely intersection result [30, Conjecture 5.1], which is a generalisation of a question of Siksek on Chabauty's method over number fields. In Sect. 2.2, we give a counterexample to this strong unlikely intersection result, which also provides a negative answer to Siksek's question.

Hast has independently obtained related results pertaining to the relationship between the Chabauty–Kim method and generalisations of the Ax–Schanuel theorem [31]. Rather than proving finiteness of $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$, Hast gives a Chabauty–Kim proof of finiteness of the set $\mathcal{X}(\mathcal{O}_{K,S})$ of integral points, assuming Klingler's Ax–Schanuel conjecture [40, Conjecture 7.5] for variations of mixed Hodge structure, as well as the assumptions in (1) to (4). The point of divergence in proving finiteness of $\mathcal{X}(\mathcal{O}_{K,S})$ rather than $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ or $\mathcal{X}(\mathcal{O}_{K,v})_{S,n}$ is that, in both proofs, one wants to prove finiteness of the Zariski closure of a set of points (either $\mathrm{Res}_{K|\mathbb{Q}}(X)(\mathbb{Q})$ or $\mathrm{Res}_{K|\mathbb{Q}}(X)(\mathbb{Q}_p)_n$) by considering its image under the unipotent Albanese morphism and intersecting with a Selmer scheme. Whilst the former descends to $\mathbb{Q}$, the latter will in general just be defined over $\mathbb{Q}_p$—this phenomenon already occurs in the case of Chabauty's method over $\mathbb{Q}$, where the set $X(\mathbb{Q}_p)_1$ would be expected to typically contain non-algebraic points even when it is finite. We elaborate on the issue of fields of definition in the subsequent subsection.

Remark 1.4 It would be interesting to adapt the proof of Theorem 1.1 to give a method for determining the rational points on more general higher dimensional varieties which have non-abelian unipotent fundamental groups. For example, can one apply the Chabauty–Kim method to determine the rational points on some of the higher dimensional Shimura varieties considered by Dimitrov and Ramakrishnan in [18]?

1.2 Unlikely intersections and fields of definition

The main new result used in the proof of Theorem 1.1 is a way of understanding the zeroes of certain transcendental functions (iterated integrals) on higher dimensional varieties. Kim's method works by constructing, under certain Galois cohomological assumptions, certain nontrivial locally analytic transcendental (Coleman) functions on $\prod_{v|p} \mathcal{X}(\mathcal{O}_v)$ whose zero locus contains $\mathcal{X}(\mathcal{O}_{K,S})$. Since Coleman functions have only finitely many zeroes on $\mathcal{X}(\mathbb{Z}_p)$, this proves finiteness when $K = \mathbb{Q}$.

Over number fields, $\prod_{v|p} \mathcal{X}(\mathcal{O}_v)$ is no longer one dimensional and hence the problem is to rule out that these functions conspire to have many zeroes in common. In this paper we resolve this problem by proving a foundational result (Proposition 4.1) on unlikely intersections for iterated integrals. In the abelian case, the main unlikely inter-

section result (Proposition 4.1) is a straightforward consequence of the Ax–Schanuel theorem for abelian varieties.

To describe how such unlikely intersections can occur, consider the case of the product of $\mathbb{P}^1 - \{0, 1, \infty\}$ with itself, with co-ordinate functions z_1, z_2. Then the Coleman functions $\log(z_1) - \log(z_2)$ and $\log(1 - z_1) - \log(1 - z_2)$ are independent, in a suitable sense, but their common zero set is not codimension 2, as it contains the diagonal. The zero locus is not Zariski dense, however. A rather complicated way of seeing this is to observe that, on any positive dimensional component of the zero locus, $\frac{dz_1}{z_1} - \frac{dz_2}{z_2}$ and $\frac{dz_1}{1-z_1} - \frac{dz_2}{1-z_2}$ are colinear. Hence such a component must be contained in the subspace

$$z_1(z_2 - 1) = z_2(z_1 - 1).$$

In this paper we show that unlikely intersections of this form are, in some sense, the only thing that can go wrong. More precisely, in Proposition 4.1 we prove the following Ax–Schanuel-type statement for iterated integrals: if the codimension of the zero set of a set of iterated integral functions on a smooth geometrically connected quasi-projective variety is 'smaller than expected', then this zero set is not Zariski dense in the subvariety. The method of proof is an elaborate version of the example above, inspired by Ax's original proof of the Ax–Schanuel theorem for tori and abelian varieties. A similar strategy is used by Blázquez-Sanz, Casale, Freitag and Nagloo [7], where a stronger and vastly more general Ax–Schanuel type theorem is proved used a suitable nonabelian generalisation of Ax's proof. Indeed, their work, specialised to the specific context of unipotent connections on products of curves, gives an elegant conceptual explanation for some of the more elaborate (and apparently unmotivated) calculations in Sect. 4. Although their argument is phrased in the language of connections on principal bundles for varieties over the complex numbers, standard arguments show their results imply unlikely intersection results for Coleman integrals. This will be pursued further in a subsequent work.

The second difficulty is establishing the existence of non-trivial Coleman functions vanishing on $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$. In the case $K = \mathbb{Q}$, by a theorem of Kim this is proved by showing that a localisation map from a Selmer scheme to local Galois cohomology variety is not dominant (this is a nonabelian, Galois cohomological analogue of the fact that Chabauty's method depends on showing that the rank of the Jacobian is less than the genus). In the Chabauty–Kim method over $\mathbb{Q}$ non-dominance is typically proved via (often conjectural) dimension bounds on certain Bloch–Kato Selmer groups associated to the étale fundamental groups of $X_{\overline{K}}$. Using Proposition 4.1, we are then able to deduce Zariski non-density results for $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ from results on dimension bounds on certain Bloch–Kato Selmer groups. To prove finiteness results, we argue by contradiction, assuming that $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ is infinite, and taking Z to be its Zariski closure. To apply the unlikely intersection result via the Chabauty–Kim method, we have to bound the intersection of Selmer groups associated to the fundamental group of the Weil restriction $\mathrm{Res}_{K|\mathbb{Q}} X_{\overline{\mathbb{Q}}}$ with local Galois cohomology groups associated to fundamental group of the $Z_{\overline{\mathbb{Q}}_p}$.

Since the unipotent fundamental group of $Z_{\overline{\mathbb{Q}}_p}$ need not surject onto that of $\mathrm{Res}_{K|\mathbb{Q}} X_{\overline{\mathbb{Q}}}$, we are compelled to study a slightly novel local–global problem in Galois cohomology. Instead of needing to bound the image of the Bloch–Kato Selmer group of a global Galois representation V in the local Galois cohomology of V, we need to bound the *intersection* of the image of the Bloch–Kato Selmer group of V with that of the local Galois cohomology of a subspace $W \subset V$ which is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$, but which need not be stable under $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$. This is done in several stages. First, although we cannot assume that Z descends to a number field, we can descend the image of its Albanese variety in that of the Weil restriction of X (see Lemma 5.5), and we know that the Albanese of Z must surject onto the Jacobian of one of the factors of $\mathrm{Res}_{K|\mathbb{Q}}(X)$. For case (2), we then use this to show that there are pieces of the fundamental group of $\mathrm{Res}_{K|\mathbb{Q}}(X)$ whose global Galois cohomology cannot contain the fundamental group. Because our assumptions in this case imply strong bounds on the relevant H^2 groups, this suffices by standard duality arguments to prove finiteness.

For cases (3) and (4), this is not enough, because our unconditional bounds on H^2 in this case are weaker. This is why we instead prove finiteness of $X(\mathcal{O}_{K_v})_{S,n}$ for some v above p. To explain how this simplifies the proof, consider the case where, for all distinct embeddings $\sigma_1, \sigma_2 : K \to \overline{K}$, $\mathrm{Hom}(\mathrm{Alb}(X_{\overline{K},\sigma_1}), \mathrm{Alb}(X_{\overline{K},\sigma_2})) = 0$. Then, up to isogeny, the image of the unipotent fundamental group of X in the fundamental group of $\mathrm{Res}(X)$ is the product of the images in the individual factors of $\mathrm{Res}(X)$. This allows us to reduce to the case where the image is very large. On the other hand, if $K|\mathbb{Q}$ is Galois and X is defined over $\mathbb{Q}$, then there is an action of $\mathrm{Gal}(K|\mathbb{Q})$ on the Galois cohomology over K of the fundamental group of X. This gives an additional structure to show that the Galois cohomology of the fundamental group of $Z/\mathbb{Q}_p$ is not contained in the global Galois cohomology of the fundamental group of $\mathrm{Res}(X)$. In cases (3) and (4) we interpolate between these two techniques, using our strong assumptions on the Jacobian of X.

1.3 Applications to explicit Chabauty–Kim

Theorem 1.1 guarantees that the algorithms of Dan-Cohen–Wewers, Dan-Cohen and Corwin–Dan-Cohen [14–16] for computing $\mathcal{O}_{K,S}$-points on $\mathbb{P}^1 - \{0, 1, \infty\}$ provably produce finite sets, extending the theoretical scope of the algorithms beyond totally real fields. To use the Chabauty or Chabauty–Kim method to determine $X(K)$ for X of genus bigger than one, at present one typically needs finiteness of $X(K \otimes \mathbb{Q}_p)_n$ when $n = 1$ or 2. When $K = \mathbb{Q}$, the foundational work of Chabauty implies that $X(\mathbb{Q}_p)_1$ is finite if $r < g$, where r is the Mordell–Weil rank of the Jacobian of X, and g is the genus. The 'quadratic Chabauty lemma' [4, Lemma 3.2] states that $X(\mathbb{Q}_p)_2$ is finite when $r < g + \rho(\mathrm{Jac}(X)) - 1$, where $\rho(\mathrm{Jac}(X))$ denotes the rank of the Neron–Severi group of $\mathrm{Jac}(X)$ (over $\mathbb{Q}$). We prove a partial generalisation of this result to number fields. We also give sufficient conditions for finiteness of $X(K \otimes \mathbb{Q}_p)_1$, providing a partial answer to a question of Siksek (see below). The latter result, which can be phrased purely in terms of the classical Chabauty–Coleman method, is proved

separately in Sect. 2, although it is also a special case of the more general results obtained later in the paper.

Proposition 1.1 *Let $K|\mathbb{Q}$ be a finite extension of degree d, and let $r_1(K)$ and $r_2(K)$ denote the number of real and complex places. Let $P_{\mathbb{R}}$ denote the set of real places of K, and for each $v \in P_{\mathbb{R}}$, let $c_v \in G_K$ denote complex conjugation with respect to an embedding $\overline{K} \hookrightarrow \mathbb{C}$ extending v. Let X/K be a smooth projective geometrically integral curve of genus $g > 1$, and let p be a prime which splits completely in K and such that, for all $v|p$, X has good reduction at v. Let r denote the rank of* $\mathrm{Jac}(X)(K)$. *Suppose that for any two distinct embeddings $\sigma_1, \sigma_2 : K \hookrightarrow \overline{\mathbb{Q}}$, we have* $\mathrm{Hom}(\mathrm{Jac}(X)_{\overline{\mathbb{Q}},\sigma_1}, \mathrm{Jac}(X)_{\overline{\mathbb{Q}},\sigma_2}) = 0$. *Then we have the following finiteness results.*

(1) *If $r \leq d(g-1)$, then for all primes p of good reduction and splitting completely in K, there is a prime v of K lying above p such that $X(K_v)_1$ is finite.*

(2) *If* $\mathrm{rk}\, H^1_f(G_{K,T}, T_p(\mathrm{Jac}(X))) \otimes \mathbb{Q}_p) \leq d(g-1) + (r_2(K)+1)(\rho(\mathrm{Jac}(X)) - 1) + \sum_{v \in P_{\mathbb{R}}} \rho(J_{\mathbb{C},v}) - \rho(J_{\mathbb{R},v})$

then for all primes p as in part (1), there is a prime v above p such that $X(K_v)_2$ is finite.

Remark 1.5 Assuming the finiteness of the p-primary part of the Tate–Shafarevich group for $(\mathrm{Jac}(X)$, we have $\mathrm{rk}\, H^1_f(G_{K,T}, T_p(\mathrm{Jac}(X)) \otimes \mathbb{Q}_p) = \mathrm{rk}\, \mathrm{Jac}(X)(K)$. By modifying the definition of the Selmer scheme as in [4, Definition 2.2] to include a condition on mapping to $J(K) \otimes \mathbb{Q}_p$, (condition (c) of [4, Definition 2.2]), one can prove finiteness of a modified version of $X(K_v)_2$, for v as above, whenever

$$r \leq d(g-1) + (r_2(K)+1)(\rho(\mathrm{Jac}(X)) - 1) + \sum_{v \in P_{\mathbb{R}}} \rho(J_{\mathbb{C},v}) - \rho(J_{\mathbb{R},v})$$

(still assuming $\mathrm{Hom}(\mathrm{Jac}(X)_{\overline{\mathbb{Q}},\sigma_1}, \mathrm{Jac}(X)_{\overline{\mathbb{Q}},\sigma_2}) = 0$ for all $\sigma_1 \neq \sigma_2$). This modified version of the Selmer scheme is also easier to compute with (see [4]) but as this distinction is not needed elsewhere in the paper, we use the simpler definition.

In the case $K = \mathbb{Q}$, case (2) of Proposition 1.1 is in fact more general than the quadratic Chabauty lemma [4, Lemma 3.2] mentioned above. Instead it reduces to [5, Proposition 2], which states that $X(\mathbb{Q}_p)_2$ is finite whenever

$$\mathrm{rk}(J) < g - 1 + \rho(J) + \mathrm{rk}(\mathrm{NS}(J_{\overline{\mathbb{Q}}})^{c=-1}),$$

where J is Jacobian of X, and $c \in \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ is a complex conjugation.

Although the condition on $\mathrm{Hom}(\mathrm{Jac}(X)_{\overline{\mathbb{Q}},\sigma_1}, \mathrm{Jac}(X)_{\overline{\mathbb{Q}},\sigma_2})$ is generic when X is not defined over a subfield of K, and is practical to check for curves of small genus and number fields of low degree, it is natural to wonder whether a weaker condition is sufficient. There are known examples where $X(K \otimes \mathbb{Q}_p)_1$ is infinite and $r = d(g-1)$

coming from the fact that X descends to a subfield of $K|\mathbb{Q}$. In [50], Siksek asks whether a sufficient condition for finiteness of $X(K \otimes \mathbb{Q}_p)_1$ is that $r \leq d(g-1)$ and X is not defined over any intermediate extension of $K|\mathbb{Q}$. In Sect. 2, we show that this question has a negative answer, but it is not clear that the condition that we obtain is optimal.

Remark 1.6 In the case when K is an imaginary quadratic field, Proposition 1.1 (modified as in the above remark) implies that $X(K_v)_2$ is finite whenever $\mathrm{rk}\, J(K) \leq 2g$ and $\rho(J) > 1$, which has applications to the scope of the algorithms developed by Balakrishnan, Besser, Bianchi and Müller [3].

1.4 Notation and plan of the paper

In Sect. 2, we explain the relation between the application of the Ax–Schanuel theorem to questions on Chabauty's method over number fields. Although the main result is essentially a special case of results proved later in the paper, we give an independent exposition that involves none of the machinery from Kim's method. We hope this may be of independent interest, and provide an illustration of how unlikely intersection results imply finiteness of Chabauty–Kim sets. In Sect. 3, we provide a brief recap on the Chabauty–Kim method over $\mathbb{Q}$ and over number fields. We also explain how the Chabauty–Kim method for X/K is related to the Chabauty–Kim method for $\mathrm{Res}_{K|\mathbb{Q}}(X)/\mathbb{Q}$, where $\mathrm{Res}_{K|\mathbb{Q}}(X)$ denotes the Weil restriction of X (following an analogous construction of Stix, in the context of the section conjecture, in [52]). In Sect. 3.5, we recall the explicit description of the p-adic iterated integrals (or more precisely, the unipotent connections) which arise in Kim's method given in [36]. This enable us to reduce the unlikely intersection statement required to a statement about zeroes of iterated integrals. In Sect. 4, we then prove the unlikely intersection result, following the strategy outlined above. In 5, we describe how to reduce the proof of finiteness of $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ to specific inequalities for the dimension of (abelian) Galois cohomology groups. In Sect. 6 we complete the proof of Theorem 1.1 by verifying these inequalities.

The following notation will be used throughout the paper. If X is a rigid analytic space over $\mathbb{Q}_p$ with formal model $\mathcal{X}$, then, for any subscheme Y of the special fibre $\mathcal{X}_{\mathbb{F}_p}$, we denote by $]Y[\subset X$ the *tube* of Y in the sense of Berthelot. This is a rigid analytic space whose $\mathbb{Q}_p$-points are exactly the $\mathbb{Q}_p$-points of X which reduce to $Y(\mathbb{F}_p)$ modulo p. When Y is an $\mathbb{F}_p$-point of X, we refer to $]Y[$ as a residue disk. If X and Y are rigid analytic spaces over $\mathbb{Q}_p$, and X has a fixed formal model $\mathcal{X}$, a *locally analytic* morphism $F : X(\mathbb{Q}_p) \to Y(\mathbb{Q}_p)$ will mean a morphism of sets which, for all residue disks $]b[$, $b \in \mathcal{X}(\mathbb{F}_p)$, has the property that $F|_{]b[(\mathbb{Q}_p)}$ comes from a morphism of rigid analytic spaces $]b[\to Y$.We will often view such a morphism as a morphism of rigid analytic spaces

$$F' : \sqcup_{b \in \mathcal{X}(\mathbb{F}_p)}]b[\to Y.$$

In particular, when we refer to the *graph* of F, we will mean the image of the graph of F' under the map

$$\sqcup_{b\in\mathcal{X}(\mathbb{F}_p)}]b[\times Y \to X \times Y.$$

When we talk about *irreducible components* of a rigid analytic space, the rigid analytic space will always be a closed affinoid subspace of a polydisk, or a union of such spaces.

We denote the Galois group of a field F by G_F. When F is a number field, and S is a set of primes of a subfield $L \subset F$, we denote by $G_{F,S}$ the maximal quotient of G_F unramified outside above all primes above S.

Recall that, given a scheme Z over K, we say that a $\mathbb{Q}$-scheme is the *Weil restriction* of X, denoted $\mathrm{Res}_{K|\mathbb{Q}}(Z)$, if it represents the functor on $\mathbb{Q}$-algebras

$$S \mapsto Z(S \times_{\mathbb{Q}} K).$$

We will sometimes write $\mathrm{Res}_{K|\mathbb{Q}}(Z)$ simply as $\mathrm{Res}(Z)$. The only statements about existence of Weil restrictions that we will need are that smooth projective curves and abelian varieties over fields, or over Dedekind domains, admit Weil restrictions [10, 7.6.4].

Given an algebraic (or pro-algebraic) group U we denote by C_iU the central series filtration

$$C_1U = U \supset C_2U = [U, U] \supset C_3U = [U, C_2U] \supset \cdots$$

and, unless otherwise indicated, we denote $C_i/C_{i+1}U$ by $\mathrm{gr}_i U$. We similarly define C_iL and $\mathrm{gr}_i L$ for a Lie algebra L.

If K is a number field, and $T \supset S \sqcup \{v|p\}$ are finite sets of primes of K, and U is a unipotent group over $\mathbb{Q}_p$ with a continuous action of $G_{K,T}$, we denote by $H^1_{f,S}(G_{K,T}, U)$ the set of isomorphism classes of $G_{K,T}$-equivariant U-torsors which are unramified at all primes not in $S \sqcup \{v|p\}$ and are crystalline at all primes above p in the sense of [35]. In the case where U is a vector space, this recovers the usual Bloch–Kato Selmer group [8]. For a continuous G-representation W, we define $\mathrm{h}^i(G, W) := \dim_{\mathbb{Q}_p} H^i(G, W)$, and similarly define $\mathrm{h}^i_{f,S}(G, W)$ etc.

If $L|K$ is a finite extension of fields, we will write Ind_L^K and Res_L^K to denote the functors $\mathrm{Ind}_{G_L}^{G_K}$ and $\mathrm{Res}_{G_L}^{G_K}$ on Galois representations.

2 Ax–Schanuel and Chabauty's method over number fields

2.1 Chabauty's method and *p*-adic unlikely intersections

The Ax–Schanuel theorem for abelian varieties [2] can be translated into the following statement (the translation is identical to the geometric statement of Ax–Schanuel for tori [1] as stated in [55]).

Theorem 2.1 (Ax–Schanuel [2]) *Let A be an abelian variety over $\mathbb{C}$ of dimension n. Let $\Delta_{\exp} \subset A \times \mathrm{Lie}(A)$ be the graph of the exponential, and let $p : A \times \mathrm{Lie}(A) \to A$ be the projection. Let V be a subvariety of $A \times \mathrm{Lie}(A)$. Let W be an irreducible component of the complex analytic space $V^{\mathrm{an}} \cap \Delta_{\exp}$. Suppose $\mathrm{codim}_{V^{\mathrm{an}}}(W) < n$. Then $p(W)$ is contained in a translate of a proper abelian subvariety of A.*

Remark 2.1 This theorem can be deduced from Ax's original theorem as follows. Theorem 1 of [2] says that there exists a complex analytic sub-group B of $A \times \mathrm{Lie}(A)$, containing V^{an} and $\Delta_{\exp}$, such that

$$\mathrm{codim}_B(\Delta_{\exp}) \leq \mathrm{codim}_{W^{\mathrm{Zar}}}(W).$$

where $W^{\mathrm{Zar}} \subset A \times \mathrm{Lie}(A)$ denotes the Zariski closure of W. Let B' be the subgroup variety of $A \times \mathrm{Lie}(A)$ generated by W^{Zar}. By Chevalley's theorem, B' is of the form $B_1 \times B_2$, for B_1 an abelian subvariety of A and B_2 a sub-vector space of $\mathrm{Lie}(A)$. If $p(W)$ is not contained in a translate of a proper abelian subvariety of A, then $p(W^{\mathrm{Zar}})$ generates A, and hence $B_1 = A$, and $p(V) \cup \Delta_{\exp}$ generates $A \times \mathrm{Lie}(A)$, so that $\mathrm{codim}_B(\Delta_{\exp}) = n$.

Now let $A/\mathbb{Q}_p$ be an abelian variety with good reduction (the generalisations of these statements to the case of bad reduction are also well known, but we omit them as we don't use them, and haven't defined the notion of locally analytic in this setting). The p-adic logarithm defines a locally analytic group homomorphism

$$\log_A : A(\mathbb{Q}_p) \to \mathrm{Lie}(A).$$

in the sense of Sect. 1.4. Theorem 2.1 can be translated into a statement about $\log_A$ via the following Lemma.

Lemma 2.1 *Let $A/\mathbb{Q}_p$ be an abelian variety with good reduction. Let $\Delta_{\log} \subset A \times \mathrm{Lie}(A)$ denote the graph of the p-adic logarithm. Choose an embedding $\mathbb{Q}_p \hookrightarrow \mathbb{C}$. Let*

$$\widehat{\Delta}_{\exp} \subset \widehat{A}_{\mathbb{C}} \times \widehat{\mathrm{Lie}}(A)_{\mathbb{C}}$$

denote the formal completion of the graph of the exponential at $(0, 0)$. Then

$$\widehat{\Delta}_{\exp} = \widehat{\Delta}_{\log, \mathbb{C}}.$$

Proof $\widehat{\Delta}_{\log, \mathbb{C}}$ and $\widehat{\Delta}_{\exp}$ are the graphs of the morphisms of formal groups

$$\widehat{\log}_A : \widehat{A}_{\mathbb{C}} \to \widehat{\mathrm{Lie}}(A)_{\mathbb{C}},$$
$$\widehat{\exp}_A : \widehat{\mathrm{Lie}}(A)_{\mathbb{C}} \to \widehat{A}_{\mathbb{C}}.$$

The morphisms $\widehat{\exp}_A$ and $\widehat{\log}_A$ are inverse, hence their graphs agree. □

Now let X be a smooth projective geometrically irreducible curve of genus g over a number field K of degree d over $\mathbb{Q}$, and let J be the Jacobian of X. Let p be a rational prime of good reduction for X. Let $\mathrm{Res}(X) := \mathrm{Res}_{K|\mathbb{Q}}(X)$ denote the Weil restriction of X. Recall that this is a smooth projective variety of dimension $d = [K : \mathbb{Q}]$ over $\mathbb{Q}$. The morphism $\mathrm{Res}(X) \to \mathrm{Res}(J)$ induces a morphism $\mathrm{Alb}(\mathrm{Res}(X)) \to \mathrm{Res}(J)$, which can be seen to be an isomorphism by base changing to $\overline{\mathbb{Q}}$. Let Y denote the formal completion of $\mathrm{Res}\, J \times \mathrm{Lie}(\mathrm{Res}(J))$ at $(0, 0)$.

Let $\log_J$ denote the p-adic logarithm map

$$\mathrm{Res}(J)(\mathbb{Q}_p) \to \mathrm{Lie}(\mathrm{Res}(J))_{\mathbb{Q}_p}.$$

Since $\log_J$ is locally analytic, the graph of $\log_J$ gives a rigid analytic space $\Delta_{\log}$, and the formal completion at the point $(0, 0)$ defines a formal subscheme $\widehat{\Delta}_{\log}$ of $Y_{\mathbb{Q}_p}$. Let $\mathrm{AJ} : \mathrm{Res}(X) \to \mathrm{Res}(J)$ denote the Abel–Jacobi map with respect to the chosen basepoint $b \in \mathrm{Res}(X)(\mathbb{Q})$. Let $\overline{J(K)} \subset \mathrm{Lie}\,\mathrm{Res}(J)_{\mathbb{Q}_p}$ denote the $\mathbb{Q}_p$-vector space generated by the image of $\mathrm{Res}(J)(\mathbb{Q})$ in $\mathrm{Lie}\,\mathrm{Res}(J)_{\mathbb{Q}_p}$ under the map log. Let $X(K \otimes \mathbb{Q}_p)_1 \subset \mathrm{Res}(X)^{\mathrm{an}}_{\mathbb{Q}_p}$ denote the rigid analytic space $(\log \circ \mathrm{AJ})^{-1}(\overline{J(K)})$.

Corollary 2.1 *Let Z be a positive dimensional geometrically irreducible subvariety of $\mathrm{Res}(X)_{\mathbb{Q}_p}$. Let L denote the image of $\mathrm{Lie}(\mathrm{Alb}(Z))$ in $\mathrm{Lie}(\mathrm{Res}(J))_{\mathbb{Q}_p}$. Let W be an irreducible component of $Z \cap X(K \otimes \mathbb{Q}_p)_1$. Suppose*

$$\mathrm{codim}_Z(W) < \mathrm{codim}_L(L \cap \overline{J(K)}).$$

Then the projection of W to $\mathrm{Res}(X)_{\mathbb{Q}_p}$ is not Zariski dense in Z. In particular, if $\mathrm{rk}(J(K)) \leq d(g-1)$, then $X(K \otimes \mathbb{Q}_p)_1$ is not Zariski dense in $\prod_{v|p} X(K_v)$.

Proof Let B denote the image of $\mathrm{Alb}(Z)$ in $\mathrm{Res}(J)_{\mathbb{Q}_p}$. Define $V \subset \mathrm{Res}(J)_{\mathbb{Q}_p} \times \mathrm{Lie}(\mathrm{Res}(J))_{\mathbb{Q}_p}$ by

$$V = \mathrm{AJ}(Z) \times \overline{J(K)}.$$

Then the map $(\mathrm{AJ}, \log_J \circ \mathrm{AJ})$ induces an isomorphism

$$X(K \otimes \mathbb{Q}_p)_1 \cap Z \simeq \Delta_{\log} \cap V.$$

Let D be a residue disk of $J_{\mathbb{Q}_p} \times \mathrm{Lie}(J)_{\mathbb{Q}_p}$ intersecting $\Delta_{\log} \cap V$ non-trivially. For any point $(x, \log(x))$ in $\Delta_{\log}(\mathbb{Q}_p)$, the group law on $J_{\mathbb{Q}_p} \times \mathrm{Lie}(J)_{\mathbb{Q}_p}$ induces an isomorphism

$$J_{\mathbb{Q}_p} \times \mathrm{Lie}(J)_{\mathbb{Q}_p} \xrightarrow{\simeq} J_{\mathbb{Q}_p} \times \mathrm{Lie}(J)_{\mathbb{Q}_p}. \tag{1}$$

sending $(x, \log(x))$ to $(0, 0)$. Let P be a point of W. Using (1), we may assume $P = (0, 0)$. Let $\widehat{W}$ denote the formal completion of W at P. Choose an embedding $\overline{\mathbb{Q}}_p \hookrightarrow \mathbb{C}$. Then, by Lemma 2.1, $\widehat{W}_{\mathbb{C}}$ is an irreducible component of the formal

completion of $V_{\mathbb{C}} \cap \Delta_{\exp}$ at the $(0,0)$. Then $\widehat{W}_{\mathbb{C}}$ is the formal completion at $(0,0)$ of an irreducible component $\widetilde{W}$ of $\Delta_{\exp} \cap V_{\mathbb{C}}$ satisfying

$$\mathrm{codim}_{V_{\mathbb{C}}}(\widetilde{W}) < \dim(B).$$

Hence, by Theorem 2.1, $p(\widetilde{W})$ is contained in a translate of a proper abelian subvariety of $B_{\mathbb{C}}$, hence the same holds for $\widehat{W}$ and hence for W. Let $B' \subset B$ be the translate of a proper abelian subvariety containing W. This implies that the Zariski closure of W is contained in the pre-image of B'. In particular, the Zariski closure does not equal Z, since it does not generate $\mathrm{Alb}(Z)$. □

2.2 Applications to Siksek's question

In [50], Siksek examined the question of when $X(K \otimes \mathbb{Q}_p)_1$ can be proved to be finite for a curve X of genus g. In particular, he asked whether a sufficient condition for finiteness of $X(K \otimes \mathbb{Q}_p)_1$ is that, for all intermediate extensions $K|L|\mathbb{Q}$ over which X admits a model X'/L, the Chabauty–Coleman condition

$$\mathrm{rk}(\mathrm{Jac}(X')(L)) \leq (g-1)[L:\mathbb{Q}] \tag{2}$$

is satisfied.

This question has a negative answer, as one can construct counterexamples as follows. Let X_0 be a curve of genus g_0 defined over $\mathbb{Q}$, such that the p-adic closure of $\mathrm{Jac}(X_0)(\mathbb{Q})$ in $\mathrm{Jac}(X_0)(\mathbb{Q}_p)$ has finite index. Let $K|\mathbb{Q}$ be a finite extension such that the rank of $\mathrm{Jac}(X_0)(K)$ is $\leq [K:\mathbb{Q}](g_0-1)$. Let $X \to X_{0,K}$ be a cover such that X is not defined over a proper subfield of K, and the Prym variety $P = \mathrm{Ker}(\mathrm{Jac}(X) \to \mathrm{Jac}(X_0)_K)^0$ has the property that the p-adic closure of $P(K)$ in $\prod_{v|p} P(K_v)$ has finite index. Then X satisfies (2), but $X(K \otimes \mathbb{Q}_p)_1$ will contain the pre-image of $X_0(\mathbb{Q}_p) \subset \prod_{v|p} X_0(\mathbb{Q}_v)$ in $\prod_{v|p} X(\mathbb{Q}_v)$, and in particular will be infinite.

For example, we can take X_0 to be the curve

$$y^2 = \left(x^4 - \frac{11}{27}\right)\left(x^2 - \frac{27}{11}\right),$$

take $K = \mathbb{Q}(\sqrt{33})$, and take X to be the degree two cover of X_0 given by

$$y^2 = x^8 + \frac{2916 \cdot b + 484}{297}x^6 + \frac{-128304 \cdot b + 168112}{8019}x^4 + \frac{214057728 \cdot b - 35529472}{23181643}t^2 + \frac{-10784721024 \cdot b + 8742087808}{64304361},$$

where $b := \sqrt{11/27}$. The Jacobian of X is isogenous to $\mathrm{Jac}(X_0)_K$ times the rank two elliptic curve

$$y^2 + \frac{2916 \cdot b + 484}{297} xy + \frac{276156864 \cdot b + 116895680}{2381643} y = x^3 + \frac{384912 \cdot b - 168112}{8019} x^2 + \frac{3594907008 \cdot b - 4270950016}{21434787} x.$$

This also gives a counterexample to Conjecture 5.1 of [30], which is a generalisation of Siksek's question to the setting of Kim's method. A generalisation of this construction has recently been considered in [54], where it is referred to as a base change Prym obstruction.

The Ax–Schanuel Theorem implies the following weaker form of Siksek's question has a positive answer. Informally, we can phrase the result as follows: Siksek's question asks whether, for finiteness of $X(K \otimes \mathbb{Q}_p)_1$, it is sufficient for all subvarieties of $\mathrm{Res}_{K|\mathbb{Q}}(X)$ arising from the diagonal embedding of $\mathrm{Res}_{L|\mathbb{Q}}(X)$ to satisfy the usual Chabauty–Coleman condition, where $L \subset K$ is a subfield. Whilst this is not true in general, the corollary below says that it is sufficient for *all* irreducible subvarieties of $\mathrm{Res}_{K|\mathbb{Q}}(X)_{\overline{\mathbb{Q}}_p}$ to satisfy a Chabauty–Coleman-type condition.

Corollary 2.2 *Let X be a smooth projective curve of genus g over K. Let $J \to B$ be a quotient of J defined over K. Suppose that the cokernel of*

$$\mathrm{Res}(B)(K) \otimes \overline{\mathbb{Q}}_p \to \mathrm{Lie}(\mathrm{Res}(B))_{\overline{\mathbb{Q}}_p}$$

has rank $\geq [K : \mathbb{Q}]$. If $X(K \otimes \mathbb{Q}_p)_1$ is infinite then there exists a positive dimensional subvariety Z of $\mathrm{Res}_{K|\mathbb{Q}}(X)_{\overline{\mathbb{Q}}_p}$, such that the image A of $\mathrm{Alb}(Z)$ in $\mathrm{Res}_{K|\mathbb{Q}}(B)_{\overline{\mathbb{Q}}_p}$ satisfies

$$\mathrm{codim}_{\mathrm{Lie}(A)} \mathrm{Lie}(A) \cap \overline{B(K)} < \dim(Z),$$

where $\overline{B(K)}$ denotes the $\overline{\mathbb{Q}}_p$-subspace of $\mathrm{Lie}(\mathrm{Res}_{K|\mathbb{Q}}(B))_{\overline{\mathbb{Q}}_p}$ generated by $B(K)$.

Proof Let $Z \subset \mathrm{Res}(X)_{\overline{\mathbb{Q}}_p}$ be a positive dimensional irreducible component of the Zariski closure of $X(K \otimes \mathbb{Q}_p)_1$. Let A denote the image of $\mathrm{Alb}(Z)$ in $\mathrm{Res}_{K|\mathbb{Q}}(B)_{\overline{\mathbb{Q}}_p}$. Since $X(K \otimes \mathbb{Q}_p)_1 \cap Z$ is Zariski dense in Z by construction, Corollary 2.1 implies that the codimension of $\mathrm{Lie}(A) \cap J(K) \otimes \overline{\mathbb{Q}}_p$ in $\mathrm{Lie}(A)$ is less than the dimension of Z. □

Proof of Proposition 1.1, case (1) Recall that we suppose that

$$\mathrm{Hom}(\mathrm{Jac}(X)_{\overline{\mathbb{Q}},\sigma_1}, \mathrm{Jac}(X)_{\overline{\mathbb{Q}},\sigma_2}) = 0 \tag{3}$$

whenever $\sigma_1 \neq \sigma_2$. Let $Z \subset \mathrm{Res}(X)_{\mathbb{Q}_p}$ be an irreducible component of the Zariski closure of $\mathrm{Res}(X)(\mathbb{Q}_p)_1$. Note that, since Z is an irreducible component of the Zariski closure of a set of $\mathbb{Q}_p$-points of $\mathrm{Res}(X)_{\mathbb{Q}_p}$, it is actually geometrically irreducible.

Suppose, for contradiction, that the projection of Z to every factor of $\mathrm{Res}(X)_{\mathbb{Q}_p} \simeq \prod_{v|p} X_{K_v}$ is dominant. Then, by assumption, $\mathrm{Alb}(Z)$ surjects onto every factor of $\mathrm{Res}(J)_{\mathbb{Q}_p}$. Then, by (3), it must be the case that $\mathrm{Alb}(Z)$ surjects onto $\mathrm{Res}(J)_{\mathbb{Q}_p}$. This contradicts Corollary 2.2. □

Remark 2.2 Note that the condition in Proposition 1.1 (concerning the homomorphisms between $J_{\sigma,\mathbb{C}}$ for different embeddings σ) certainly implies that X does not descend to a subfield, however it is strictly stronger. The explicit counterexample given above has the property that it can be explained by a quotient curve which does descend to $\mathbb{Q}$. It is natural to wonder if there exist 'stronger' counterexamples not explained by a quotient curve which descends to a subfield. For example, does there exist a genus two curve X defined over a quadratic field $K|\mathbb{Q}$, with simple Jacobian J, which gives a negative answer to Siksek's question?

3 The Chabauty–Kim method

3.1 Selmer varieties

To describe the main obstacle to proving finiteness over general number fields, we first explain Kim's method over $\mathbb{Q}$, following [35, 36]. Let $\mathcal{X}$, S and p be as in the introduction. Let T_0 denote the union of the set of primes in S, the set of primes ramifying in $K|\mathbb{Q}$ and the set of primes of bad reduction for X, and let $T := T_0 \cup \{v|p\}$. Suppose we have a K-rational point $b \in \mathcal{X}(\mathcal{O}_{K,S})$. For any field $L|K$, and any L-point $y \in X(L)$, we have a $\mathrm{Gal}(\overline{L}|L)$-equivariant $\pi_1^{\text{ét}}(X_{\overline{L}}, b)$-torsor (where $\pi_1^{\text{ét}}(X_{\overline{L}}, b)$ denotes the étale fundamental group of $X_{\overline{L}}$) given by the étale torsor of paths $\pi_1^{\text{ét}}(X_{\overline{L}}; b, y)$. Hence we have a commutative diagram

$$\begin{array}{ccc} \mathcal{X}(\mathcal{O}_{K,S}) & \longrightarrow & H^1(G_K, \pi_1^{\text{ét}}(X_{\overline{K}}, b)) \\ \downarrow & & \downarrow \mathrm{loc} \\ \prod_{v\in S} X(K_v) \times \prod_{v\in T\setminus S} \mathcal{X}(\mathcal{O}_{K_v}) & \longrightarrow & \prod_{v\in T} H^1(G_{K_v}, \pi_1^{\text{ét}}(X_{\overline{K}_v}, b)) \end{array} \tag{4}$$

Hence a natural obstruction to $(x_v) \in \prod_{v\in S} X(K_v) \times \prod_{v\in T\setminus S} \mathcal{X}(\mathcal{O}_{K_v})$ coming from $x \in \mathcal{X}(\mathcal{O}_{K,S})$ is that $[\pi_1^{\text{ét}}(X_{\overline{K_v}}; b, x_v)]$ lies in the subspace $\mathrm{loc}\, H^1(G_K, \pi_1^{\text{ét}}(X_{\overline{K}}, b))$.

In practice, the set $H^1(G_K, \pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b))$ is rather mysterious, and Kim's method starts by replacing it with a more tractable object. Namely, for any variety Z over a field K of characteristic zero, and $b \in Z(\overline{L})$, we define $\pi_1^{\text{ét},\mathbb{Q}_p}(X_{\overline{L}}, b)$ to be the $\mathbb{Q}_p$-unipotent completion of $\pi_1^{\text{ét}}(Z_{\overline{L}}, b)$ [17, §10], and define

$$U_n(Z) = U_n(Z)(b) := \pi_1^{\text{ét},\mathbb{Q}_p}(Z_{\overline{L}}, b)/C_{n+1}\pi_1^{\text{ét},\mathbb{Q}_p}(Z_{\overline{L}}, b).$$

Returning to the setting of $\mathcal{X}/\mathcal{O}_{K,S}$ and $b \in \mathcal{X}(\mathcal{O}_{K,S})$ as above, we have a commutative diagram

$$\begin{array}{ccc} \mathcal{X}(\mathcal{O}_{K,S}) & \xrightarrow{\quad j_n \quad} & H^1(G_{K,T}, U_n(X)(b)) \\ \downarrow & & \downarrow \mathrm{loc}_n \\ \prod_{v\in S} X(K_v) \times \prod_{v\in T\setminus S} \mathcal{X}(\mathcal{O}_{K_v}) & \xrightarrow[\prod_{v\in T} j_{n,v}]{} & \prod_{v\in T} H^1(G_{K_v}, U_n(X)(b)), \end{array}$$

where the map j_n may be defined as follows: by definition of the unipotent completion, we have a Galois equivariant map $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}}, b) \to U_n(X)(b)$, and hence by functoriality a map

$$H^1(G_K, \pi_1^{\text{ét}}(X_{\overline{K}}, b)) \to H^1(G_K, U_n(b)).$$

By Grothendieck's specialization theorem [47, §X], the image of $[\pi_1^{\text{ét}}(X_{\overline{K}}; b, x)]$ in $H^1(G_K, U_n(b))$ will be unramified at all v outside of T, and hence defines an element of the subspace $H^1(G_{K,T}, U_n(b))$.

Hence a natural obstruction to $(x_v) \in \prod_{v\in S} X(K_v) \times \prod_{v\in T\setminus S} \mathcal{X}(\mathcal{O}_{K_v})$ coming from $x \in \mathcal{X}(\mathcal{O}_{K,S})$ is that $(j_{n,v}(x_v))$ lies in the subspace $\mathrm{loc}_n H^1(G_{K,T}, U_n(b))$. For a rational prime p we denote by $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ the image of $(\prod_{v\in T} j_{n,v})^{-1} \mathrm{loc}_n H^1(G_{K,T}, U_n)$ in $\prod_{v|p} \mathcal{X}(\mathcal{O}_v)$ under the projection

$$\prod_{v\in S} X(K_v) \times \prod_{v\in T\setminus S} \mathcal{X}(\mathcal{O}_{K_v}) \to \prod_{v|p} \mathcal{X}(\mathcal{O}_v).$$

That is, $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ is simply the set of all tuples (x_v) in $\prod_{v|p} \mathcal{X}(\mathcal{O}_{K_v})$ which extend to a tuple (x_v) in $\prod_{v\in S} X(K_v) \times \prod_{v\in T\setminus S} \mathcal{X}(\mathcal{O}_{K_v})$ for which $(j_{n,v}(x_v))$ lies in the image of $H^1(G_{K,T}, U_n(X)(b))$. For v a prime above p, we define $\mathcal{X}(\mathcal{O}_{K_v})_{S,n}$ to be the projection of $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ to $X(K_v)$. Equivalently, it is the set of $\mathcal{O}_{K_v}$-points whose $H^1(G_{K_v}, U_n)$ class extends to a $\prod_{v'\in T\setminus S} H^1(G_{K_{v'}}, U_n)$ class in the image of $H^1(G_{K,T}, U_n)$.

By a theorem of Kim and Tamagawa [39, Corollary 0.2], for v prime to p and not in S, the map $j_{n,v}$ has finite image. Let $\alpha \in \prod_{v\in T_0 - S} j_{n,v}(\mathcal{X}(\mathcal{O}(K_v)))$. Let $\mathrm{Sel}(U_n)_\alpha \subset H^1_{f,T}(G_{K,T}, U_n(b))$ denote the fibre of α with respect to the localisation map (the Selmer scheme of U_n with local conditions α). Let $\mathcal{X}(\mathcal{O}_{K,S})_\alpha \subset \mathcal{X}(\mathcal{O}_{K,S})$ denote the subset of points mapping to $\mathrm{Sel}(U_n)_\alpha(\mathbb{Q}_p)$ under j_n, and let $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_\alpha$ denote the subset of p-adic points mapping to $\mathrm{loc}_p(\mathrm{Sel}(U_n)_\alpha)$. There is a commutative diagram

$$\begin{array}{ccc} \mathcal{X}(\mathcal{O}_{K,S})_\alpha & \xrightarrow{j_n} & \mathrm{Sel}(U_n)_\alpha \\ \downarrow & & \downarrow \mathrm{loc}_p \\ \prod_{v|p} \mathcal{X}(\mathcal{O}_v) & \xrightarrow{\prod_{v|p} j_{n,v}} & \prod_{v|p} H^1_f(G_{K_v}, U_n(X)(b)). \end{array} \tag{5}$$

We define

$$\mathrm{Sel}(U_n) := \sqcup_\alpha \mathrm{Sel}(U_n)_\alpha,$$

where the disjoint union is over all α in the finite set

$$\prod_{v \in T_0 - S} j_{n,v}(\mathcal{X}(\mathcal{O}_{K_v})) \subset \prod_{v \in T_0 - S} H^1(G_{K_v}, U_n(X)(b)).$$

Note that

$$\mathcal{X}(\mathbb{Z}_p \otimes \mathcal{O}_K)_n = \left(\prod_{v|p} j_v \right)^{-1} (\mathrm{Sel}(U_n)).$$

More generally for any G_K-stable quotient U of U_n, we can define maps $j_v : X(K_v) \to H^1(G_K, U)$, Selmer schemes $\mathrm{Sel}(U)$, and global maps $j : \mathcal{X}(\mathcal{O}_{K,S}) \to \mathrm{Sel}(U)$, and $\mathcal{X}(\mathbb{Z}_p \otimes \mathcal{O}_K)_{S,U}$. Whenever U is a quotient of U', we have an inclusion

$$\mathcal{X}(\mathbb{Z}_p \otimes \mathcal{O}_K)_{S,U} \supset \mathcal{X}(\mathbb{Z}_p \otimes \mathcal{O}_K)_{S,U'}.$$

We recall the interpretation of $\mathrm{Sel}(U)_\alpha$ in terms of twisting.

Lemma 3.1 *Let $\widetilde{\alpha} \in H^1(G_{K,T}, U)$ be a cohomology class whose image in $\prod_{v \in S} H^1(G_{K_v}, U)$ is equal to $\alpha = (\alpha_v)$. Let $U^{\widetilde{\alpha}}$ denote the twist of U by the torsor $\widetilde{\alpha}$. Then we have an inclusion*

$$\mathrm{Sel}(U)_\alpha \hookrightarrow H^1_{f,S}(G_{K,T}, U^{\widetilde{\alpha}})$$

Proof Recall from [48, §1.5.2 Proposition 34] that the twisting construction defines an isomorphism

$$H^1(G_{K,T}, U^{\widetilde{\alpha}}) \simeq H^1(G_{K,T}, U),$$

which sends the trivial torsor to the class of $\widetilde{\alpha}$, and is functorial in both arguments. Hence, under this isomorphism, classes which are trivial at $v \neq p$ go to classes which are equal to α_v at v, and classes which are crystalline go to classes which are crystalline. □

In [36], Kim proves two fundamental properties of the diagram (5). First, the Galois cohomology sets $\mathrm{Sel}(U)$ and $H^1_f(G_{\mathbb{Q}_p}, U)$ are representable by $\mathbb{Q}_p$-schemes of finite type, in such a way that the morphism loc_p is algebraic. Second, the map loc_α is algebraic, and that for all $v|p$, j_v is locally analytic (in the sense defined in the introduction), and for all $z \in \mathcal{X}(\mathcal{O}_v)$, the map $j_v|_{]z[}$ has Zariski dense image. If $K = \mathbb{Q}$ and loc_α is not dominant, then the set $\mathcal{X}(\mathbb{Z}_p)_\alpha$ is thus finite, since on each residue disk it is given by a non-trivial power series.

3.2 Trading degree for dimension in the Chabauty–Kim method

Over number fields, the situation is slightly more complicated. Suppose that the image of loc_α has codimension d in $\prod_{v|p} H^1_f(G_{K_v}, U(b))$. Then, on each residue polydisk $]z[\subset \prod_{v|p} \mathcal{X}(\mathcal{O}_v)$, we deduce that $]z[\cap \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)$ is contained in the zeroes of d power series. However, this does not imply that $]z[\cap \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)$ is finite.

First, we replace the problem of finding K-rational points on X with that of finding $\mathbb{Q}$-rational points on the Weil restriction $\mathrm{Res}_{K|\mathbb{Q}}(X)$. We recall some properties of the Weil restriction from [52]. Given topological groups G, H, N with $H < G$ finite index and a continuous action of H on N, define $\mathrm{Ind}_H^G(N)$ to be group of continuous left H-equivariant maps $G \to N$. This has a natural continuous action of G (see [48, I.5.8]).

Proposition 3.1 ([52, Proposition 8]) *Let G be a profinite group, and H a finite index subgroup. Let U be a topological group with a continuous action of H, and let $\mathrm{Ind}_H^G U \to U$ denote the non-abelian induction, as defined in* [52, 2.1.2]. *Then the natural map*

$$H^1(G, \mathrm{Ind}_H^G U) \to H^1(H, U).$$

is an isomorphism.

Lemma 3.2 (Stix, [52]) *There is an isomorphism*

$$\pi_1^{\text{ét}}(\mathrm{Res}(X), b) \simeq \mathrm{Ind}_K^{\mathbb{Q}} \pi_1^{\text{ét}}(X, b),$$

inducing a $G_{\mathbb{Q}}$-equivariant isomorphism

$$\pi_1^{\text{ét}}(\mathrm{Res}(X)_{\overline{\mathbb{Q}}}, b) \simeq \mathrm{Ind}_K^{\mathbb{Q}} \pi_1^{\text{ét}}(X_{\overline{K}}, b).$$

By Proposition 3.1, this induces an isomorphism

$$H^1(G_K, \pi_1^{\text{ét}}(X_{\overline{K}}, b)) \simeq H^1(G_{\mathbb{Q}}, \pi_1^{\text{ét}}(\mathrm{Res}(X)_{\overline{\mathbb{Q}}}, b)),$$

giving a commutative diagram whose vertical maps are bijections

$$\begin{array}{ccccc} X(K) & \longrightarrow & H^1(G_K, \pi_1^{\text{ét}}(X_{\overline{K}}, b)) & \longrightarrow & H^1(G_K, U_n(X)(b)) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Res}(X)(\mathbb{Q}) & \longrightarrow & H^1(G_{\mathbb{Q}}, \pi_1^{\text{ét}}(\mathrm{Res}(X)_{\overline{\mathbb{Q}}}, b) & \longrightarrow & H^1(G_{\mathbb{Q}}, U_n(\mathrm{Res}(X)(b)). \end{array}$$

Lemma 3.3 *Let G be a topological group, H a finite index subgroup, and $K < G$ a closed subgroup. Let U be a topological group with a continuous action of H. Then we have a K-equivariant isomorphism of topological groups*

$$\mathrm{Ind}_H^G(U) \simeq \prod_{x \in H\backslash G/K} \mathrm{Ind}_{K\cap xHx^{-1}}^K U^x.$$

where U^x denote the group U with action twisted by conjugating by x.

Proof Recall that $\mathrm{Ind}_H^G(U)$ is, by definition, the set of continuous H-equivariant functions $G \to U$. Such a function is uniquely determined by where it sends $H\backslash G$. Hence, via the bijection $G/H \simeq \sqcup_{x\in H\backslash G/K} HxK$, we obtain a bijection

$$\mathrm{Ind}_H^G(U) \to \prod_{x \in H\backslash G/K} \mathrm{Ind}_{K\cap xHx^{-1}}^K U^x.$$

which may be checked to be K-equivariant, as in the classical case of Mackey's restriction formula. □

Lemma 3.3 and Proposition 3.1 together imply that, for all primes $l \neq p$, we have isomorphisms

$$\prod_{v|l} H^1(G_{K_v}, U_n(X)(b)) \simeq H^1(G_{\mathbb{Q}_\ell}, U_n(\mathrm{Res}(X)(b)). \tag{6}$$

For the remainder of this paper, we denote $U_n(\mathrm{Res}(X))(b)$ by $U_n(b)$, or sometimes simply U_n.

Lemma 3.4 *At p, we have an isomorphism of unipotent groups with filtration over $\mathbb{Q}_p$*

$$U_n^{\mathrm{dR}}(\mathrm{Res}_{K|\mathbb{Q}}(X)_{\mathbb{Q}_p})(b) \simeq \prod_{\sigma: K\hookrightarrow \mathbb{Q}_p} U_n^{\mathrm{dR}}(X_{\mathbb{Q}_p,\sigma})(b_\sigma),$$

where the product is over all σ in $\mathrm{Hom}(K, \mathbb{Q}_p)$.

Proof This follows from the fact that, since p splits completely in K, we have

$$\mathrm{Res}_{K|\mathbb{Q}}(X) \times_{\mathbb{Q}} \mathbb{Q}_p \simeq \prod_{\sigma} X \times_{K,\sigma} \mathbb{Q}_p.$$

□

Hence we obtain a commutative diagram whose vertical maps are bijective

$$\begin{array}{ccccc} \prod_{v|p} X(K_v) & \longrightarrow & \prod_{v|p} H^1_f(G_{K_v}, U_n(X)(b)) & \longrightarrow & \prod_{v|p} U_n^{\mathrm{dR}}(X_{K_v})/F^0 \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Res}(X)(\mathbb{Q}_p) & \longrightarrow & H^1_f(G_{\mathbb{Q}_p}, U_n(\mathrm{Res}(X))(b)) & \longrightarrow & U_n^{\mathrm{dR}}(\mathrm{Res}(X)_{\mathbb{Q}_p})/F^0 \end{array}$$

If $S \subset S'$, then by definition $\mathcal{X}(\mathbb{Z}_p \otimes \mathcal{O}_K)_{S,n} \subset \mathcal{X}(\mathbb{Z}_p \otimes \mathcal{O}_K)_{S',n}$, and in particular finiteness of the latter implies finiteness of the former. Hence, enlarging the set S if necessary, we may assume that S is of the form $\{v|l : l \in S_0\}$, for a finite set S_0 of rational primes. Then, by (6) and the preceding commutative diagrams, the bijection $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p) \simeq \mathrm{Res}_{\mathcal{O}_{K,S}|\mathbb{Z}_{S_0}}(\mathcal{X})(\mathbb{Z}_p)$ induces a bijection

$$\mathrm{Res}_{\mathcal{O}_{K,S}|\mathbb{Z}_{S_0}}(\mathcal{X})(\mathbb{Z}_p)_{S_0,n} \simeq \mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}. \tag{7}$$

To ease notation, we will sometimes write $\mathrm{Res}_{\mathcal{O}_{K,S}|\mathbb{Z}_{S_0}}(\mathcal{X})$ simply as $\mathrm{Res}_{K|\mathbb{Q}}(\mathcal{X})$, or $\mathrm{Res}(\mathcal{X})$. Hence (7) reduces Theorem 1.1 to proving finiteness of $\mathrm{Res}_{K|\mathbb{Q}}(\mathcal{X})(\mathbb{Z}_p)_{S,n}$.

We recall the following result from [6]. Although the proof was given for curves, it also applies for any smooth geometrically irreducible quasi-projective variety.

Lemma 3.5 [6, §2] *Let $U(b)$ be a quotient of $U_n(b)$, and b' another basepoint. Let $U(b')$ be the corresponding quotient of $U_n(b')$. Then*

$$X(\mathbb{Q}_p)_{U(b)} = X(\mathbb{Q}_p)_{U(b')}.$$

3.3 Tangential localization

In this subsection we recall Kim's description of the map on tangent spaces

$$d\,\mathrm{loc}_p : T_c H^1_f(G_{\mathbb{Q},T}, U_n) \to T_{\mathrm{loc}_p(c)} H^1_f(G_{\mathbb{Q}_p}, U_n)$$

in terms of (abelian) Galois cohomology. For a variety Z, we let $L_n(Z)$ denote the Lie algebra of the group $U_n(Z)$, and similarly denote by $L_n^{\mathrm{dR}}(Z)$ the Lie algebra of $U_n^{\mathrm{dR}}(Z)$. When $Z = \mathrm{Res}(X)$, we write these simply as L_n and L_n^{dR}. The following result is proved by Kim for Galois-stable quotients of fundamental groups of curves. Iterated intersection with generic hyperplanes then implies the result for unipotent fundamental groups of arbitrary smooth geometrically connected projective varieties, by the Lefschetz hyperplane theorem for fundamental groups [25, XII Corollary 3.5].

Proposition 3.2 ([38, Propositions 1.1, 1.2 and 1.3]) *For any $c \in H^1_f(G_{\mathbb{Q},T}, U_n)$, there is a commutative diagram whose vertical maps are isomorphisms*

$$\begin{array}{ccc} T_c H^1_{f,S}(G_{\mathbb{Q},T}, U_n) & \xrightarrow{d\,\mathrm{loc}_p} & T_{\mathrm{loc}_p(c)} H^1_f(G_{\mathbb{Q}_p}, U_n) \\ \downarrow & & \downarrow \\ H^1_{f,S}(G_{\mathbb{Q},T}, L_n^c) & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_{\mathbb{Q}_p}, L_n^c) \end{array}$$

where L_n^c denotes the twist of L_n by c by the adjoint action of U_n on L_n. In particular, if the map $\mathrm{loc}_p : H^1_{f,S}(G_{\mathbb{Q},T}, L_n^c) \to H^1_f(G_{\mathbb{Q}_p}, L_n^c)$ is not surjective then $\mathrm{loc}_p : H^1_{f,S}(G_{\mathbb{Q},T}, U_n) \to H^1_f(G_{\mathbb{Q}_p}, U_n)$ is not dominant in a neighbourhood of c.

Lemma 3.6 *Let U be a Galois stable quotient of U_n, with Lie algebra L. Let $U^{\mathrm{dR}} := D_{\mathrm{dR}}(U)$. Let H be a $G_{\mathbb{Q}_p}$-stable subgroup of U. Let W be an irreducible component of $\mathrm{loc}_p H^1_{f,S}(G_{\mathbb{Q},T}, U) \cap D_{\mathrm{dR}}(H)/F^0$. Then*

$$\dim W \leq \max_{c \in H^1_{f,S}(G_{\mathbb{Q},T}, U)} \dim \mathrm{loc}_p H^1_{f,S}(G_{\mathbb{Q},T}, L^c) \cap \mathrm{Lie}(D_{\mathrm{dR}}(H^{\mathrm{loc}_p c}))/F^0,$$

where $\mathrm{Lie}(H)^{\mathrm{loc}_p c}/F^0$ is defined to be zero if $\mathrm{loc}_p c$ is not in the image in H/F^0, and $\mathrm{loc}_p H^1_{f,S}(G_{\mathbb{Q},T}, L^c) \subset H^1_f(G_{\mathbb{Q}_p}, L^{\mathrm{loc}_p c})$ is viewed as a subscheme of $\mathrm{Lie}(D_{\mathrm{dR}}(U^{\mathrm{loc}_p c}))/F^0$ via the Bloch–Kato exponential.

Proof The dimension of W is bounded by the generic dimension of its tangent space (i.e. the dimension of the tangent space at the generic point $\eta \in W$). Since the map

$$T_c(\mathrm{loc}_p^{-1} W) \to T_{\mathrm{loc}_p(c)} W$$

is generically surjective, we have

$$\begin{aligned} \dim W &\leq \dim T_\eta(W) \\ &\leq \max_{c \in \mathrm{loc}_p^{-1} H/F^0} \dim d\,\mathrm{loc}_p\, T_c H^1_{f,S}(G_{\mathbb{Q},T}, U) \cap T_{\mathrm{loc}_p(c)}(D_{\mathrm{dR}}(H)/F^0) \\ &= \max_{c \in H^1_f(G_{\mathbb{Q},T}, U)} \mathrm{loc}_p\, H^1_{f,S}(G_{\mathbb{Q},T}, L^c) \cap \mathrm{Lie}(D_{\mathrm{dR}}(H^{\mathrm{loc}_p c}))/F^0. \end{aligned}$$

□

By a *virtual basepoint*, we shall mean a $\mathbb{Q}_p$-point $z \in \mathrm{Res}(\mathcal{X})(\mathbb{Z}_p)$ such that $j(z)$ lies in the image of $\mathrm{Sel}(U)$, together with a torsor $P \in \mathrm{Sel}(U)$ such that $\mathrm{loc}_p(P) = j(P)$. In particular, the notion of a virtual basepoint depends on a choice of quotient of $\pi_1^{\text{ét},\mathbb{Q}_p}(\mathrm{Res}(X)_{\overline{\mathbb{Q}}}, b)$, but by Lemma 3.5 the property of $z \in \mathrm{Res}(\mathcal{X})(\mathbb{Z}_p)$ extending to a virtual basepoint is independent of the choice of basepoint. Given a virtual basepoint

(z, P), we obtain a $\mathbb{Q}_p$-unipotent group U^P defined to be the twist of U by the $G_{\mathbb{Q},T}$-equivariant U-torsor P. Then U^P is equipped with an action of $G_{\mathbb{Q},T}$, and morphisms

$$\begin{aligned} j_{z,v} &: \mathrm{Res}(X)(\mathbb{Q}_v) \to H^1(G_{\mathbb{Q}_v}, U^P) \\ j_{z,p} &: \mathrm{Res}(X)(\mathbb{Q}_p) \to H^1_f(G_{\mathbb{Q}_p}, U^P) \\ j_z &: \mathcal{X}(\mathcal{O}_{K,S}) \to \mathrm{Sel}(U^P). \end{aligned}$$

Lemma 3.7 *For every collection of local conditions such that $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_\alpha$ is non-empty, there is a virtual basepoint $(b, P) \in X(\mathbb{Q}_p)$ such that*

$$\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_\alpha \subset j_b^{-1}(\mathrm{loc}_p\, H^1_{f,S}(G_{\mathbb{Q},T}, U^P)). \tag{8}$$

Proof If $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_\alpha$ is non-empty, then by definition there exists $P \in H^1(G_{K,T}, U_n(X))$ such that $\mathrm{loc}_v(P)) = \alpha_v$ for all $v \in T_0 - S$, and $\mathrm{loc}_p(P) = j(b)$ for some $b \in \mathrm{Res}(\mathcal{X})(\mathbb{Q}_p)$. Then, taking (b, P) as a virtual basepoint, we deduce (8) from Lemma 3.1. □

Often, when we work with virtual basepoints (b, P), we will simply write U rather than U^P, and write the virtual basepoint simply as b.

3.4 The unipotent Albanese morphism

We now recall some properties of the morphism $\mathcal{X}(\mathcal{O}_v) \to H^1_f(G_{K_v}, U_n)$ when $v|p$ from [36]. We refer to [36] and the references therein for the background material regarding p-adic Hodge theory. As we always take p to be a prime which splits completely in K, we henceforth fix an isomorphism $K_v \simeq \mathbb{Q}_p$ and work over $\mathbb{Q}_p$. Let $\mathcal{X}$ be a smooth curve over $\mathbb{Z}_p$. Fontaine's functor D_{cris} sends continuous $\mathbb{Q}_p$ representations of $G_{\mathbb{Q}_p}$ to filtered ϕ-modules over $\mathbb{Q}_p$. Recall that a filtered ϕ-module over $\mathbb{Q}_p$ is a finite dimensional vector space W over $\mathbb{Q}_p$, equipped with a $\mathbb{Q}_p$-linear Frobenius automorphism ϕ, and a decreasing filtration $F^\bullet$ on W.

As explained in [36], Fontaine's functor induces functors D_{cris} and D_{dR} on unipotent groups over $\mathbb{Q}_p$ with a continuous action of $G_{\mathbb{Q}_p}$. The target of D_{cris} is the category of unipotent groups U over $\mathbb{Q}_p$, together with an automorphism ϕ of U, and a filtration Fil by subgroups on U (we shall refer to an object of this category as a filtered ϕ-group). The target of D_{dR} is the category of unipotent groups over $\mathbb{Q}_p$ equipped with a filtration by subgroups. We say a $G_{\mathbb{Q}_p}$-equivariant U-torsor P is *crystalline* if it admits a $G_{\mathbb{Q}_p}$-equivariant trivialisation when base changed to B_{cris} (if $\mathcal{O}(U)$ is ind-crystalline, this is the same as saying that $\mathcal{O}(P)$ is ind-crystalline). The functor D_{cris} induces an equivalence of categories between crystalline U-torsors and filtered ϕ-torsors over $D_{\mathrm{cris}}(U)$ (where a filtered ϕ-torsor for a filtered ϕ-group is simply a torsor with compatible filtration and ϕ-action). By [36, Proposition 1], if U is crystalline and $D_{\mathrm{cris}}(U)^{\phi=1} = 1$, this induces an isomorphism of $\mathbb{Q}_p$-schemes (a 'non-abelian Bloch–

Kato logarithm')

$$H^1_f(G_{\mathbb{Q}_p}, U) \simeq D_{\mathrm{dR}}(U)/F^0.$$

Let $U^{\mathrm{cris}}(b)$ denote the Tannakian fundamental group of the category of unipotent isocrystals on $\mathcal{X}_{\mathbb{F}_p}$. This is a pro-unipotent group over $\mathbb{Q}_p$. Let $U^{\mathrm{dR}}(b)$ denote the Tannakian fundamental group of the category of unipotent flat connections on $X_{\mathbb{Q}_p}$. This is a pro-unipotent group over $\mathbb{Q}_p$. By Chiarellotto–Le Stum [12, Proposition 2.4.1], we have an isomorphism of $\mathbb{Q}_p$-group schemes

$$U^{\mathrm{cris}}(b) \simeq U^{\mathrm{dR}}(b).$$

Let $U_n^{\mathrm{cris}}(b)$ and $U_n^{\mathrm{dR}}(b)$ denote the respective maximal n-unipotent quotients. Then $U_n^{\mathrm{cris}}(b)$ has the structure of a filtered ϕ group over $\mathbb{Q}_p$. By Olsson's non-abelian comparison theorem [46, Theorem 1.11], $U_n(b)$ is crystalline, and we have an isomorphism of filtered ϕ groups over $\mathbb{Q}_p$

$$D_{\mathrm{cris}}(U_n(b)) \simeq U_n^{\mathrm{cris}}(b).$$

Putting all this together, we obtain a locally analytic morphism

$$j_{n,p} : \mathcal{X}(\mathbb{Z}_p) \to U_n^{\mathrm{dR}}(b)/F^0.$$

3.5 The universal connection

Let $b \in \mathcal{X}(\mathbb{Z}_p)$ be a virtual base-point. The goal of this subsection is to describe the map $j_{n,p}$ in a formal neighbourhood of b, following Kim [36]. Let $\mathcal{C}^{\mathrm{dR}}(X)$ denote the category of unipotent flat connections on X. A *pointed flat connection* will be a flat connection $\mathcal{V}$ on X, together with an element $v \in b^*\mathcal{V}$.

Definition 3.1 (The depth n universal connection, [36, section 1], [26, section 2]). The depth n universal connection $\mathcal{E}_n$ on a pointed geometrically integral variety (Z, b) is a pointed flat connection $(\mathcal{E}_n, e_n)$ that is n-unipotent, such that for all n-unipotent flat connections $\mathcal{V}$, and $v \in b^*\mathcal{V}$, there exists a unique morphism of connections $f : \mathcal{E}_n \to \mathcal{V}$ such that $b^*(f)(e_n) = v$. When we want to emphasise the dependence on Z, we write it as $\mathcal{E}_n(Z)$.

Lemma 3.8 *For all n, a universal n-unipotent pointed flat connection exists, and there is a canonical isomorphism*

$$\varprojlim b^*\mathcal{E}_n \simeq \mathcal{U}(\mathrm{Lie}(\pi_1^{\mathrm{dR}}(Z, b))),$$

where $\mathcal{U}(\mathrm{Lie}(\pi_1^{\mathrm{dR}}(Z, b)))$ denotes the universal enveloping algebra of the Lie algebra of $\pi_1^{\mathrm{dR}}(Z, b)$.

Proof More generally, we can define a depth n universal object in any Tannakian category $(\mathcal{C}, \omega)$ with as a pair $(\mathcal{V}_n, v_n)$, where $\mathcal{V}_n$ is an n-unipotent object of $\mathcal{C}$, v_n is an element of $\omega(\mathcal{V}_n)$, and for all n-unipotent objects $\mathcal{W}$, and $w \in \omega(\mathcal{W})$, there is a unique morphism $\mathcal{V}_n \to \mathcal{W}$ sending v_n to w.

If $F : (\mathcal{C}, \omega) \to (\mathcal{C}', \omega')$ is an equivalence of Tannakian categories, then it sends universal n-unipotent objects to universal n-unipotent objects. In particular, if $\mathcal{C}$ is the category $\mathcal{C}^{\mathrm{dR}}(Z)$ of unipotent flat connections on Z, with fibre functor b^*, then $\mathcal{C}$ has a universal n-unipotent object if and only if the category of representations of $\pi_1^{\mathrm{dR}}(\mathcal{C}^{\mathrm{dR}}(Z), b)$, with fibre functor given by the forgetful functor, does.

Using the equivalence between $\pi_1^{\mathrm{dR}}(\mathcal{C}^{\mathrm{dR}}(Z), b)$-representations and $\mathcal{U}(\mathrm{Lie}(\pi_1^{\mathrm{dR}}(Z, b)))$-modules, we see that $\mathcal{U}(\mathrm{Lie}(\pi_1^{\mathrm{dR}}(Z, b)))/I^{n+1}$ is a universal n-unipotent object, where I denotes the augmentation ideal. □

The following Lemma describes the morphisms of connections of the universal unipotent connection corresponding to certain natural morphisms of $\pi_1^{\mathrm{dR}}(Z, b)$ modules.

Lemma 3.9 *Let $\mathcal{E}_n$ be as above.*

(1) *Let $x \in b^*\mathcal{E}_n$, and let $m(-, x) : \mathcal{E}_n \to \mathcal{E}_n$ denote the unique morphism of connections which, in the fibre at b, sends 1 to x. Then, for all $y \in b^*\mathcal{E}_n$,*

$$y \cdot x = b^*(m(, x))(y).$$

More generally, for any unipotent flat connection $\mathcal{V}$, and any $v \in b^*\mathcal{V}, x \in \varprojlim b^*\mathcal{E}_n$, the action of x on v is given by $b^*(f)(x)$, where $f : \varprojlim \mathcal{E}_n \to \mathcal{V}$ is the unique (pro-)morphism of connections sending 1 to v.

(2) *Let*

$$\Delta : \varprojlim \mathcal{E}_n \to \varprojlim (\mathcal{E}_n \otimes \mathcal{E}_n) \tag{9}$$

denote the unique morphism of pro-connections which, in the fibre at b, sends 1 to $1\widehat{\otimes}1$. Then $b^*\Delta$ is equal to the co-multiplication on $\varprojlim b^*\mathcal{E}_n$.

Proof As in the proof of Lemma 3.8, it is enough to check this with $\mathcal{C}^{\mathrm{dR}}(Z)$ replaced by the category of $\pi_1^{\mathrm{dR}}(Z, b)$-representations. Hence part (1) is immediate. For part (2), the co-multiplication is a morphism of (pro-)representations of $\pi_1^{\mathrm{dR}}(Z, b)$. Hence, by universal properties, it is uniquely determined by the fact that it sends 1 to $1\widehat{\otimes}1$. □

Let Z' be an affine open of b, and let $\widehat{Z}$ denote the formal completion of Z at b. The bundle $\mathcal{E}_n$ is unipotent, and hence admits a trivialisation

$$\tau : \mathcal{E}_n|_{Z'} \xrightarrow{\simeq} \mathcal{O}_{Z'} \otimes b^*\mathcal{E}_n.$$

With respect to this trivialisation, the connection ∇_n is given by $d - \Lambda$, for some $\Lambda \in \mathrm{End}(b^*\mathcal{E}_n^{\mathrm{dR}}(b)) \otimes_K \Omega_{Z|K}$. The universal connection $(\mathcal{E}_n)$ carries a filtration by sub-bundles $(\varprojlim F^\bullet \mathcal{E}_n)$ satisfying the Griffiths transversality condition

$$\nabla_n(F^i\mathcal{E}_n) \subset F^{i-1}\mathcal{E}_n \otimes \Omega^1_{Z|K}$$

(see [26, §3]). Replacing Z' by a smaller affine open neighbourhood if necessary, we may choose a group-like section $(F_n) \in \varprojlim H^0(Z', F^0\mathcal{E}_n)$—i.e. a section which satisfies

$$\Delta((F_n)_n) = (F_n \widehat{\otimes} F_n)_n.$$

The connection $\mathcal{E}_n$ admits a trivialisation on $\widehat{Z}$, i.e. an isomorphism of connections

$$G : (\mathcal{E}_n|_{\widehat{Z}}, \nabla) \simeq (b^*\mathcal{E}_n^{\mathrm{dR}} \otimes_K \mathcal{O}(\widehat{Z}), d)$$

Via the trivialisation G, we may view F_n as a function $\widehat{Z} \to b^*\mathcal{E}_n$. Via the trivialisation τ, we obtain an endomorphism $(\tau|_{\widehat{Z}}) \circ G^{-1}$ in $\mathrm{End}(b^*\mathcal{E}_n) \otimes \mathcal{O}(\widehat{Z})$. This endomorphism sends 1 to something in $1 + I$ (recall that I denotes the augmentation ideal of $\varprojlim b^*\mathcal{E}_n$), hence we have a well-defined element

$$\boldsymbol{J}_{n,\tau} := \log((\tau|_{\widehat{Z}}) \circ G^{-1}(1)) \in Ib^*\mathcal{E}(Z) \widehat{\otimes} \mathcal{O}(\widehat{Z}),$$

In words, $\exp(\boldsymbol{J}_{n,\tau})$ is a horizontal section of $(\mathcal{E}_n, \nabla_n)$ on a formal neighbourhood of b, described with respect to the affine chart τ. In particular, by definition $\boldsymbol{J}_{n,\tau}(G)$ satisfies

$$d \exp(\boldsymbol{J}_{n,\tau}(G)) = \Lambda(\exp \boldsymbol{J}_{n,\tau}(G)). \tag{10}$$

Lemma 3.10 *The section* $\exp(\boldsymbol{J}_\tau) := (\exp(\boldsymbol{J}_{n,\tau}))_n$ *is group-like, i.e. it satisfies*

$$\Delta(\exp(\boldsymbol{J}_\tau)) = (\exp(\boldsymbol{J}_\tau)) \widehat{\otimes} (\exp(\boldsymbol{J}_\tau)).$$

Proof Since they are both horizontal sections of $\nabla_{\mathcal{E}\widehat{\otimes}\mathcal{E}}$, the left hand side and right hand side are equal if and only if they are equal at one fibre, and at b they both equal $1 \widehat{\otimes} 1$. □

We deduce that $\boldsymbol{J}_{n,\tau}$ lies in $L_n^{\mathrm{dR}}(Z) \widehat{\otimes} \mathcal{O}(\widehat{Z})$ (recall that $L_n^{\mathrm{dR}}(Z)$ is defined to be the Lie algebra of $U_n^{\mathrm{dR}}(Z)$). We also sometimes think of $\boldsymbol{J}_{n,\tau}$ as a morphism

$$\boldsymbol{J}_{n,\tau} : \widehat{Z} \to L_n^{\mathrm{dR}}(Z)$$

Remark 3.1 At this point, there is no obvious reason for working with $\boldsymbol{J}_{n,\tau}$ rather than $\exp(\boldsymbol{J}_{n,\tau})$. The reason for working with $\boldsymbol{J}_{n,\tau}$ is that, (as a consequence of (10)), $\boldsymbol{J}_{n,\tau}$ satisfies a particularly simple differential equation (see (21) and Lemma 4.6) which is used in the proof of the unlikely intersection result needed for the proof of Theorem 1.1.

Lemma 3.11 *Let X be a smooth geometrically irreducible curve over $\mathbb{Q}_p$, and b a $\mathbb{Q}_p$ point of X. Let τ be a trivialisation of $\varprojlim \mathcal{E}_n(b)$ as above. Then the unipotent Albanese morphism*

$$X(\mathbb{Q}_p) \to U_n^{\mathrm{dR}}(X_{\mathbb{Q}_p})/F^0$$

is given, on a formal neighbourhood of b, by $\exp(\boldsymbol{J}_{n,\tau}) \cdot F_n^{-1}$.

Proof This follows from Kim's explicit description of the map j_n in [36, §1]. The map j_n can be defined by sending z to the class of u in U_n^{dR}/F^0, where $u \in U_n^{\mathrm{dR}}$ is defined as follows: let p_ϕ be the unique element of $P_n^{\mathrm{dR}}(b, z)^{\phi=1}$, and choose $p_H \in F^0 P_n^{\mathrm{dR}}(b, z)$, then define u by $p_\phi = u \cdot p_H$. Although u depends on the choice of p_H, its class in U_n^{dR}/F^0 does not.

This is related to the parallel transport map as follows. The element $p^\phi(b, z)$ is an element of $\mathrm{Hom}(b^*\mathcal{E}_n, z^*\mathcal{E}_n)$. When b and z are on the same residue disk, this homomorphism is given by (rigid analytic) parallel transport (see [36], above Lemma 4). Hence, in a formal neighbourhood of b, it is given by $\exp(\boldsymbol{J}_{n,\tau})$, and similarly p_H is given by F_n, hence $u = \exp(\boldsymbol{J}_{n,\tau}) \cdot F_n^{-1}$. □

3.6 Higher Albanese manifolds

Recall that, given a quasi-projective variety Z over $\mathbb{C}$, we can define a higher Albanese manifold as follows [27, 28]. Let $U_n^{\mathrm{dR}}(Z)$ denote the n-unipotent de Rham fundamental group of Z. Let $U_n^{\mathrm{Be}}(Z)$ denote the $\mathbb{Q}$-unipotent Betti fundamental group of Z at b, i.e. the maximal n-unipotent quotient of the $\mathbb{Q}$-unipotent completion of $\pi_1(Z(\mathbb{C}), b)$. Abusing notation, we will denote by $U_n^{\mathrm{Be}}(Z)(\mathbb{Z})$ the image of $\pi_1(Z(\mathbb{C}), b)$ in $U_n^{\mathrm{Be}}(Z)(\mathbb{Q})$. By the Riemann–Hilbert correspondence, we have an isomorphism of unipotent groups over $\mathbb{C}$

$$U_n^{\mathrm{Be}}(Z)_{\mathbb{C}} \simeq U_n^{\mathrm{dR}}(Z).$$

The nth higher Albanese manifold of Z is the double quotient

$$\mathcal{H}_n := U_n^{\mathrm{Be}}(Z)(\mathbb{Z}) \backslash U_n^{\mathrm{dR}}(Z)(\mathbb{C}) / F^0 U_n^{\mathrm{dR}}(Z)(\mathbb{C}).$$

There is an nth higher Albanese map (see [28, §5])

$$j_n^{\mathrm{Be}} : Z(\mathbb{C}) \to \mathcal{H}_n,$$

which is a map of complex manifolds. Roughly speaking the definition in loc. cit. is as follows. For any $b, z \in Z(\mathbb{C})$, we may naturally give the path space

$$(\mathbb{Z}\pi_1(Z, b)/I^{n+1}) \times_{\pi_1(Z(\mathbb{C}),b)} \pi_1(Z(\mathbb{C}); b, z)$$

a mixed Hodge structure (where I is the augmentation ideal), in such a way that the associated graded is independent of b and z. This defines a map from $Z \times Z$ to a

variety of isomorphism classes of mixed Hodge structure with fixed associated graded. Fixing one component (i.e. restricting to $\{b\} \times Z$) one may then show that the image is contained in a variety isomorphic to $\mathcal{H}_n$.

The formal completion of $\mathcal{H}_n$ at the identity is isomorphic to the formal completion of $U_n^{\mathrm{dR}}(Z)(\mathbb{C})/F^0 U_n^{\mathrm{dR}}(Z)(\mathbb{C})$ at the identity, hence we have a morphism of formal schemes

$$\widehat{j}_n^{\mathrm{Be}} : \widehat{Z}_{\mathbb{C}} \to \widehat{U_n^{\mathrm{dR}}/F^0}_{\mathbb{C}}.$$

Lemma 3.12 *The formal completion of j_n^{Be} is given by is given by*

$$\widehat{j}_n^{\mathrm{Be}} = \exp(\boldsymbol{J}_{n,\tau}) \cdot F_n^{-1},$$

where $\boldsymbol{J}_{n,\tau}$ and F_n are as in Sect. 3.5. In particular, for any isomorphism $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$ we obtain an identification of the formal completions of $j_{n,p}$ at b (base changed to $\mathbb{C}$ and the formal completion of j_n^{Be} at b,

Proof This follows from the description of the unipotent Albanese morphism given in [28, §5] and [27, Proposition 3.2, (3.3)]. □

We deduce the following Lemma.

Lemma 3.13 *Let $i : Z \hookrightarrow \mathrm{Res}(X)_{\overline{\mathbb{Q}}_p}$ be an irreducible subvariety, and $b \in Z(\overline{\mathbb{Q}}_p) \cap \mathrm{Res}(X)(\mathbb{Q}_p)$. Let $\widehat{Z}$ and $\widehat{\mathrm{Res}(X)}_{\overline{\mathbb{Q}}_p}$ denote the formal completions at b. Then the restriction of $j_{n,p}$ to $\widehat{Z}$ lands in the image of $\widehat{U}_n^{\mathrm{dR}}(Z)/F^0$ in $\widehat{U}_n^{\mathrm{dR}}(\mathrm{Res}(X))/F^0$, and the diagram*

$$\begin{array}{ccc} \widehat{Z}_b & \xrightarrow{\exp(\boldsymbol{J}_{n,\tau}) \cdot F_n^{-1}} & \widehat{U}_n^{\mathrm{dR}}(Z)/F^0 \\ \downarrow & & \downarrow \\ \widehat{\mathrm{Res}(X)}_b & \xrightarrow{\widehat{j}_n} & \widehat{U}_n^{\mathrm{dR}}(\mathrm{Res}(X))/F^0. \end{array}$$

commutes. In particular, the pre-image of the graph of j_n in $\widehat{Z} \times \widehat{U}_n^{\mathrm{dR}}/F^0$ under the map

$$\begin{aligned} \widehat{Z} \times L_n^{\mathrm{dR}}(Z) &\to \widehat{\mathrm{Res}(X)} \times \widehat{U}_n^{\mathrm{dR}}/F^0 \\ (z, x) &\mapsto (i(z), \exp(x) \cdot F_n^{-1}(z)) \end{aligned}$$

is equal to the graph of $\boldsymbol{J}_{n,\tau}$.

Proof This follows from the previous lemma, together with the fact that Hain's higher Albanese morphism is functorial in complex manifolds [28, §3]. □

4 Unlikely intersections among zeroes of iterated integrals

The aim of this section is to prove the following proposition, which is the unlikely intersection result needed to establish Theorem 1.1. Given a scheme V, and a formal subscheme W of the formal completion of V at a point x, we say that W is Zariski dense if there is no proper closed subscheme of V whose formal completion at x contains W.

Proposition 4.1 *Let Z be a smooth irreducible subvariety of $\mathrm{Res}(X)_{\overline{\mathbb{Q}}_p}$. Let V be an irreducible subvariety of $L_n^{\mathrm{dR}}(Z) \times Z$, containing $(0, b) \in L_n^{\mathrm{dR}}(Z) \times Z$, such that the projection of V to Z is dominant and $(0, b)$ is a smooth point of V. Let $\widehat{V}$ and $\widehat{L}_n^{\mathrm{dR}}(Z)$ denote the formal completions of V and $L_n^{\mathrm{dR}}(Z)$ at b and 0 respectively. Let $\Delta \subset \widehat{L}_n^{\mathrm{dR}}(Z) \times \widehat{Z}$ denote the graph of $\boldsymbol{J}_{n,\tau}$. Let $W = \Delta \cap \widehat{V}$. Suppose W is irreducible and*

$$\mathrm{codim}_{\Delta} W < \mathrm{codim}_{L_n^{\mathrm{dR}}(Z)\times Z} V.$$

Then W is not Zariski dense in V.

For example, we can apply this result when V is the Zariski closure of Δ, and $W = \Delta$. Then W is Zariski dense in V by definition, and hence we deduce

$$0 = \mathrm{codim}_{\Delta}(W) = \mathrm{codim}_{L_n^{\mathrm{dR}}(Z)\times Z} V. \tag{11}$$

(i.e. the graph of $\boldsymbol{J}_{n,\tau}$ is Zariski dense in $L_n^{\mathrm{dR}}(Z) \times Z$). This could also more elegantly be proved following the topological argument in [21].

Proposition 4.1 can be informally thought of as saying that algebraic relations between n-unipotent iterated integrals must have a geometric explanation. In the $1-$unipotent (or abelian) case, this is due to Ax [2]. The idea of the general proof is inspired by Ax's approach: we inductively show that non-trivial algebraic relations between n-unipotent iterated integrals come from geometry by differentiating them to produce relations between $(n-1)$-unipotent iterated integrals (the difficult part being to show that these relations must also be non-trivial).

We also note that this Proposition translates into a criterion for finiteness of $\mathrm{Res}(\mathcal{X})(\mathbb{Z}_p)_n$ which will be used repeatedly in subsequent sections. To state the criterion, we introduce the following notation: for $(Z, z) \to (Y, y)$ a morphism of varieties over a field L sending z to y, we define $U_n(Z/Y) \subset U_n(Y) = U_n(Y)(y)$ to be the image of $\pi_1^{\text{ét},\mathbb{Q}_p}(Z_{\overline{L}}, z)$ in $U_n(Y)$. For $i \leq n$, we define

$$\mathrm{gr}_i(U_n(Z/Y)) := \mathrm{Ker}(U_i(Z/Y) \to U_{i-1}(Z/Y)),$$

and similarly for $U_i^{\mathrm{dR}}(Z/Y)$. Note that, in general, $\mathrm{gr}_i(U_i(Z/Y))$ is not the same as $C_i(U_i(Z/Y))/C_{i+1}(U_i(Z/Y))$. Since the homomorphism

$$\pi_1^{\text{ét},\mathbb{Q}_p}(Z_{\overline{L}}, z) \to \pi_1^{\text{ét},\mathbb{Q}_p}(Y_{\overline{L}}, y)$$

respects the central series filtrations, we have an induced morphism

$$U_n(Z, z) \to U_n(Y, y),$$

however this morphism need not be strict with respect to the central series filtration. For example, this non-strictness occurs when $Z = E - \{x_1, x_2\}$, for E an elliptic curve with points x_1 and x_2, $Y = (E - \{x_1\}) \times (E - \{x_2\})$, and the map is the diagonal embedding $Z \to Y$. However if X is projective morphisms will be strict, since the weight filtration on U_n will agree with the central series filtration.

Proposition 4.2 *Suppose that, for every irreducible subvariety $Z \subset \mathrm{Res}(X)_{\mathbb{Q}_p}$, we have*

$$\mathrm{codim}_{U_n^{\mathrm{dR}}(Z/\mathrm{Res}(X))/F^0}(\mathrm{loc}_p(\mathrm{Sel}(U_n)) \cap U_n^{\mathrm{dR}}(Z/\mathrm{Res}(X))/F^0) \geq \dim Z. \quad (12)$$

Then $\mathrm{Res}(X)(\mathbb{Z}_p)_n$ is finite.

Proof Fix an $\mathbb{F}_p$ point $\overline{b}$ of $\mathrm{Res}(X)$. Let $\widetilde{Z} \subset \mathrm{Res}(X)_{\mathbb{Q}_p}$ denote the Zariski closure of $\mathrm{Res}(\mathcal{X})(\mathbb{Z}_p)_n \cap]\overline{b}[$. Let $\widetilde{Z} = Z_0 \sqcup Z_1 \sqcup \cdots \sqcup Z_N$ be a stratification of $\widetilde{Z}$ into smooth irreducible subvarieties. Since $\widetilde{Z}$ is the Zariski closure of a set of $\mathbb{Q}_p$-points of $\mathrm{Res}(X)_{\mathbb{Q}_p}$, the irreducible components are geometrically irreducible. Let $Z = Z_i$ be a component of the stratification. To prove finiteness of $\mathrm{Res}(\mathcal{X})(\mathbb{Z}_p)_n$, it will be enough to prove that $Z \cap \mathrm{Res}(\mathcal{X})(\mathbb{Z}_p)_n$ is zero dimensional. We do this using Proposition 4.1 applied to Z.

To apply Proposition 4.1, we must define a subvariety V of $Z \times L_n^{\mathrm{dR}}(Z)$ where $(b, 0)$ is smooth. We do this in the next two paragraphs. If there is a point b' of $\mathrm{Res}(X)(\mathbb{Z}_p)_n \cap Z \cap]\overline{b}[$ where $j_n(b')$ is a smooth point of $\mathrm{loc}_p(\mathrm{Sel}(U_n)) \cap U_n^{\mathrm{dR}}(Z/Y)/F^0$ (here and below, we view this as a reduced subscheme of $U_n^{\mathrm{dR}}(Z/Y)/F^0$), then we define $V_0 := \mathrm{loc}_p(\mathrm{Sel}(U_n)) \cap U_n^{\mathrm{dR}}(Z/Y)/F^0$. If not, then $j_n(\mathrm{Res}(X)(\mathbb{Z}_p)_n \cap Z \cap]\overline{b}[)$ lands in the singular locus of $\mathrm{loc}_p(\mathrm{Sel}(U_n(b))) \cap U_n^{\mathrm{dR}}(Z/Y, b)/F^0$, and hence stratifying as above there is a proper closed subvariety V_0 of $\mathrm{loc}(\mathrm{Sel}(U_n) \cap U_n^{\mathrm{dR}}(Z/Y)/F^0$ which contains $j_n(\mathrm{Res}(X)(\mathbb{Z}_p)_n \cap Z \cap]\overline{b}[)$ and a point b' of $\mathrm{Res}(X)(\mathbb{Z}_p)_n \cap Z \cap]\overline{b}[)$ such that $j_n(b')$ is a smooth point of V_0. By Lemma 3.5, we may assume $b = b'$. Since our condition on b holds outside a closed analytic subset, we may also assume that the formal completion of $\mathrm{Res}(X)(\mathbb{Z}_p)_n \cap Z$ at b is irreducible.

Let W_0 denote the formal completion of $\mathrm{Res}(\mathcal{X})(\mathbb{Z}_p)_n \cap Z$ at b. Recall that, by Lemma 3.13, the pre-image of the graph of j_n in $\widehat{Z}_b \times \widehat{L}_n^{\mathrm{dR}}(Z)$ is given by the graph of $\boldsymbol{J}_{n,\tau}$. We apply Proposition 4.1 with V being the product of Z with the pre-image of V_0 in $L_n^{\mathrm{dR}}(Z)$. By our choice of b, $W := V \cap \Delta$ is an irreducible formal scheme (recall Δ is the graph of $\boldsymbol{J}_{n,\tau}$). We then apply Proposition 4.1 to deduce

$$\mathrm{codim}_{\Delta}(W) \geq \mathrm{codim}_{L_n^{\mathrm{dR}}(Z)} V. \quad (13)$$

On the other hand by definition of V we have

$$\mathrm{codim}_{Z \times L_n^{\mathrm{dR}}(Z)}(V) \geq \mathrm{codim}_{U_n^{\mathrm{dR}}(Z/Y)/F^0}(\mathrm{loc}_p(\mathrm{Sel}(U_n)) \cap U_n^{\mathrm{dR}}(Z/Y)/F^0). \quad (14)$$

Since $j(W_0) \subset \mathrm{loc}_p(\mathrm{Sel}(U_n))$, we have $W_0 \subset W$, and (12), (14) and (13) together imply the Lemma. □

4.1 Universal connections and reduced form

In the proof of Proposition 4.1, it will be useful to have a fairly explicit description of the map $\boldsymbol{J}_{n,\tau}$, and hence of the connection $(\mathcal{E}_n, \nabla_n)$. For this, we introduce the notion of the *reduced form* of a connection, which is inspired by Kim's description of the universal connection [36]. As above, Z is a smooth irreducible affine subvariety of $\mathrm{Res}(X)_{\overline{\mathbb{Q}}_p}$. Let d_n denote the rank of $\mathcal{E}_n$, and let r_n denote the dimension of $U_n^{\mathrm{dR}}(Z)$.

Definition 4.1 (Reduced form) Let Q be a complement of $d\mathcal{O}(Z)$ in $H^0(Z, \Omega)$.

A n-nilpotent matrix $M \in \mathrm{End}(\oplus_{i=0}^n V_i) \otimes H^0(Z, \Omega)$ (for $V_0, \ldots, V_n$ vector spaces over K) is in reduced form (relative to the complement Q) if it is block n-nilpotent and all of its entries lie in Q.

An n-unipotent connection $(\mathcal{V}, \nabla)$ in reduced form is an isomorphism $\mathcal{V} \simeq \oplus_{i=0}^n \mathcal{O}_Z \otimes V_i$ with respect to which $\nabla = d + \Lambda$, where $\Lambda \in \mathrm{End}(\oplus V_i) \otimes H^0(Z, \Omega)$ is an n-nilpotent matrix in reduced form.

Lemma 4.1 *Let $\mathcal{V}$ be an n-unipotent connection on a smooth affine variety Z over a field K of characteristic zero. Then $\mathcal{V}$ can be written in reduced form. All morphisms f between connections $(\oplus V_i \otimes \mathcal{O}_Z, \nabla)$, $(\oplus W_i \otimes \mathcal{O}_Z, \nabla')$ in reduced form are K-linear, i.e. $f \in \mathrm{Hom}(\oplus V_i, \oplus W_j) \otimes \mathcal{O}(Z)$ actually has entries in $\mathrm{Mat}_{n,m}(K)$.*

Proof This may be proved in a similar fashion to [36, Lemma 2]. We argue by induction on n, the case $n = 0$ being immediate. If $\mathcal{V}$ is an extension of an $(n-1)$-unipotent connection $\mathcal{V}'$ by a trivial connection $\mathcal{V}'' = (V'' \otimes \mathcal{O}, d)$, then we can assume $\mathcal{V}'$ can be written in reduced form, say

$$\mathcal{V}' \simeq \oplus_{i=0}^{n-1} \mathcal{V}_i \simeq \oplus_{i=0}^{n-1} V_i \otimes \mathcal{O}$$

so that $\nabla_{\mathcal{V}'} = d + \Lambda$, where $\Lambda = \sum_{0 \le i < j < n} \Lambda_{ij}$ and $\Lambda_{ij} \in \mathrm{Hom}(V_i, V_j) \otimes Q$. Since Z is affine, we can choose a vector bundle splitting of the short exact sequence

$$0 \to \mathcal{V}'' \to \mathcal{V} \to \mathcal{V}' \to 0, \tag{15}$$

so that we can write $\mathcal{V}$ as $\mathcal{V}' \oplus \mathcal{V}''$, with connection given by $d + \Lambda + \Lambda'$, where $\Lambda' \in \mathrm{Hom}(\mathcal{V}', \mathcal{V}'') \otimes H^0(Z, \Omega)$. We want to show that, changing the basis by an element of $1 + \mathrm{Hom}(\mathcal{V}', \mathcal{V}'')$, we can make Λ' of the form $\sum \Lambda'_i$, where

$$\Lambda'_i \in \mathrm{Hom}(V_i, V'') \otimes Q. \tag{16}$$

Write Λ' as $\sum \Lambda'_i$, with Λ'_i in $\mathrm{Hom}(V_i, V'') \otimes H^0(Z, \Omega)$. If we change the splitting of (15) by $1 + \sum M_i$, where $M_i \in \mathrm{Hom}(\mathcal{V}_i, \mathcal{V}'')$, this will change Λ' by

$$\Lambda'_i \mapsto \Lambda'_i + dM_i - \sum_{j>i} M_j \circ \Lambda_{ij}. \tag{17}$$

We show that we can change our basis so that the Λ_i' satisfy (16) by descending induction on i. When $i = n-1$, (16) implies that there is an $M \in \mathrm{Hom}(\mathcal{V}_{n-1}, \mathcal{V}'')$ such that

$$\Lambda_{n-1}' - dM \in \mathrm{Hom}(V_{n-1}, V'') \otimes Q.$$

Changing the splitting of (15) by M, we obtaining a splitting for which Λ_{n-1}' satisfies (16). Now suppose we have a splitting of (15) such that $\Lambda_{n-1}', \ldots, \Lambda_{n-i+1}'$ satisfy (16). Then (16) implies there is an $M \in \mathrm{Hom}(\mathcal{V}_{n-i}, \mathcal{V}'')$ such that

$$\Lambda_{n-i}' - dM \in \mathrm{Hom}(V_{n-i}, V'') \otimes Q.$$

If we change the splitting of (15) by M, then by (17), $\Lambda_{n-1}', \ldots, \Lambda_{n-i+1}$ will be unchanged, and Λ_{n-i} will now lie in $\mathrm{Hom}(V_{n-i}, V'') \otimes Q$. Hence $\mathcal{V}$ is in reduced form.

For the second part of the lemma, write the homomorphism f as $\sum f_{ij}$, where $f_{ij} \in \mathrm{Hom}(\oplus V_i, \oplus W_j) \otimes \mathcal{O}(Z)$. Write $\nabla = d + \sum_{i<j} \Lambda_{ij}$ and $\nabla' = d + \sum_{i<j} \Lambda_{ij}'$ with the notation as above. Then the identity

$$df_{ij} + \sum_{k<j} \Lambda_{kj}' f_{ik} = \sum_{i<k} f_{kj} \Lambda_{ik},$$

and the fact that $Q \cap d\mathcal{O}(Z) = 0$, shows $df_{ij} = 0$ for all i and j by a double induction on i and j. □

Definition 4.2 We write $\mathcal{E}_n$ in reduced form as $\oplus_{i=0}^{d_n} \mathcal{O}_Z \cdot e_i$ (i.e. we write it in reduced form, and then pick a basis for each vector space V_i), and $\nabla_n = d + \Lambda_n$. The matrix Λ_n is n-nilpotent, and its upper left k-nilpotent submatrix is equal to $\mathcal{E}_k$, for all $k < n$ (i.e. the quotient $\mathcal{E}_n \to \mathcal{E}_k$ is just given by projecting onto the first $(k+1)$-blocks). If τ is a trivialisation of $\mathcal{E}_n$ coming from its reduced form, we denote $\boldsymbol{J}_{n,\tau}$ simply by $\boldsymbol{J}_n$.

4.2 An explicit description of the universal connection

The main result of this section is a differential equation satisfied by $\boldsymbol{J}_n$, which is used in the inductive step of the proof of Proposition 4.1. Let $\mathcal{E}_n \simeq \mathcal{O}_Z^{\oplus d_n}$ be a bundle trivialisation of $\mathcal{E}_n$ putting it in reduced form. Let Λ_n be the connection matrix for its reduced form. Recall that by Lemma 3.8, $\varprojlim b^*\mathcal{E}_n$ is isomorphic via Tannaka duality to the universal enveloping algebra of $\pi_1^{\mathrm{dR}}(Z, b)$, viewed as a pro-representation of $\pi_1^{\mathrm{dR}}(Z, b)$. Recall that the Lie algebra $L_\infty^{\mathrm{dR}}(Z) \subset \varprojlim b^*\mathcal{E}_n$ is defined to be the subspace satisfying $\epsilon(x) = 0$ and $\Delta(x) = x\widehat{\otimes}1 + 1\widehat{\otimes}x$, and $L_n^{\mathrm{dR}}(Z) \subset b^*\mathcal{E}_n$ is the image of $\mathrm{Lie}(\pi_1^{\mathrm{dR}}(Z, b))$ in $b^*\mathcal{E}_n$. By making a K-linear change of basis (preserving the unipotent filtration) if necessary, we may (and do) henceforth assume that there is a sub-basis e_{l_i} of e_i forming a basis of $L_n^{\mathrm{dR}}(Z)$. Define $b_{ijk} \in K$, $1 \leq i, j, k \leq r_n$, by

$$[e_{l_i}, e_{l_j}] = \sum b_{ijk} e_{l_k}. \tag{18}$$

Lemma 4.2 *There is an element* $\boldsymbol{\omega} = \sum_{i=1}^{r_n} e_{l_i} \otimes \omega_i$ *of* $L_n^{\mathrm{dR}}(Z) \otimes H^0(Z, \Omega)$ *such that the connection* ∇_n *on* $\mathcal{E}_n$ *is given by*

$$v \mapsto \boldsymbol{\omega} \cdot v + dv,$$

and $\boldsymbol{\omega} = \nabla(1_n)$.

Proof First, we show that $\boldsymbol{\omega} := \nabla(1_n)$ has the property that, for all v in $b^*\mathcal{E}_n$, $\nabla(v \otimes 1) = \boldsymbol{\omega} \cdot v$. Let f be the unique morphism $\mathcal{E}_n \to \mathcal{E}_n$ such that $b^*(f)(1_n) = v$. Then, since f is K-linear with respect to the trivialisation, we have

$$\nabla(v \otimes 1) = f(\boldsymbol{\omega}).$$

By Lemma 3.9, $f(\boldsymbol{\omega}) = \boldsymbol{\omega} \cdot v$.

We now show that $\boldsymbol{\omega}$ is in $L_n^{\mathrm{dR}}(Z) \otimes H^0(Z, \Omega)$. It is convenient to instead show this in the limit over n: i.e. that $\boldsymbol{\omega} \in \varprojlim H^0(Z, \mathcal{E}_n \otimes \Omega^1)$ lies in $\varprojlim H^0(Z, L_n^{\mathrm{dR}}(Z) \otimes \Omega^1)$. Since, in $\mathcal{E}_0$, we have $\nabla(1_0) = 0$, the first condition $\boldsymbol{\omega} \in \mathrm{Ker}(\epsilon \otimes 1)$ is satisfied. The second condition is that $\Delta(\boldsymbol{\omega}) = \boldsymbol{\omega}\widehat{\otimes}1_n + 1_n\widehat{\otimes}\boldsymbol{\omega}$. By Lemma 3.9, Δ is the unique morphism of pro-connections

$$\varprojlim \mathcal{E}_n \to \varprojlim (\mathcal{E}_n \otimes \mathcal{E}_n)$$

sending (1_n) to $(1_n \otimes 1_n)$. Hence $\Delta(\boldsymbol{\omega}) = \nabla(1_n\widehat{\otimes}1_n) = \boldsymbol{\omega}\widehat{\otimes}1_n + 1_n\widehat{\otimes}\boldsymbol{\omega}$, by definition of the tensor product of two connections. □

We write $\boldsymbol{J} = \sum J_i \otimes e_{l_i} \in \mathcal{O}(\widehat{Z}) \otimes L_n^{\mathrm{dR}}(Z)$. Recall $\boldsymbol{J}(b) = 0$ and

$$d\exp(\boldsymbol{J}) = \boldsymbol{\omega} \cdot \exp(\boldsymbol{J}) \tag{19}$$

in $H^0(\widehat{Z}, \Omega)$. Let $t_i \in \mathcal{O}(\widehat{L}_n^{\mathrm{dR}}(Z))$ be the ith coordinate function with respect to the basis (e_{l_i}). Define

$$\boldsymbol{t} = \sum t_i \otimes e_{l_i} \in H^0(L_n^{\mathrm{dR}}(Z), \mathcal{O}) \otimes L_n^{dR}(Z).$$

Recall $\Delta \subset \widehat{Z} \times \widehat{L}_n^{\mathrm{dR}}(Z)$ denotes the graph of $\boldsymbol{J}$. Then Δ is the zero set of the functions $t_i - J_i$ (here we view t_i and J_i as functions on $\widehat{Z} \times \widehat{L}^{\mathrm{dR}}(Z)$ via pulling back; to ease notation we suppress the pull-back from the notation).

To describe the derivative of $\boldsymbol{J}$, we make use of Poincaré's Lemma on the derivative of the exponential function. Given an N-nilpotent Lie algebra L, and a formal power series $F = \sum_{i \geq 0} a_i t^i$, and $x \in L$, we write $F(\mathrm{ad}_x)$ to mean the operator $\sum_{i=0}^{N} a_i (\mathrm{ad}_x)^i$ on L. Finally, if F, G are nonzero power series in $K[\![t]\!]$ such that $H := F/G$ lies in $K[\![t]\!]$, we further abuse notation by writing $F(\mathrm{ad}_x)/G(\mathrm{ad}_x)$ to mean the operator $H(\mathrm{ad}_x)$.

Lemma 4.3 *Let* $\exp : L_n^{\mathrm{dR}}(Z) \to b^*\mathcal{E}_n(Z)$ *denote the exponential function. Then*

$$d\exp(x) = \frac{e^{\mathrm{ad}_x} - 1}{\mathrm{ad}_x}(dx) \cdot e^x.$$

Proof It will be enough to prove this identity in the universal enveloping algebra of $L_n^{\mathrm{dR}}(Z)$, as $b^*\mathcal{E}_n(Z)$ is a quotient of the universal enveloping algebra of $L_n^{\mathrm{dR}}(Z)$, compatible with the exponential and logarithm maps. Hence this follows from the usual version of Poincaré's formula (see e.g. [11, II.5.11]). □

We define $\widetilde{\theta}_i \in H^0(L_n^{\mathrm{dR}}(Z) \times Z, \Omega)$ by

$$\sum \widetilde{\theta}_i \otimes e_{l_i} = \widetilde{\boldsymbol{\theta}} := \frac{e^{\mathrm{ad}_{\boldsymbol{t}}} - 1}{\mathrm{ad}_{\boldsymbol{t}}} d\boldsymbol{t} - \boldsymbol{\omega}.$$

We define θ_i to be the image of $\widetilde{\theta}_i$ in $H^0(V, \Omega)$ and $\overline{\theta}_i$ to be the image of θ_i in $H^0(V, \Omega) \otimes \mathcal{O}(W)$.

Remark 4.1 The θ_i have the following interpretation in terms of foliations on principal bundles. The frame bundle on $\mathcal{E}_n^{\mathrm{dR}}$ descends to a U_n^{dR}-bundle P. The choice of trivialisation of $\mathcal{E}_n^{\mathrm{dR}}$ on Z defines a trivialisation of P, i.e. an isomorphism $P \simeq U_n^{\mathrm{dR}} \times Z$. With respect to this isomorphism, the connection form Ω on P can be viewed as an element of $H^0(Z \times U_n^{\mathrm{dR}}, \Omega) \otimes L_n^{\mathrm{dR}}$. As explained in [7, 2.7], the connection form is given by $\boldsymbol{t}^{-1}d\boldsymbol{t} - \boldsymbol{t}^{-1}\boldsymbol{\omega}\boldsymbol{t}$. Via the exponential map, this may be viewed as an element Ω' of $H^0(Z \times L_n^{\mathrm{dR}}, \Omega) \otimes L_n^{\mathrm{dR}}$. Then we see that

$$\Omega' = \boldsymbol{t}^{-1}\widetilde{\boldsymbol{\theta}}\boldsymbol{t}.$$

Hence finding linear relations between the θ_i is equivalent to finding linear relations between the coefficients of Ω, as in the proof of Theorem 3.6 of loc. cit.

Let V and W be as in Proposition 4.1. Let $I \subset \mathcal{O}(\widehat{V})$ denote the ideal of functions vanishing on W. We have an exact sequence [24, 20.7.20]

$$I/I^2 \to \widehat{\Omega}_{\widehat{V}|\overline{\mathbb{Q}}_p} \otimes \mathcal{O}(W) \to \widehat{\Omega}_{W|\overline{\mathbb{Q}}_p} \to 0. \tag{20}$$

Lemma 4.4 *The image of* I/I^2 *in* $\widehat{\Omega}_{V|K} \otimes \mathcal{O}(W)$ *under*

$$I/I^2 \to \widehat{\Omega}_{\widehat{V}|K} \otimes \mathcal{O}(W)$$

is spanned by $\overline{\theta}_1, \ldots, \overline{\theta}_{r_n}$.

Proof The image of I/I^2 is spanned by the functions $dt_1 - dJ_1, \ldots, dt_{r_n} - dJ_{r_n}$, so it will be enough to show that the submodule spanned by these differentials is equal to the submodule spanned by $\theta_1, \ldots, \theta_{r_n}$. By (10) and Lemma 4.2, $\exp(\boldsymbol{J})$ satisfies

$$d(\exp(\boldsymbol{J})) = \boldsymbol{\omega} \cdot \exp(\boldsymbol{J}).$$

Hence, by Lemma 4.3, the function $\boldsymbol{J}$ satisfies the differential equation

$$d\boldsymbol{J} = \frac{\mathrm{ad}_{\boldsymbol{J}}}{e^{\mathrm{ad}_{\boldsymbol{J}}} - 1}(\boldsymbol{\omega}). \tag{21}$$

Hence the image of I/I^2 is equal to the submodule spanned by

$$d\boldsymbol{t} - \frac{\mathrm{ad}_{\boldsymbol{t}}}{e^{\mathrm{ad}_{\boldsymbol{t}}} - 1}(\boldsymbol{\omega}). \tag{22}$$

since $t_i = J_i$ on W. Finally, the map

$$\boldsymbol{v} \mapsto \frac{e^{\mathrm{ad}_{\boldsymbol{t}}} - 1}{\mathrm{ad}_{\boldsymbol{t}}}(\boldsymbol{v})$$

is an $\mathcal{O}(W)$-linear automorphism of $L_n^{\mathrm{dR}}(Z) \otimes \mathcal{O}(W)$, hence the submodule spanned by the coordinates of $\boldsymbol{\theta}$ is equal to the submodule spanned by the coordinates of $\frac{\mathrm{ad}_{\boldsymbol{t}}}{e^{\mathrm{ad}_{\boldsymbol{t}}} - 1} \cdot \boldsymbol{\theta}$, which equals (22). □

4.3 Proof of Proposition 4.1

We suppose that the codimension of Δ in W is less than the codimension of V in $L_n^{\mathrm{dR}}(Z) \times Z$. Let $\overline{\mathbb{Q}}_p(V)$ denote the function field of V, and $\overline{\mathbb{Q}}_p(W)$ the function field of W. By the exact sequence (20)

$$I/I^2 \otimes \overline{\mathbb{Q}}_p(W) \to \widehat{\Omega}_{\widehat{V}_{\overline{\mathbb{Q}}_p}|\overline{\mathbb{Q}}_p} \otimes \overline{\mathbb{Q}}_p(W) \to \widehat{\Omega}_{\overline{\mathbb{Q}}_p(W)|\overline{\mathbb{Q}}_p} \to 0$$

and the inequality $\dim(W) \leq \mathrm{rk}\, \widehat{\Omega}_{W|\overline{\mathbb{Q}}_p}$, we deduce that $\overline{\theta}_1, \ldots, \overline{\theta}_{r_n}$ are linearly dependent in $\widehat{\Omega}_{\widehat{V}|\overline{\mathbb{Q}}_p} \otimes \overline{\mathbb{Q}}_p(W)$. We henceforth assume that W is Zariski dense in V, and assume, as hypothesis for contradiction, that the $\overline{\theta}_i$ are $\overline{\mathbb{Q}}_p(W)$-linearly dependent. By our assumption that W is Zariski dense in V, this implies that the θ_i are $\overline{\mathbb{Q}}_p(V)$-linearly dependent. In this subsection, we aim to show that such a dependence contradicts the Zariski density of W. The following elementary Lemma gives a couple of ways to prove that a formal sub-scheme is not Zariski dense.

Lemma 4.5 *Let V be an integral variety over $\overline{\mathbb{Q}}_p$ and W an integral closed formal subscheme of the formal completion of V at a $\overline{\mathbb{Q}}_p$-point b at which V is smooth.*

(1) *Suppose there are h_1, h_2 in $\overline{\mathbb{Q}}_p(V)$ such that $h_1 dh_2$ is zero in $\Omega_{\overline{\mathbb{Q}}_p(W)|\overline{\mathbb{Q}}_p}$, but non-zero in $\Omega_{\overline{\mathbb{Q}}_p(V)|\overline{\mathbb{Q}}_p}$. Then W is not Zariski dense in V.*

(2) *Let M be an $\mathcal{O}_V$-submodule of $\mathcal{O}_V^{\oplus r}$. Suppose the $\overline{\mathbb{Q}}_p(W)$-rank of the image of $M \otimes \overline{\mathbb{Q}}_p(W)$ in $\overline{\mathbb{Q}}_p(W)^{\oplus r}$ is less than the $\overline{\mathbb{Q}}_p(V)$-rank of $M \otimes \overline{\mathbb{Q}}_p(V)$. Then W is not Zariski dense in V.*

Proof (1) If $h_1 dh_2 = 0$ then either $h_1 = 0$ or $dh_2 = 0$. Write $h_i = f_i/g_i$, with $f_i, g_i \in \mathcal{O}_{V,b}$. Then in the first case W is contained in the zero locus of f_1. In the second case h_2 is constant on W, say equal to λ, and hence W is contained in the zero locus of $f_2 - \lambda g_2$.

(2) Suppose the generic rank of M is s, and $m_1, \ldots, m_s$ are generically independent elements of M, say $m_i = \sum f_{ij} e_j$. Then W is contained in the zero set of the determinants of the (s, s)-minors of (f_{ij}).

□

Combining this with Lemma 4.4, we deduce that to prove Proposition 4.1, it will be enough to prove that, if $\theta_1, \ldots, \theta_{r_n}$ are not $\overline{\mathbb{Q}}_p(V)$-linearly independent, then there exists $h_1, h_2 \in \overline{\mathbb{Q}}_p(V)$ such that $h_1 dh_2 \neq 0$, and $h_1 dh_2$ is in the $\overline{\mathbb{Q}}_p(V)$-span of $\theta_1, \ldots, \theta_{r_n}$. We prove this by induction on n.

The case $n = 1$ is elementary: in this case θ_i is of the form $dt_i - \omega_i$, where $\omega_1, \ldots, \omega_{r_1}$ are closed 1-forms forming a basis of $H^1_{\mathrm{dR}}(Z/\overline{\mathbb{Q}}_p)$. Suppose

$$\sum_{i=1}^{r_1} a_i \theta_i = 0 \tag{23}$$

in $\Omega_{\overline{\mathbb{Q}}_p(V)|\overline{\mathbb{Q}}_p}$. Suppose (23) is minimal among all non-trivial relations, in the sense that it has a minimal number of nonzero a_i among all relations (23) for which the a_i are not identically zero. Without loss of generality a_1 is non-zero, and re-scaling if necessary, we may assume $a_1 = 1$. Since ω_i are closed for $i \leq r_1$, we have

$$da_i \wedge \theta_i = d(\sum a_i \wedge \theta_i) = 0$$

in $\Omega^2_{\overline{\mathbb{Q}}_p(V)|\overline{\mathbb{Q}}_p}$. If all of the da_i are zero in $\Omega_{\overline{\mathbb{Q}}_p(V)|\overline{\mathbb{Q}}_p}$, then we have

$$d\left(\sum a_i t_i\right) = \sum a_i \omega_i,$$

hence the map $H^1_{\mathrm{dR}}(Z_{\overline{\mathbb{Q}}_p}/\overline{\mathbb{Q}}_p) \to H^1_{\mathrm{dR}}(V/\overline{\mathbb{Q}}_p)$ has a non-trivial kernel. Dually, this implies that the map on Albanese varieties is not dominant, and hence that $V \to Z$ is not dominant, giving a contradiction.

If the da_i are not all zero, but are in the $\overline{\mathbb{Q}}_p(V)$-span of the θ_i, then the Proposition is proved, by Lemma 4.5. Hence we reduce to the case that the da_i are not all zero, and not all in the $\overline{\mathbb{Q}}_p(V)$-span of the θ_i (say $da_2 \notin \sum \overline{\mathbb{Q}}_p(V) \cdot \theta_i$). Then there is a derivation

$$D : \Omega_{\overline{\mathbb{Q}}_p(V)|\overline{\mathbb{Q}}_p} \to \overline{\mathbb{Q}}_p(V)$$

for which $D(\theta_i) = 0$ for all i but $D(da_2) \neq 0$. Then

$$\sum D(da_i) \cdot \theta_i = 0$$

is a non-trivial relation, which has fewer non-zero terms than (23) since $da_1 = 0$, contradicting our assumption that (23) was minimal.

Now suppose $n > 1$, and let M_k denote the submodule of $\Omega_{\overline{\mathbb{Q}}_p(V)|\overline{\mathbb{Q}}_p}$ spanned by $\theta_1, \ldots, \theta_{r_k}$. We suppose that

$$\{h_1 dh_2 : h_1, h_2 \in \overline{\mathbb{Q}}_p(V)\} \cap M_n = 0.$$

Hence, by induction rk $M_{n-1} = r_{n-1}$. Suppose as hypothesis for contradiction that rk $M_n < r_n$, and hence there are non-zero $a_i \in \overline{\mathbb{Q}}_p(V)$ such that

$$\sum_{i=1}^{r_n} a_i \theta_i = 0. \tag{24}$$

To deduce the inductive step, we use the following differential equation satisfied by the θ_i (in the notation of Remark 4.1, this identity could also be deduced from the Cartan structure equation for the connection form Ω).

Lemma 4.6 *$\widetilde{\boldsymbol{\theta}}$ satisfies*

$$d\widetilde{\boldsymbol{\theta}} = \frac{1}{2}[\widetilde{\boldsymbol{\theta}}, \widetilde{\boldsymbol{\theta}}] + [\widetilde{\boldsymbol{\theta}}, \boldsymbol{\omega}].$$

(here the Lie bracket may be thought of as the Lie bracket on the differential graded Lie algebra $L_n^{\mathrm{dR}}(Z) \otimes H^0(L_n \times Z, \Omega^\bullet)$). Equivalently, we have

$$d\widetilde{\theta}_k = \sum_{i,j} b_{ijk} \widetilde{\theta}_i \wedge (\frac{1}{2}\widetilde{\theta}_j + \omega_j),$$

where b_{ijk} are as in (18).

Proof We prove this in $\varprojlim L_n^{\mathrm{dR}}(Z) \otimes H^0(L_n \times Z, \Omega^\bullet)$. Then it is enough to prove

$$[\boldsymbol{t}, d\widetilde{\boldsymbol{\theta}}] = \frac{1}{2}[\boldsymbol{t}, [\widetilde{\boldsymbol{\theta}}, \widetilde{\boldsymbol{\theta}}]] + [\boldsymbol{t}, [\widetilde{\boldsymbol{\theta}}, \boldsymbol{\omega}]].$$

since $\mathrm{ad}_{\boldsymbol{t}}$ is injective on $\varprojlim L_n^{\mathrm{dR}}(Z) \otimes H^0(U_n \times Z, \Omega^\bullet)$. From Lemma 4.3 we derive

$$\begin{aligned} d(e^{\mathrm{ad}_t} \cdot d\boldsymbol{t}) &= d(e^{\boldsymbol{t}} \cdot d\boldsymbol{t} \cdot e^{-\boldsymbol{t}}) \\ &= \left[\frac{e^{\mathrm{ad}_t} - 1}{\mathrm{ad}_{\boldsymbol{t}}} d\boldsymbol{t}, e^{\mathrm{ad}_t} d\boldsymbol{t} \right]. \end{aligned}$$

Since the connection ∇ is flat we have $d\boldsymbol{\omega} = \frac{1}{2}[\boldsymbol{\omega}, \boldsymbol{\omega}]$. Hence

$$\begin{aligned}
[\boldsymbol{t}, d\widetilde{\boldsymbol{\theta}}] &= [\boldsymbol{t}, d\widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}] - [\boldsymbol{t}, d\boldsymbol{\omega}] \\
&= d[\boldsymbol{t}, \widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}] - [d\boldsymbol{t}, \widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}] - [\boldsymbol{t}, d\boldsymbol{\omega}] \\
&= [\widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}, e^{\mathrm{ad}_{\boldsymbol{t}}} d\boldsymbol{t}] - \widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}, d\boldsymbol{t}] - \frac{1}{2}[\boldsymbol{t}, [\boldsymbol{\omega}, \boldsymbol{\omega}]] \\
&= [\widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}, [\boldsymbol{t}, \widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}]] - \widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}, d\boldsymbol{t}] - \frac{1}{2}[\boldsymbol{t}, [\boldsymbol{\omega}, \boldsymbol{\omega}]] \\
&= \frac{1}{2}[\boldsymbol{t}, [\widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}, \widetilde{\boldsymbol{\theta}} + \boldsymbol{\omega}]] - \frac{1}{2}[\boldsymbol{t}, [\boldsymbol{\omega}, \boldsymbol{\omega}]].
\end{aligned}$$

□

Note that, since $\theta_1, \ldots, \theta_{r_{n-1}}$ are linearly independent, there is $r_{n-1} < i \leq r_n$ such that $a_i \neq 0$. We choose the a_i minimally in the sense that the size of the set $\{i \in \{r_{n-1}+1, \ldots, r_n\} : a_i \neq 0\}$ is minimal among all non-trivial relations (24) (where *non-trivial* simply means the a_i are not all zero).

By Lemma 4.6 we have

$$d\left(\sum a_i \theta_i\right) = \sum \theta_i \wedge \left(-da_i + \sum b_{ijk} a_k \left(\frac{1}{2}\theta_j + \omega_j\right)\right) = 0. \tag{25}$$

Suppose that for $r_{n-1} < i \leq r_n$, the a_i are not all constant. Pick j_0 between r_{n-1} and r_n such that a_{j_0} is non-zero. Rescaling if necessary, we may assume $a_{j_0} = 1$. We claim that, after this rescaling, the a_i are all constant for $i > r_{n-1}$. Suppose a_{j_1} is non-constant. Since, by assumption, da_{j_1} is not in the span of the θ_i, there is a derivation

$$D : \Omega_{\overline{\mathbb{Q}}_p(V)|\overline{\mathbb{Q}}_p} \to \overline{\mathbb{Q}}_p(V)$$

such that $D(\theta_i) = 0$ for all i, and $D(da_{j_1}) \neq 0$. Write $c_i := D(-da_i + \sum b_{ijk} a_k (\frac{1}{2}\theta_j + \omega_j))$. Then

$$D\left(d\left(\sum_{i=1}^{r_n} a_i \theta_i\right)\right) = \sum_{i=1}^{r_{n-1}} c_i \theta_i = 0 \tag{26}$$

Since $b_{ijk} = 0$ whenever i or j are greater than r_{k-1}, we have, for all $i > r_{n-1}$,

$$c_i = D(-da_i).$$

In particular $c_{j_1} \neq 0$ and $c_{j_0} = 0$. Then (26) is a non-trivial relation with a smaller number of non-zero terms between r_{n-1} and r_n, contradicting our assumption of minimality of (24).

Hence we may assume that for $r_{n-1} < i \leq r_n$, the a_i are in $\overline{\mathbb{Q}}_p$. Define

$$\alpha_i = da_i - \sum b_{ijk} a_k \omega_j.$$

Then (25) can be rewritten

$$\sum_{i=1}^{r_{n-1}} \theta_i \wedge \alpha_i = \frac{1}{2} \sum_k a_k \sum_{i,j \leq r_{n-1}} b_{ijk} \theta_i \wedge \theta_j.$$

Hence, by our assumption that $\theta_1, \ldots, \theta_{r_{n-1}}$ are $\overline{\mathbb{Q}}_p(V)$-linearly independent, each α_i is in the $\overline{\mathbb{Q}}_p(V)$-span of $\theta_1, \ldots, \theta_{r_{n-1}}$, and in fact can be written as

$$\alpha_i = \sum \lambda_{ij} \theta_j \tag{27}$$

where

$$\lambda_{ij} - \lambda_{ji} = \sum_k b_{ijk} a_k. \tag{28}$$

A solution to (27) has the following interpretation. We can define a connection on $L_n^{\mathrm{dR}}(Z) \otimes \mathcal{O}_Z$ by $x \mapsto [\boldsymbol{\omega}, x]$, or with respect to our chosen basis by

$$e_{l_j} \mapsto \sum b_{ijk} \omega_{l_i} e_{l_k}.$$

Let $\mathcal{L}_n^{\mathrm{dR}}(Z)$ denote the unipotent flat connection corresponding, by Tannaka duality, to $L_n^{\mathrm{dR}}(Z)$ with the adjoint action of $\pi_1^{\mathrm{dR}}(Z, b)$. By Lemmas 3.9 and 4.2, we have $\mathcal{L}_n^{\mathrm{dR}}(Z) \simeq L_n^{\mathrm{dR}}(Z) \otimes \mathcal{O}_Z$ with connection given by

$$v \otimes 1 \mapsto [\boldsymbol{\omega}, v].$$

The dual connection $\nabla_{L_n^{\mathrm{dR}*}}$ on $\mathcal{L}_n^{\mathrm{dR}}(Z)^*$ is given by

$$e_{l_j}^* \mapsto \sum -b_{ikj} \omega_i e_{l_k}^*.$$

Hence the α_i can also be interpreted as the coefficients, with respect to the basis $e_{l_i}^*$, of $\nabla_{L_n^{\mathrm{dR}*}}(\boldsymbol{a})$, where $\boldsymbol{a} = \sum a_i e_{l_i}^*$. As the following lemma explains, the condition that $\alpha_i \in M_{n-1}$ for all i is equivalent to the existence of a morphism $\mathcal{E}_{n-1} \to \mathcal{L}_n^{\mathrm{dR}}(Z)^*$. Let $\pi : V \to Z$ denote the projection.

Lemma 4.7 (1) *M_n is equal to the submodule spanned by the coefficients of $\pi^* \nabla_n(\exp(\boldsymbol{t}))$ with respect to the basis e_i, where $\pi^* \nabla_n$ denotes the connection $\mathcal{E}_n^{\mathrm{dR}}(Z)$ pulled back to V.*

(2) *Suppose* $\{0\} = \{h_1 dh_2 : h_1, h_2 \in \overline{\mathbb{Q}}_p(V)\} \cap M_{n-1}$, *and* $\mathrm{rk}\, M_{n-1} = r_{n-1}$. *Let* $\mathcal{V} = (\mathcal{O}_Z^{\oplus N}, \nabla_{\mathcal{V}})$ *be an* $(n-1)$*-unipotent flat connection on* Z *in reduced form. Let* $x \in V(\overline{\mathbb{Q}}_p)$, *and let* $\mathcal{O}_{V,x}$ *denote the local ring of* V *at* x. *Then, for each* $\overline{v} \in x^*\pi^*\mathcal{V}$, *a lift of* $\overline{v}$ *to* $v \in \pi^*\mathcal{V}(\mathcal{O}_{V,x})$ *such that* $\nabla_{\pi^*\mathcal{V}}(v)$ *lies in the subspace* $\mathcal{O}_V^{\oplus N} \otimes M_{n-1}$ *is unique if it exists.*

(3) *Given any morphism of flat connections*

$$P : \mathcal{E}_{n-1} \to \mathcal{V}$$

on Z, *we have a solution to*

$$\nabla_{\pi^*\mathcal{V}}(v) \in \approx^*\mathcal{V} \otimes M_{n-1} \tag{29}$$

given by $v = P\exp(\boldsymbol{t})$. *In particular, by the universal property of* $\mathcal{E}_m$, *for all* $m > 0$, *and any* $\overline{v}$ *in* $b^*\mathcal{V}$, *there exists a unique lift of* $\overline{v}$ *to* $v \in \pi^*\mathcal{V}(V)$ *satisfying* $\nabla_{\pi^*\mathcal{V}}(v) \in M_m$.

Proof (1) As in the proof of Lemma 4.6, this follows from Lemma 4.3, which gives

$$\begin{aligned}\nabla_n(\exp(\boldsymbol{t})) &= d\exp(\boldsymbol{t}) - \boldsymbol{\omega} \cdot \exp(\boldsymbol{t}) \\ &= \boldsymbol{\theta} \cdot \exp(\boldsymbol{t}).\end{aligned}$$

(2) We prove this by induction on the minimal degree of unipotence of $\mathcal{V}$. For 0-unipotent connections, $\nabla(\sum a_i \otimes e_i) = da_i \otimes e_i$, so the result is immediate. Given the result for k-unipotent connections, let $\mathcal{V}$ be $(k+1)$-unipotent, and let

$$0 \to \mathcal{V}' \to \mathcal{V} \xrightarrow{\tau} \mathcal{V}'' \to 0$$

be a short exact sequence where $\mathcal{V}'$ is 0-unipotent and $\mathcal{V}''$ is k-unipotent. Let v and w be two lifts of $\overline{v}$ to sections in $\pi^*\mathcal{V}(\mathcal{O}_{V,x})$ such that $\nabla_{\pi^*\mathcal{V}}(v)$ and $\nabla_{\pi^*\mathcal{V}}(w)$ are in $\pi^*\mathcal{V} \otimes M_{n-1}$. Then $\tau(v)$ and $\tau(w)$ are equal at x, and satisfy $\nabla_{\pi^*\mathcal{V}''}(\tau(v)), \nabla_{\pi^*\mathcal{V}''}(\tau(w)) \in \pi^*\mathcal{V}'' \otimes M_{n-1}$. Since $\mathcal{V}''$ is k-unipotent, we have $\tau(v) = \tau(w)$, hence $v - w$ is a section of the trivial connection $\mathcal{V}'$ satisfying $\nabla_{\pi^*\mathcal{V}'}(v - w) \in \pi^*\mathcal{V}' \otimes M_{n-1}$, hence is zero.

(3) By Lemma 4.1, the morphism is K-linear, since both connections are in reduced form. Hence it satisfies

$$P\nabla_{n-1} = \nabla_{\mathcal{V}} P,$$

hence $P\exp(\boldsymbol{t})$ satisfies (29).

□

Now suppose we have a solution to

$$\alpha_i = \sum \lambda_{ij}\theta_j \tag{30}$$

with λ_{ij} in $\overline{\mathbb{Q}}_p(V)$. Let x be a point at which none of the λ_{ij} have a pole, then by Lemma 29, a solution to (30) with $\lambda_{ij} \in \mathcal{O}(Z)_x$ is unique given their value at x, and for every choice of (c_{ij}) with c_{ij} in $\overline{\mathbb{Q}}_p$, there is a unique lift to $\lambda_{ij} \in \mathcal{O}(Z)_x$ satisfying $\lambda_{ij}(x) = c_{ij}$, and coming from a morphism of flat connections $\mathcal{E}_{n-1} \to \mathcal{L}_n$. In particular the λ_{ij} are actually in $\mathcal{O}(Z)$. We claim that for all $i \in \{r_{n-2}+1, \dots, r_{n-1}\}$, $j \in \{1, \dots, r_1\}$, if (28) holds then, for all $i \geq r_{n-2}+1$, $\lambda_{ji} = 0$.

For $i \in \{r_{n-2}+1, \dots r_{n-1}\}$, we have

$$\alpha_i = da_i - \sum_{k=r_{n-1}+1}^{r_n} b_{ijk} a_k \omega_j.$$

since $b_{ijk} = 0$ if $i > r_{n-2}$ and $k \leq r_{n-1}$. Since a_k is constant for $k > r_{n-1}$, we deduce

$$a_i = \sum b_{ijk} a_k t_j$$

is a solution, hence for i in $\{r_{n-1}+1, \dots, r_n\}$, we have

$$\lambda_{ij} = \sum_{k=r_{n-1}+1}^{r_n} b_{ijk} a_k.$$

This completes the proof of the claim.

This means that the map

$$\mathcal{E}_{n-1} \to \mathcal{L}_n^*$$

factors through $\mathcal{E}_{n-2}$, or equivalently that the action of $b^*\mathcal{E}_{n-1}$ on $\sum a_k e_{l_k}^*$ factors through $b^*\mathcal{E}_{n-2}$. Since we assume a_k is non-zero for some $k \in \{r_{n-1}+1, \dots, r_n\}$, the $b^*\mathcal{E}_{n-1}$-module generated by $\sum a_k e_{l_k}^*$ is not $(n-2)$-unipotent. Hence we obtain a contradiction, completing the proof of Proposition 4.1.

5 The intersection of $j_n(Z)$ with the Selmer variety

In this section we prove certain techniques for proving finiteness of $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ and $\mathcal{X}(\mathcal{O}_{K_v})_{S,n}$. First, we prove a general result which allows to prove finiteness after passing to a finite extension. The only wrinkle this introduces is that, as we have chosen to work with a prime which splits completely in K, passing to a finite extension will compel us to work with a prime splitting completely in the extension field.

Lemma 5.1 *Let $L|K$ be a finite extension of $\mathbb{Q}$, and X a curve over K as in the introduction. Let p be a rational prime which splits completely in L.*

(1) *If $\mathcal{X}(\mathcal{O}_L \otimes \mathbb{Z}_p)_{S,n}$ is finite, then $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n}$ is finite.*
(2) *Let w be a prime of K lying above p, and v a prime of L lying above w. If $\mathcal{X}(\mathcal{O}_v)_{S,n}$ is finite, then $\mathcal{X}(\mathcal{O}_w)_{S,n}$ is finite.*

Proof We have diagonal embeddings of $\mathrm{Res}_{K|\mathbb{Q}}(X)$ into $\mathrm{Res}_{L|\mathbb{Q}}(X_L)$ which, upon base change to $\mathbb{Q}_p$, induce embeddings of X_{K_w} into $\prod_{v'|w} X_{L_{v'}}$, where the product is over primes of L lying above w. On the other hand, we also have inclusions of $H^1_{f,S}(G_{K,S}, U_n(X))$ into $H^1_{f,S}(G_{L,S}, U_n(X))$. We obtain a commutative diagram

$$\begin{array}{ccc} \mathrm{Res}_{K|\mathbb{Q}}(X)(\mathbb{Q}) & \longrightarrow & H^1_{f,S}(G_{\mathbb{Q},S}, \mathrm{Ind}_K^{\mathbb{Q}} U_n(X)) \\ \downarrow & & \downarrow \\ \mathrm{Res}_{L|\mathbb{Q}}(X_L)(\mathbb{Q}) & \longrightarrow & H^1_{f,S}(G_{\mathbb{Q},S}, \mathrm{Ind}_L^{\mathbb{Q}} U_n(X)), \end{array}$$

and similarly for local fields, giving inclusions

$$\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_{S,n} \hookrightarrow \mathcal{X}(\mathcal{O}_L \otimes \mathbb{Z}_p)_{S,n}$$

and

$$\mathcal{X}(\mathcal{O}_{K_w})_{S,n} \hookrightarrow \mathcal{X}(\mathcal{O}_{L_v})_{S,n}$$

□

Lemma 5.2 *Let U be a Galois-stable finite-dimensional quotient of the $\mathbb{Q}_p$-unipotent fundamental group of X. Suppose* $\mathrm{Hom}(J_{\sigma_1,\mathbb{C}}, J_{\sigma_2,\mathbb{C}}) = 0$ *for all distinct embeddings $\sigma_i : K \hookrightarrow \mathbb{C}$. Then, if*

$$\sum_{i=1}^{n} \mathrm{h}^1_f(G_K, \mathrm{gr}_i(U)) \leq [K : \mathbb{Q}] + \sum_{i=1}^{n} \sum_{v|p} \dim D_{\mathrm{dR}}(U)/F^0,$$

then there is a prime $v|p$ of K such that $X(K_v)_U$ is finite.

Proof By Proposition 3.2, $\dim \mathrm{Sel}(U)$ is bounded above by $\dim H^1_f(G_K, \mathrm{Lie}(U^c))$ for all twists of U by cocycles $c \in \mathrm{Sel}(U)$. Since $\mathrm{gr}_i(U) \simeq \mathrm{gr}_i(U^c)$, for each such c, we have

$$\mathrm{h}^1_f(G_K, \mathrm{Lie}(U^c)) \leq \sum_{i=1}^{n} \mathrm{h}^1_f(G_K, \mathrm{gr}_i(U))$$

On the other hand

$$\sum_{v|p} \dim U^{\mathrm{dR}}(X_v)/F^0 = \dim \sum_{i=1}^{n} \sum_{v|p} \dim D_{\mathrm{dR}}(\mathrm{gr}_i(U))/F^0.$$

Hence, if the inequality in the statement of the Lemma holds, then by Proposition 4.2 the Zariski closure of $X(K \otimes \mathbb{Q}_p)_U$ is a proper subvariety, all of whose positive

dimensional irreducible components Z satisfy

$$\operatorname{codim}_{U^{\mathrm{dR}}(Z/\operatorname{Res}(X))/F^0}(\operatorname{loc}_p(\operatorname{Sel}(U)) \cap U^{\mathrm{dR}}(X/\operatorname{Res}(X))/F^0) < \dim Z. \quad (31)$$

Since there are no nonzero homomorphisms between the different factors of $\operatorname{Res}(J)_{\mathbb{Q}_p}$, the image of $\operatorname{Alb}(Z)$ in $\operatorname{Res}(J)_{\mathbb{Q}_p}$ is the product of the images in the different factors. Hence if Z dominates each factor of $\operatorname{Res}(X)_{\mathbb{Q}_p}$, then its geometric unipotent fundamental group surjects onto the geometric unipotent fundamental group of $\operatorname{Res}(X)_{\mathbb{Q}_p}$, contradicting (31). □

This straightforwardly implies case (2) of Proposition 1.1.

Proof of 1.1, case (2) Let U be, as in [5, Proposition 2.2], the quotient of U_2 which is an extension of V_pJ by $\operatorname{Ker}(\operatorname{NS}(J_{\overline{K}}) \to \operatorname{NS}(X_{\overline{K}})) \otimes \mathbb{Q}_p(1)$. By [5, Lemma 2.3], we have

$$h^1_f(G_{K,S}, \operatorname{gr}_2 U) = \sum_{v \in P_{\mathbb{R}}} (\dim \operatorname{NS}(J_{\overline{K}})^{c_v=1} - \dim \operatorname{NS}(J)).$$

Hence case (2) of Proposition 1.1 follows from Lemma 5.2. □

5.1 Semi-simplicity properties of graded pieces of fundamental groups

Let $n > 0$, and let X be a smooth projective curve of genus $g > 1$ over K with $n-1$ marked points $x_i \in X(K)$. Let $Y = X - \{x_1, \ldots, x_{n-1}\}$. Let $\mathcal{M}_{g,n,K}$ denote the moduli stack of n-pointed curves of genus g over K. For $x_n \in Y(K)$, we have a short exact sequence

$$1 \to \pi_1(Y_{\overline{K}}, x) \to \pi_1(\mathcal{M}_{g,n,K}, [(X, (x_i)_{i=1}^n)]) \to \pi_1(\mathcal{M}_{g,n-1,K}, [(X, (x_i)_{i=1}^{n-1})]) \to 1,$$

(see e.g. Nakamura–Tsunogai [44]). This induces an outer action of $\pi_1(\mathcal{M}_{g,n-1,K}, [(X, (x_i))])$ on $\pi_1^{\text{ét}}(Y_{\overline{K}}, x_n)$, which induces an outer action on the Malcev completion of $\pi_1^{\text{ét}}(Y_{\overline{K}}, x_n)$, and hence an action on the graded pieces $\operatorname{gr}_i(U_i(Y)(x)$. When $n = 1$ or 2, the action of $\pi_1(\mathcal{M}_{g,n-1,K}, [(X, (x_i))])$ on $U_1(Y) = H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ has Zariski dense image in $\operatorname{GSp}(U_1(X))$ (see e.g. [29, §8]). The action of G_K on $\operatorname{gr}_i(U_i(Y))$ factors through the action of $\pi_1(\mathcal{M}_{g,0,K}, [X])$ via the morphism

$$\operatorname{Gal}(\overline{K}|K) \to \pi_1(\mathcal{M}_{g,n-1,K}, [(X, (x_i))]) \quad (32)$$

induced by the morphism $\operatorname{Spec}(K) \to \mathcal{M}_{g,n-1,K}$ induced by $[(X, (x_i))]$.

Lemma 5.3 *Let X/K be either projective or a projective curve minus a point.*

(1) *The commutator homomorphism*

$$U_1(X)^{\otimes i} \to \operatorname{gr}_i(U_i(X))$$

admits a G_K-equivariant section.

(2) *Let $U_i = U_i(\mathrm{Res}(X))$, and let $W \subset V = U_1$ denote the image of the $\mathbb{Q}_p$-Tate module of an abelian subvariety of $\mathrm{Res}(J)_L$, for some $L|\mathbb{Q}$. Then the image of $W^{\otimes i}$ in $\mathrm{gr}_i(U_i)$ is a $G_{L,T}$-stable direct summand of $\mathrm{gr}_i(U_i)$.*

Proof Let $n = 1$ or 2 depending on whether X is projective or projective minus a point $x \in \overline{X}(K)$, and let $S = \emptyset$ or $\{x\}$. By the homomorphism (32), to prove the first claim it is enough to prove them with G_K replaced by $\pi_1(\mathcal{M}_{g,n-1,K}, [(\overline{X}, S)])$. Since $\pi_1(\mathcal{M}_{g,n-1,K}, [(\overline{X}, S)])$ has Zariski dense image in $\mathrm{GSp}(U_1(X))$, it is enough to prove them with $\pi_1(\mathcal{M}_{g,n-1,K}, [(\overline{X}, S)])$ replaced by $\mathrm{GSp}(U_1(X))$, which proves the Lemma. The second claim follows from part (1), together with the fact that the image of $W^{\otimes i}$ in $V^{\otimes i}$ is a direct summand, since $W \subset V$ is a direct summand. □

5.2 Further reductions

Given Proposition 4.2, to prove finiteness of $\mathcal{X}(\mathcal{O}_K \otimes \mathbb{Z}_p)_n$, it is enough to prove that, for any positive-dimensional, geometrically irreducible smooth quasi-projective subvariety $Z \subset \mathrm{Res}(X)_{\mathbb{Q}_p}$, and any virtual basepoint $b \in Z(\mathbb{Q}_p) \cap \mathrm{Res}(X)(\mathbb{Q}_p)$, there is a Galois-stable quotient U of $U_n(\mathrm{Res}(X))$, such that

$$\mathrm{codim}_{U(Z/\mathrm{Res}(X))/F^0}(\mathrm{loc}_p(\mathrm{Sel}(U)_\alpha) \cap U(Z/\mathrm{Res}(X))/F^0) > \dim(Z). \quad (33)$$

First, we reduce proving (33) to proving an inequality involving abelian Galois cohomology. Recall from Lemma 3.7 that, by changing b to a 'virtual basepoint' we may assume α is the trivial collection of local conditions, and hence $\mathrm{Sel}(U)_\alpha \subset H^1_{f,S}(G_{\mathbb{Q},T}, U)$. Recall that, by Proposition 3.2, we have

$$\begin{aligned}&\dim H^1_{f,S}(G_{\mathbb{Q},T}, U) \cap U^{\mathrm{dR}}(Z/\mathrm{Res}(X))/F^0 \\ &\quad \leq \max_{c \in H^1_{f,S}(G_{\mathbb{Q},T}, U)} \dim \mathrm{loc}_p H^1_{f,S}(G_{\mathbb{Q},T}, L^c) \cap L^{\mathrm{dR}}(Z/\mathrm{Res}(X))^c/F^0,\end{aligned}$$

where $L^{\mathrm{dR}}(Z/\mathrm{Res}(X))^c/F^0$ is defined to be 0 if c is not in $U^{\mathrm{dR}}(Z/\mathrm{Res}(X))/F^0$. Hence we can estimate the dimension of $H^1_{f,S}(G_{\mathbb{Q},T}, U) \cap U^{\mathrm{dR}}(Z/\mathrm{Res}(X))/F^0$ using the following Lemma.

Lemma 5.4 *Let U be a Galois stable quotient of U_N, with Lie algebra L, and $c \in H^1_{f,S}(G_{\mathbb{Q},T}, U_n)$. Let $Z \subset \mathrm{Res}(X)_{\mathbb{Q}_p}$ be an irreducible subvariety, and let $L^{\mathrm{dR}}(Z/\mathrm{Res}(X))$ denote the image of $\varprojlim L_i^{\mathrm{dR}}(Z)$ in $D_{\mathrm{dR}}(L)$. We have*

$$\begin{aligned}&\mathrm{codim}_{L^{\mathrm{dR}}(Z/\mathrm{Res}(X))^c/F^0} \mathrm{loc}_p H^1_{f,S}(G_{\mathbb{Q},T}, L^c) \cap L^{\mathrm{dR}}(Z/\mathrm{Res}(X))^c/F^0) \\ &\geq \sum_{i=1}^{N} \mathrm{codim}_{\mathrm{gr}_i(L^{\mathrm{dR}}(Z/\mathrm{Res}(X)))/F^0} H^1_{f,S}(G_{\mathbb{Q},T}, \mathrm{gr}_i(L)) \cap (\mathrm{gr}_i(L^{\mathrm{dR}}(Z/\mathrm{Res}(X)))/F^0) \\ &\quad - \sum_{i=1}^{N-1} \dim \mathrm{Ker}(H^1_{f,S}(G_{\mathbb{Q},T}, \mathrm{gr}_i(L)) \to H^1_f(G_{\mathbb{Q}_p}, \mathrm{gr}_i(L))).\end{aligned}$$

Proof We have

$$\dim L^{\mathrm{dR}}(Z/\operatorname{Res}(X))^c/F^0 = \sum_{i=1}^{N} \dim \operatorname{gr}_i(L^{\mathrm{dR}}(Z/\operatorname{Res}(X)))/F^0.$$

Hence it is enough to prove that

$$\begin{aligned}&\dim \operatorname{loc}_p(H^1_{f,S}(G_{\mathbb{Q},T}, L^c)) \cap L^{\mathrm{dR}}(Z/\operatorname{Res}(X))^c/F^0\\ &\leq \sum_{i=1}^{N} \dim \operatorname{loc}_p H^1_{f,S}(G_{\mathbb{Q},T}, \operatorname{gr}_i(L)) \cap (\operatorname{gr}_i(L^{\mathrm{dR}}(Z/\operatorname{Res}(X)))/F^0)\\ &\quad + \sum_{i=1}^{N-1} \dim \operatorname{Ker}(H^1_{f,S}(G_{\mathbb{Q},T}, \operatorname{gr}_i(L)) \to H^1_f(G_{\mathbb{Q}_p}, \operatorname{gr}_i(L))).\end{aligned}$$

Note that U_n acts unipotent on L, hence we may replace $\operatorname{gr}_i(L)$ with $\operatorname{gr}_i(L^c)$ in the above.

This is then just linear algebra: more generally suppose $A = A_\bullet$, $B = B_\bullet$ are finite dimensional vector space with separated exhaustive decreasing filtrations, such that A is a strict filtered subspace of B, and $C_{i,j}$ $(i < j)$ are finite dimensional vector spaces such that, for all $i < j < k$, we have a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & C_{j,k} & \longrightarrow & C_{i,k} & \longrightarrow & C_{i,j} \\ & & \downarrow{\scriptstyle \phi_{j,k}} & & \downarrow{\scriptstyle \phi_{i,k}} & & \downarrow{\scriptstyle \phi_{j,k}} \\ 0 & \longrightarrow & B_j/B_k & \longrightarrow & B_i/B_k & \longrightarrow & B_i/B_j \longrightarrow 0. \end{array}$$

Then

$$\begin{aligned}&\dim \operatorname{Ker}(\phi_{i,j}(C_{i,j}) \cap (A_i/A_j) \to \phi_{i,i+1}(C_{i,i+1}) \cap (A_i/A_{i+1}))\\ &\leq \dim \operatorname{Ker}(\phi_{i,i+1}) + \dim \phi_{i+1,j}(C_{i+1,j}) \cap (A_{i+1}/A_j).\end{aligned}$$

Hence, for all $i < j$,

$$\begin{aligned}\dim \phi_{i,j}(C_{i,j}) \cap (A_i/A_j) \leq &\sum_{i \leq k < j} \dim \phi_{k,k+1}(C_{k,k+1}) \cap (A_k/A_{k+1})\\ &+ \sum_{i<k<j} \dim \operatorname{Ker}(\phi_{k-1,k}).\end{aligned}$$

Applying this when $B_i = C_i L^{\mathrm{dR}}$, $A_i = C_i L^{\mathrm{dR}}(Z/\operatorname{Res}(X))$ and $C_{i,j} = H^1_{f,S}(G_{\mathbb{Q},T}, C_i L/C_j L)$ completes the proof of Lemma. □

One subtlety in estimating the dimension of the intersection of $\mathrm{gr}_i U^{\mathrm{dR}}(Z/\mathrm{Res}(X))/F^0$ with $\mathrm{loc}_p\, H^1_{f,S}(G_{\mathbb{Q},T}, \mathrm{gr}_i(U))_{\overline{\mathbb{Q}}_p}$ is that we do not assume that Z is defined over $\mathbb{Q}$, or even over a number field. However in spite of this, $\mathrm{gr}_i U^{\mathrm{dR}}(Z/\mathrm{Res}(X))/F^0$ behaves as if it was defined over a number field, in the following sense.

Lemma 5.5 *Let $A = \mathrm{Alb}(\mathrm{Res}(X))$, where X is either a projective curve or a projective curve minus a point. Let $f : Z \hookrightarrow \mathrm{Res}(X)_{\overline{\mathbb{Q}}_p}$ be a geometrically irreducible subvariety of $\mathrm{Res}(X)_{\overline{\mathbb{Q}}_p}$. There exists a finite extension $L|\mathbb{Q}$ such that $f_* H^{\text{ét}}_1(\mathrm{Alb}(Z)_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p) \subset H^{\text{ét}}_1(A_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ is stable under the action of $\mathrm{Gal}(L|\mathbb{Q})$.*

Proof First, note that since X is projective, or projective minus a point, its Albanese variety is abelian. Hence it is enough to show that, for any injective morphism of abelian varieties $g : B \to A_{\overline{\mathbb{Q}}_p}$, defined over $\overline{\mathbb{Q}}_p$, there is a finite extension $L|\mathbb{Q}$ such that $g_* H^{\text{ét}}_1(B, \mathbb{Q}_p)$ is G_L-stable. There is an endomorphism $\phi \in \mathrm{End}(A_{\overline{\mathbb{Q}}_p})$ such that

$$g_* H^{\text{ét}}_1(B, \mathbb{Q}_p) = \phi_*(H^{\text{ét}}_1(\mathrm{Alb}(\mathrm{Res}(X))_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)).$$

Indeed, we may take the endomorphism to be the composite

$$A_{\overline{\mathbb{Q}}_p} \to A^*_{\overline{\mathbb{Q}}_p} \to B^* \to B \to A_{\overline{\mathbb{Q}}_p},$$

for some choice of polarisation on B (since the map $A^*_{\overline{\mathbb{Q}}_p} \to B^*$ is surjective, the image of $H^{\text{ét}}_1(A_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ under this endomorphism is exactly $g_* H^{\text{ét}}_1(B, \mathbb{Q}_p)$). Hence it is enough to show that there exists a finite extension $L|\mathbb{Q}$ such that $\mathrm{End}(A_L) \simeq \mathrm{End}(A_{\overline{\mathbb{Q}}_p})$, which follows from the classification of endomorphisms of abelian varieties [43, Corollary IV.1]. □

Lemma 5.6 *Let $K|\mathbb{Q}$ be a finite extension, and $n > 1$. Let W be a subspace of $V := \mathrm{Ind}_K^{\mathbb{Q}} \mathbb{Q}_p(n)$, stable under $G_{\mathbb{Q}_p}$. Then*

$$\dim \mathrm{loc}_p\, H^1(G_{\mathbb{Q},T}, V) \cap H^1(G_{\mathbb{Q}_p}, W) \leq \dim W^{c=-1},$$

where $c \in G_{\mathbb{Q}}$ is complex conjugation with respect to an inclusion $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

Proof Let $L|\mathbb{Q}$ denote a totally imaginary Galois extension containing $K|\mathbb{Q}$, with Galois group G, and $H := \mathrm{Gal}(L|K)$. Let $M := \mathrm{Ind}_L^{\mathbb{Q}} \mathbb{Q}_p(n)$. We have an isomorphism $M \simeq \mathbb{Q}_p[G](n)$, and an inclusion

$$V \hookrightarrow W.$$

Hence it is enough to prove that for any $W \subset \mathbb{Q}_p[G]$, we have

$$\dim \mathrm{loc}_p\, H^1(G_{\mathbb{Q},T}, M) \cap H^1(G_{\mathbb{Q}_p}, W(n)) \leq \dim W^{c=(-1)^{n+1}}.$$

By Shapiro's lemma, we have a commutative diagram whose vertical arrows are isomorphisms

$$\begin{array}{ccc} H^1(G_{\mathbb{Q},T}, M) & \longrightarrow & H^1(G_{\mathbb{Q}_p}, M) \\ \downarrow & & \downarrow \\ H^1(G_{L,T}, \mathbb{Q}_p(n)) & \longrightarrow & \oplus_{w|p} H^1(G_{L_w}, \mathbb{Q}_p(n)) \end{array}$$

hence it is enough to prove the claim for the dimension of the image of the bottom horizontal map. Both $H^1(G_{L,T}, \mathbb{Q}_p(n))$ and $\oplus_{w|p} H^1(G_{L_w}, \mathbb{Q}_p(n))$ have the structure of $\mathrm{Gal}(L|\mathbb{Q})$-modules, with respect to which the localisation map is $\mathrm{Gal}(L|\mathbb{Q})$-equivariant.

We claim that we have an isomorphism of Galois modules

$$H^1(G_{L,T}, \mathbb{Q}_p(n)) \simeq \mathrm{Ind}_{\langle \overline{c} \rangle}^{\mathrm{Gal}(L|\mathbb{Q})} \chi^{n+1}, \tag{34}$$

where χ is the unique nontrivial character of $\langle \overline{c} \rangle$, and $\overline{c}$ now denotes the image of c in $\mathrm{Gal}(L|\mathbb{Q})$, and an isomorphism

$$H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p[G](n)) \simeq \mathbb{Q}_p[G]. \tag{35}$$

induced by $H^1(G_{\mathbb{Q}_p}, \mathbb{Q}_p(n)) \simeq \mathbb{Q}_p$.

For the first claim, note that Borel's theorem [9] proves a $\mathrm{Gal}(L|\mathbb{Q})$-equivariant isomorphism $K_{2n+1}(L) \otimes \mathbb{R} \simeq \mathrm{Ind}_{\langle \overline{c} \rangle}^{\mathrm{Gal}(L|\mathbb{Q})} \chi^{n+1} \otimes \mathbb{R}$. This implies a Galois-equivariant isomorphism $K_{2n+1}(L) \otimes \mathbb{Q} \simeq \mathrm{Ind}_{\langle \overline{c} \rangle}^{\mathrm{Gal}(L|\mathbb{Q})} \chi^{n+1}$. Hence, by Soulé's theorem [51], we obtain the isomorphism (34).

For the isomorphism (35), we may use the fact that the Bloch–Kato logarithm is Galois-equivariant by construction, and hence we have $\mathrm{Gal}(L_w|\mathbb{Q}_p)$-equivariant isomorphisms

$$H^1(G_{L_w}, \mathbb{Q}_p(n)) \simeq H^1_f(G_{L_f}, \mathbb{Q}_p(n)) \simeq L_f.$$

Having proved these isomorphisms, we deduce that the image of $H^1(G_{\mathbb{Q},T}, V)$ in $H^1(G_{\mathbb{Q}_p}, V)$ must be contained in $\mathrm{Ker}(1 + (-1)^n c)$. This implies the Lemma. □

5.3 Metabelian quotients of fundamental groups

We say a group G is *metabelian* if $[[G, G], [G, G]]$ is zero, and similarly a Lie algebra L is metabelian if $[[L, L], [L, L]] = 0$. The free metabelian Lie algebra on a vector space W is simply the quotient of the free pro-nilpotent Lie algebra L on W by the double commutator $[[L, L], [L, L]]$. Given a vector space W, we denote by $\widehat{\mathrm{Sym}}^{\bullet}(W)$ the completion of the symmetric algebra on W with respect to the ideal generated by W. If L is a metabelian Lie algebra, the adjoint action of L on $[L, L]$ factors through L^{ab}, and gives $[L, L]$ the structure of a module over $\widehat{\mathrm{Sym}}^{\bullet}(L^{\mathrm{ab}})$.

In the proof of cases (3) and (4) of Theorem 1.1, we will use metabelian quotients of the unipotent fundamental group. This follows the proof of these results over $\mathbb{Q}$ [13, 37]. To extend the arguments of loc. cit. to the number field situation, we will need the following properties of metabelian Lie algebras.

Lemma 5.7 *Let L^{ma} be the free metabelian $\mathbb{Q}_p$-Lie algebra on generators $x_1, \dots, x_n$.*

(1) *Let M denote the $\mathbb{Q}_p[x_1, \dots, x_n]$ module*

$$M = \{(v_1, \dots, v_n) \in \mathrm{Sym}^\bullet(L^{\mathrm{ma,ab}})^{\oplus n} : \sum v_i x_i = 0\}.$$

Then we have an isomorphism of $\mathbb{Q}_p[\![x_1, \dots, x_n]\!]$ modules

$$\widehat{M} \simeq [L^{\mathrm{ma}}, L^{\mathrm{ma}}].$$

via the identification $\widehat{\mathrm{Sym}}^\bullet(L^{\mathrm{ma,ab}}) \simeq \mathbb{Q}_p[\![x_1, \dots, x_n]\!]$.

(2) *Let $\overline{L}^{\mathrm{ma}}$ be the maximal metabelian quotient on the Lie algebra of the $\mathbb{Q}_p$-unipotent fundamental group of a smooth projective irreducible curve X over an algebraically closed field F of characteristic zero. Let $x_1, \dots x_{2g}$ be a symplectic basis of $H := H^{\text{ét}}_1(X, \mathbb{Q}_p)$. Define*

$$M = \{(v_1, \dots, v_n) \in \mathrm{Sym}^\bullet(H)^{\oplus n} : \sum v_i x_i = 0\},$$

and define $m := (v_{g+1}, \dots, v_{2g}, -v_1, \dots, -v_g) \in M$. Then we have an isomorphism of $\widehat{\mathrm{Sym}}^\bullet(H)$-modules.

$$[\overline{L}^{\mathrm{ma}}, \overline{L}^{\mathrm{ma}}] \simeq \widehat{M}/\widehat{\mathrm{Sym}}^\bullet(H) \cdot m.$$

Given an element x of $[L^{\mathrm{ma}}, L^{\mathrm{ma}}]$, we refer to the coefficients v_i of the corresponding element of $\widehat{M}$ as the *Fox differentials* of x (motivated by Ihara's construction, used in the proof of Lemma 5.7).

Proof (1) Let G be the free pro-p group on generators $\gamma_1, \dots, \gamma_n$. Let $\overline{G}$ be the maximal metabelian quotient

$$\overline{G} := G/[[G, G], [G, G]].$$

We claim that L^{ma} is isomorphic to the Lie algebra of the $\mathbb{Q}_p$-Malcev completion of $\overline{G}$. This follows from universal properties: L^{ma} is the Lie algebra of the metabelian quotient U of the free pro-unipotent $\mathbb{Q}_p$-group on generators x_i, which we will denote by $\widetilde{U}$. The category of continuous $\mathbb{Q}_p$-representations of $\overline{G}$ is equivalent to the category of metabelian representations of $\widetilde{U}$, which is equivalent to the category of representations of U.

Let G_i and U_i denote the maximal i-unipotent quotients of $\overline{G}$ and U respectively. We have an isomorphism of $\widehat{\mathrm{Sym}}^\bullet(V)$-modules

$$[\overline{G}, \overline{G}] \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq [U_i, U_i].$$

Hence it is enough to compute the action of the Lie algebra of $\overline{G}$ on $[G, G]$. Let $\mathcal{L}$ denote the $\mathbb{Z}_p$-Lie algebra of $\overline{G}$: this is the $\mathbb{Z}_p$-module $\varprojlim \oplus_{i\leq n} \mathrm{gr}_i(\overline{G})$, with Lie bracket induced by the commutator on $\overline{G}$. Then, by [45, 2.3.2], we have an isomorphism of $\mathbb{Q}_p$-Lie algebras

$$\mathcal{L}\widehat{\otimes}_{\mathbb{Z}_p}\mathbb{Q}_p \simeq L^{\mathrm{ma}}. \tag{36}$$

The conjugation action of G^{ab} on $[\overline{G}, \overline{G}]$ gives it the structure of a $\mathbb{Z}_p[\![G^{\mathrm{ab}}]\!]$-module. On the other hand, the Lie bracket on $[\mathcal{L}, \mathcal{L}]$ gives it the structure of a module over $\mathbb{Z}_p[\![G^{\mathrm{ab}}]\!]$. From the definitions, we obtain an isomorphism of $\mathbb{Z}_p[\![G^{\mathrm{ab}}]\!]$-modules

$$[\mathcal{L}, \mathcal{L}] \simeq \mathrm{gr}^\bullet[\overline{G}, \overline{G}]. \tag{37}$$

In particular, we obtain a non-canonical isomorphism of $\mathbb{Q}_p[\![x_1, \ldots, x_n]\!]$-modules

$$[L^{\mathrm{ma}}, L^{\mathrm{ma}}] \simeq [\overline{G}, \overline{G}]\widehat{\otimes}_{\mathbb{Z}_p[\![G^{\mathrm{ab}}]\!]}\mathbb{Q}_p[\![x_1, \ldots, x_n]\!]$$

where x_i acts on $[\overline{G}, \overline{G}]$ by $\gamma_i - 1$. Hence it will be enough to prove that we have an isomorphism of $\mathbb{Z}_p[\![x_1, \ldots, x_n]\!]$-modules

$$[\overline{G}, \overline{G}] \simeq \{(v_1, \ldots, v_n) \in \mathbb{Z}_p[\![G^{\mathrm{ab}}]\!] : \sum v_i x_i = 0\}.$$

This is a special case of a theorem of Ihara [32, Theorem 2.2].

(2) By [29], we know that $\mathrm{gr}^\bullet \overline{L}^{\mathrm{ma}}$ is isomorphic to a free pro-nilpotent $\mathbb{Q}_p$-Lie algebra on generators $x_1, \ldots, x_{2g}$, modulo the Lie ideal generated by $\sum_{i=1}^{g}[x_i, x_{g+i}]$. Hence part (2) follows from part (1).

□

6 Proof of Theorem 1.1

We first recall the following result, which is a corollary of Euler characteristic formulae/Poitou–Tate duality for finite Galois representations, and roughly says that for global Galois cohomology, showing that H^1 is small, showing that H^2 is small, and showing that H^1 of the Tate dual is small are equivalent problems.

Lemma 6.1 (1) [34, Lemma 2] *For any finite dimensional $\mathbb{Q}_p$-representation W of $G_{K,T}$, we have*

$$\begin{aligned}\mathrm{h}^1(G_{K,T}, W) &= \mathrm{h}^2(G_{K,T}, W) + \mathrm{h}^0(G_{K,T}, W) + \sum_{v\in P_{\mathbb{R}}} \dim W^{c_v=-1} \\ &\quad +(\#P_{\mathbb{C}})\cdot \dim W,\end{aligned}$$

where $P_{\mathbb{R}}$ and $P_{\mathbb{C}}$ denote the set of real and complex places of K respectively, and the decomposition group at $v \in P_{\mathbb{R}}$ is generated by c_v.

(2) [22, Remark 1.2.4] *If $K = \mathbb{Q}$, and $H^0(G_{\mathbb{Q},T}, W)$, $H^0(G_{\mathbb{Q},T}, W^*(1))$ and $D_{\mathrm{cris}}(W)^{\phi=1}$ are all zero, then*

$$\begin{aligned} &\mathrm{h}^1_f(G_{\mathbb{Q}_p}, W) - \mathrm{h}^1_f(G_{\mathbb{Q},T}, W) \\ &\quad = \mathrm{h}^0(G_{\mathbb{R}}, W) - \dim H^1_f(G_{\mathbb{Q},T}, W^*(1)). \end{aligned}$$

(3) [22, 1.2.2] *For any number field K and $\mathbb{Q}_p$-Galois representation W,*

$$\begin{aligned} &\dim(\mathrm{Ker}(H^1(G_{K,T}, W) \to \oplus_{v\in T} H^1(G_{K_v}, W))) \\ &\quad = \dim \mathrm{Ker}(H^2(G_{K,T}, W^*(1)) \to \oplus_{v\in T} H^2(G_{K_v}, W^*(1))). \end{aligned}$$

6.1 Theorem 1.1, case (1)

In this subsection we prove Theorem 1.1 in the case $X = \mathbb{P}^1_K - D$. First, we make use of the following Lemma to reduce to the case where S is empty.

Lemma 6.2 *For all $i > 1$, any Galois stable quotient W of $\mathrm{gr}_i(U)$, and any $v \neq p$, we have $H^1(G_{\mathbb{Q}_v}, W) = 0$.*

Proof Let $I_v < G_{\mathbb{Q}_v}$ denote the inertia subgroup, and ϕ_v a generator of $G_{\mathbb{Q}_v}/I_v$. Tate duality gives an exact sequence (see e.g. [22, 3.3.9])

$$0 \to H^1(G_{\mathbb{F}_v}, W^{I_v}) \to H^1(G_{\mathbb{Q}_v}, W) \to H^1(G_{\mathbb{Q}_v}, W^*(1))^* \to 0.$$

We have

$$H^1(G_{\mathbb{F}_v}, W^{I_v}) \simeq W^{I_v}/(\phi - 1)W^{I_v}.$$

Since W and $W^*(1)$ have weight $-2i$ and $2 - 2i$ respectively, we deduce $H^1(G_{\mathbb{Q}_v}, W) = 0$. □

Using the Euler characteristic formula above, we can reduce the computation of dimensions of Galois cohomology groups of Artin–Tate representations (i.e. Tate twists of Artin representations) to a theorem of Soulé [51, Theorem 5].

Theorem 6.1 (Soulé) *For any number field K, and any $n > 1$,*

$$\mathrm{h}^2(G_{K,T}, \mathbb{Q}_p(n)) = 0,$$

We deduce case (1) of Theorem 1.1 as follows. Let Z be an irreducible $\mathbb{Q}_p$-subvariety of $\mathrm{Res}(X)_{\mathbb{Q}_p}$, and let $U_n(Z/X)$ be as in Proposition 4.2. By Lemma 5.4, and Theorem 6.1, it is enough to prove that for infinitely many n, $\mathrm{gr}_n(U_n^{\mathrm{dR}}(Z/X))/F^0 = \mathrm{gr}_n(U_n^{\mathrm{dR}}(Z/X))$ is not contained in $\mathrm{loc}_p H^1_f(G_{\mathbb{Q}}, \mathrm{gr}_n(U_n))$. By Lemma 5.6, it is enough to prove that, for infinitely many n, $\mathrm{gr}_n(U_n(Z/X))$ is not contained in $U_n^{c=-1}$.

This follows from the fact that $\oplus_n \mathrm{gr}_n(U_n(Z/X))$ is a sub-Lie algebra of the graded Lie algebra $\oplus_n \mathrm{gr}_n U_n$.

6.2 Theorem 1.1, case (2)

In this subsection we prove Theorem 1.1 in the case X is a smooth projective curve of genus $g > 0$, and we assume either the Bloch–Kato conjectures or Jannsen's conjecture, which we now recall.

Conjecture 6.1 (Bloch–Kato, [8, Conjecture 5.3]) *Let Z be a smooth projective variety over $\mathbb{Q}$. For any $n > 0$ and $2r - 1 \neq n$, the map*

$$ch_{n,r} : K_{2r-1-n}(Z) \otimes \mathbb{Q}_p \to H^1_g(G_{\mathbb{Q}}, H^n(Z_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(r)))$$

is an isomorphism.

Conjecture 6.2 (Jannsen, [34, Conjecture 1]) *Let Z be a smooth projective variety over K with good reduction outside T. Then*

$$H^2(G_{K,T}, H^i(Z_{\overline{K}}, \mathbb{Q}_p(n))) = 0$$

whenever $i + 1 < n$ or $i > 2n$.

In particular, when $2r-1-n < 0$, since negative K-groups are zero, Conjecture 6.1 implies $H^1_f(G_{\mathbb{Q}}, H^n_{\text{ét}}(Z_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(r))) = 0$.

6.2.1 Finiteness assuming Conjecture 6.1

Part (2) of Lemma 6.1 implies the following corollary of Conjecture 6.1.

Lemma 6.3 *Let X be a smooth projective geometrically irreducible curve of genus $g > 1$. Suppose Conjecture 6.1 holds for $H^n_{\text{ét}}(X^n_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(n))$. Then, for any Galois stable direct summand W of $H^n_{\text{ét}}(X^n_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(n))$, we have*

$$\mathrm{h}^1_f(G_{\mathbb{Q}_p}, W) - \mathrm{h}^1_f(G_{\mathbb{Q},T}, W) = \mathrm{h}^0(G_{\mathbb{R}}, W)$$

when $n > 2$.

This means that, for all but finitely many i,

$$\mathrm{Ker}(H^1_f(G_{\mathbb{Q},T}, \mathrm{gr}_i(U_i)) \to H^1_f(G_{\mathbb{Q}_p}, \mathrm{gr}_i(U_i))) = 0.$$

Similarly, by part (3) of Lemma 6.1, Jannsen's conjecture implies that the localisation map

$$H^1_f(G_{K,T}, H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p(i))) \hookrightarrow \oplus_{v|p} H^1_f(G_{K_v}, H^i_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p(i))) \tag{38}$$

is injective for $i > 1$. This implies that

$$\sum_{i=1}^{n} \dim \mathrm{Ker}(\mathrm{loc}_p : H^1_f(G_{\mathbb{Q},T}, \mathrm{gr}_i(U_i)) \to H^1_f(G_{\mathbb{Q}_p}, \mathrm{gr}_i(U_i))) \\ = \dim \mathrm{Ker}(H^1_f(G_{\mathbb{Q},T}, V) \to H^1_f(G_{\mathbb{Q}_p}, V)). \tag{39}$$

To prove finiteness of $X(K \otimes \mathbb{Q}_p)_n$, we now show that $U_n(Z/\mathrm{Res}(X))$ contains a large Artin–Tate part, and use this to apply Lemma 5.6. This is done by showing that the unipotent fundamental group of a projective curve contains many Tate motives.

Lemma 6.4 *(Hain) Let X be projective. Then*

$$\mathrm{gr}_6(U_6(X))^{\mathrm{Sp}(U_1(X))} \neq 0.$$

Proof This is proved in Hain [29, §9]. For the sake of completeness we briefly recall the argument. Let $\mathfrak{p} := \varinjlim \oplus \mathrm{gr}_i(U_i(X))$, viewed as a graded Lie algebra, so that $U_1(X)$ has weight -1, and let $\mathrm{sp}(U_1(X)) := \mathrm{Lie}(\mathrm{Sp}(U_1(X)))$. By computing the Lie algebra cohomology of $\mathfrak{p}$, Hain shows that, for all $i < -2$, the complex

$$\mathrm{gr}^W_i(\wedge^\bullet \mathfrak{p}) : \ldots \to \mathrm{gr}^W_i(\wedge^2 \mathfrak{p}) \to \mathrm{gr}^W_i \mathfrak{p} \to 0$$

is exact. Hence given the irreducible representations arising in $\mathrm{gr}_1(U_i(X)), \ldots, \mathrm{gr}_{i-1}(U_i(X))$, one may compute $\mathrm{gr}_i(U_i(X))$ as an $\mathrm{sp}(U_1(X))$-representation using the complex $\mathrm{gr}^W_{-i}(\wedge^\bullet \mathfrak{p})$. We obtain a non-zero morphism of $\mathrm{sp}(U_1(X))$-representations $\mathbb{Q}_p \to \mathrm{gr}_6(U_6(X))$. □

Lemma 6.5 *Let X be a smooth projective curve over a number field K. Let $\mathrm{gr}^\bullet(L)$ be the associated graded of the Lie algebra of the $\mathbb{Q}_p$ pro-unipotent completion of the étale fundamental group of $X_{\overline{K}}$. Then $\mathrm{gr}^\bullet(L)$ contains a free Lie algebra generated by $\mathbb{Q}_p(3)$ and $\mathbb{Q}_p(5)$.*

Proof By the previous lemma, $\mathbb{Q}_p(3)$ is a direct summand of $\mathrm{gr}^6(L)$. This follows from the fact that it is enough to prove this as a statement about representations of $\mathrm{GSp}(V)$, for V a $2g$-dimensional vector space with a nondegenerate symplectic form. Namely one wants to prove the corresponding statement for $L(V)$, which we define to be the free Lie algebra on V modulo the Lie ideal generated by $\mathbb{Q}_p(1) \subset \wedge^2 V$. Then it is enough to replace $\mathrm{GSp}(V)$ with $\mathrm{Sp}(V)$ and prove that $L(V)$, as a representation of $\mathrm{Sp}(V)$, contains an invariant vector in $\mathrm{gr}^6 L(V)$.

Similarly, to prove the Lemma it is enough to prove that $L(V)$ contains a free Lie algebra with trivial $\mathrm{Sp}(V)$ action, and generators lying in $\mathrm{gr}^6(L(V))$ and $\mathrm{gr}^{10}(L(V))$. By a theorem of Labute [42, Theorem 1], if L is a free Lie algebra on a vector space V of dimension > 2, modulo a Lie ideal generated by one element in $\wedge^2 V$, then $[L, L]$ is a free Lie algebra (more precisely Labute's theorem says it is a sub-Lie algebra of a free Lie algebra, and thus is free by Shirsov's theorem). Hence, to prove that $L(V)$ contains the free Lie algebra mentioned above, it is enough to prove that $\mathrm{gr}^6(L(V))$ and $\mathrm{gr}^{10}(L(V))$ both contain copies of the trivial representation.

Hain proves in loc. cit. that $\mathrm{gr}^6(L(V))$ contains a copy of the trivial representation. Now let I be the Lie ideal in $[L(V), L(V)]$ generated by the copy of $\mathbb{Q}_p(3)$ in the 6th graded piece. By another theorem of Labute [41, Theorem 1], $I/[I, I]$ is a free rank one $\mathcal{U}(L/I)$ module, where $\mathcal{U}(L/I)$ is the universal enveloping algebra of L/I. In particular, for all $i \geq 6$, $\mathrm{gr}^{i-6}(\mathcal{U}(L/I))$ is a direct summand of $\mathrm{gr}^i(L(V))$ as an $\mathrm{Sp}(V)$ representation. To show that $\mathrm{gr}^{10}(L(V))$ contains a copy of the trivial representation, it is hence enough to show that $\mathrm{gr}^4\mathcal{U}(L/I)$ contains a copy of the trivial representation. By the Poincaré–Birkhoff–Witt theorem, $\mathcal{U}(L/I)$ is isomorphic, as a representation of $\mathrm{Sp}(V)$, to the symmetric algebra on $\mathcal{U}(L/I)$. In particular, we see that $I/[I, I]$ contains a copy of $\mathrm{Sym}^2\,\mathrm{gr}^2(L)$, which contains a copy of the trivial representation. This can be seen by direct computation, or from the fact that, since $\mathrm{gr}^2(L)$ is self-dual as a representation of $\mathrm{Sp}(V)$, either $\mathrm{Sym}^2\,\mathrm{gr}^2(L)$ or $\wedge^2\mathrm{gr}^2(L)$ must contain a copy of the trivial representation, and the latter does not. □

We now deduce case (2) of Theorem 1.1, assuming Jannsen's conjecture, as follows. Let L^t be the maximal Artin–Tate subspace of the graded Lie algebra $\oplus\mathrm{gr}^i(\mathrm{Lie}(U_i(\mathrm{Res}(X))))$, i.e. the maximal subrepresentation each of whose summands becomes a Tate twist after a finite extension. By Lemma 6.5, this is infinite dimensional, and contains a free Lie algebra. Since $\mathrm{gr}^\bullet(U_n(Z/\mathrm{Res}(X)))$ is Galois stable over a finite extension of $\mathbb{Q}$, and $U_n(Z/\mathrm{Res}(X))$ surjects onto a factor of $U_n(\mathrm{Res}(X))$, the intersection of $\mathrm{gr}^\bullet(U_n(Z/\mathrm{Res}(X))$ with L^t is infinite-dimensional and contains a free Lie algebra. Hence the dimension of the image of $\oplus\mathrm{gr}_i U_i(Z/\mathrm{Res}(X)) \cap L^t$ in $L^t/(L^t)^{c=-1}$ is infinite dimensional, and hence by Lemma 5.6, together with (39), $X(K \otimes \mathbb{Q}_p)_n$ is finite.

6.3 Proof of Theorem 1.1, case (3)

We follow the argument in [37]. Recall E/K is an elliptic curve with complex multiplication and $X = E - O$. Let $\overline{U}_n$ denote the maximal metabelian quotient of $U_n(X)$. By Lemma 5.7, $\varprojlim[\overline{U}_n, \overline{U}_n]$ is a free module of rank one over the completed symmetric algebra of $V := V_pE$. The Tate module has a decomposition $T_pE \simeq T_\pi E \oplus T_{\overline{\pi}}E$ over L where $L|K$ is the field over which the CM is defined. Let a and b be generators of $\mathrm{Lie}(\overline{U}_n)$ whose images in V generate $V_\pi E := \mathbb{Q}_p \otimes T_\pi E$ and $V_{\overline{\pi}}E := \mathbb{Q}_p \otimes T_{\overline{\pi}}E$ respectively. Then $\mathrm{Lie}(\overline{U}_n)$ has a $\mathbb{Q}_p$ basis a, b and $\mathrm{ad}(a)^i\mathrm{ad}(b)^j[a, b]$ for $i+j \leq n-2$. Let $L_{\geq i,\geq j}$ denote the subspace generated by $\mathrm{ad}(a)^k\mathrm{ad}(b)^l[a, b]$ for $k \geq i, l \geq j$. Then $L_{\geq i,\geq j}$ is a Lie ideal, and $L_{\geq i,\geq j} + L_{\geq j,\geq i}$ is a $\mathrm{Gal}(\overline{K}|K)$-stable Lie ideal. Let $\overline{L}_n$ denote the quotient of $\mathrm{Lie}(\overline{U}_n)$ by $L_{\geq 1,\geq 1}$. We have isomorphisms

$$\mathrm{gr}_i\overline{L}_n \simeq (\mathrm{Ind}_L^K(V_\pi(E)^{\otimes(n-3)}))(1)$$

for all $3 \leq i \leq n$.

By Lemma 5.1 we may enlarge the field K and hence we may assume that $K|\mathbb{Q}$ is Galois, and that all isogenies between $E_{\sigma,\overline{K}}$ for different embeddings σ are in fact defined over K. Hence, if $H < \mathrm{Gal}(K|\mathbb{Q})$ is the subgroup generated by all σ such that E is isogenous (over K or equivalently $\overline{K}$) to E_σ, then V descends to a Galois representation V_0 of $K_0 := K^H$.

Let $L(V)$ be the associated graded Lie algebra of $\varprojlim \overline{L}_n$. Equivalently, we may define $L(V)$ to be the free metabelian Lie algebra on $\overleftarrow{V}$ modulo the ideal generated by $\mathbb{Q}_p(2)$. We may similarly define $L(V_0)$. Recall that we have an isomorphism of representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p|\mathbb{Q}_p)$

$$\mathrm{Res}^{\mathbb{Q}}_{\mathbb{Q}_p} \mathrm{Ind}^{\mathbb{Q}}_{K_0} L(V_0) \simeq \oplus_{w|p} \mathrm{Res}^{K_0}_{K_{0,w}} L(V_0).$$

and that in this way we think of $H^1_f(G_{K_{0,w}}, \mathrm{gr}_n L(V_0))$ as a direct summand of $H^1_f(G_{\mathbb{Q}_p}, \mathrm{Ind}^{\mathbb{Q}}_{K_0} \mathrm{gr}_n L(V_0))$.

Lemma 6.6 *For any infinite set $\mathcal{S}$ of positive integers, there is a prime w of K_0 lying above p with the following property. For a positive proportion of n in $\mathcal{S}$, the intersection of $\mathrm{loc}_p H^1_f(G_{\mathbb{Q}}, \mathrm{Ind}^{\mathbb{Q}}_{K_0} \mathrm{gr}_n(L(V_0)))$ with $H^1_f(G_{K_{0,w}}, \mathrm{gr}_n(L(V_0)))$ has dimension at most one.*

Proof Since E has potentially good reduction at all primes, for all v in S there is a finite Galois extension $L_w|K_v$ such that the action of G_{L_w} on $V_p(E)$ is unramified of weight -1. Hence for all $i > 2$, and any G_{K_v}-stable quotient W of $\mathrm{gr}_i(U)$, arguing as in Lemma 6.2, we have $H^1(G_{L_w}, W) = 0$. By the Hochschild–Serre spectral sequence, and the fact that $H^1(\mathrm{Gal}(L_w|K_v), W') = 0$ for all representations W' (or that $H^0(G_{L_w}, W) = 0$), we deduce that $H^1(G_{K_{0,w}}, W) = 0$ for all $i > 2$. Hence for all $i > 2$, we have

$$H^1_f(G_{K_0,T}, \mathrm{gr}_i \overline{L}_i) = H^1_{f,S}(G_{K_0,T}, \mathrm{gr}_i \overline{L}_i).$$

It will be enough to prove that for all but finitely many i, $h^1(G_{K_0,T}, \mathrm{gr}_i L(V_0)) = [K_0 : \mathbb{Q}]$. By Lemma 6.1, it will hence be enough to prove that $h^2(G_{K_0,T}, \mathrm{gr}_i L(V_0)) = 0$, or equivalently that $h^1_f(G_{K_0,T}, \mathrm{gr}_i L(V_0)^*(1)) = 0$. It will hence be enough to prove that

$$H^1(G_{L,T}, V_\pi(E)^{\otimes n}) \to \oplus_{v \in T} H^1(G_{L_v}, V_\pi(E)^{\otimes n})$$

is injective for all but finitely n (and similarly for $V_{\overline{\pi}}(E)$.

Let X_∞ denote the Galois group of the maximal unramified $\mathbb{Z}_p$-extension L_∞ of L, where $\Lambda = \mathbb{Z}_p[\![\mathrm{Gal}(L_\infty|L)]\!]$. From the Hochschild–Serre spectral sequence we have an exact sequence

$$H^1(\mathrm{Gal}(L_\infty|L), V_\pi(E)^{\otimes i}) \to H^1(G_{L,T}, V_\pi(E)^{\otimes i}) \to \mathrm{Hom}_\Lambda(X_\infty, V_\pi(E)^{\otimes i}),$$

using the isomorphism $\mathrm{Hom}_\Lambda(X_\infty, V_\pi(E)^{\otimes i}) \simeq H^0(\mathrm{Gal}(L_\infty|L), H^1(\mathrm{Gal}(\overline{\mathbb{Q}}|L_\infty), V_\pi(E)^{\otimes i}))$. Since $H^1(\mathrm{Gal}(L_\infty|L), V_\pi(E)^{\otimes i}) = 0$ for all $i \neq 0$, it is enough to bound the dimension of $\mathrm{Hom}_\Lambda(X_\infty, V_\pi(E)^{\otimes i})$. By Iwasawa's theorem [33, Theorem 5], X_∞ is a torsion Λ-module, hence $\mathrm{Hom}_\Lambda(X_\infty, V_\pi(E)^{\otimes i}) = 0$ for all but finitely many i, and similarly for $V_{\overline{\pi}}(E)$. □

Now we take $\mathcal{S}$ to be $2 + e \cdot \mathbb{Z}_{>0}$, where $e := \#\mu(F)$, $F := \mathrm{End}(E_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$ and $\mu(F)$ is its group of roots of unity. Let w be a prime as in Lemma 6.6 for the set $\mathcal{S}$. Let $Z \subset (\mathrm{Res}_{K|\mathbb{Q}} E)_{\mathbb{Q}_p}$ be an irreducible subvariety dominating a factor above w. We will henceforth identify $\mathrm{Ind}_K^{\mathbb{Q}} L(V_0)$ with the associated graded Lie algebra of the corresponding quotient of $\varprojlim U_n(\mathrm{Res}(X))$. Let $\overline{L}_i(Z/\mathrm{Res}(X))$ denote the image of the $\mathbb{Q}_p$-nilpotent Lie algebra of $Z_{\overline{\mathbb{Q}}_p}$ in $\mathrm{Ind}_K^{\mathbb{Q}} \overline{L}_i$. To complete the proof of case (3) of Theorem 1.1, we need to show that, for infinitely many $i > 0$, $H^1_f(G_{\mathbb{Q}_p}, \mathrm{gr}_i(\overline{L}_i(Z/\mathrm{Res}(X))))$ is not contained in $\mathrm{loc}_p H^1_f(G_{\mathbb{Q},S}, \mathrm{Ind}_K^{\mathbb{Q}} \mathrm{gr}_i(\overline{L}_i))$. Since there are no isogenies between $E_{\overline{K},v_1}$ and $E_{\overline{K},v_2}$ if v_1 lies above w and v_2 does not, the image of $V_p \mathrm{Alb}(Z)$ in $V_p(\mathrm{Res}(J)) \simeq \mathrm{Ind}_K^{\mathbb{Q}} V_p E$ is a direct sum of the image in $\oplus_{v|w} V_p E_v$ and the image in $\oplus_{v\nmid w} V_p E_w$. It follows that $\overline{U}_n(Z/\mathrm{Res}(X))$ is a direct product of its image in $\prod_{v|w} \overline{U}_n(X_v)$ and its image in $\prod_{v\nmid w} \overline{U}_n(X_v)$. Hence, to show that for infinitely many i, $H^1_f(G_{\mathbb{Q}_p}, \mathrm{gr}_i(\overline{U}_i(Z/\mathrm{Res}(X))))$ is not contained in $\mathrm{loc}_p H^1_{f,S}(G_{\mathbb{Q},S}, \mathrm{Ind}_K^{\mathbb{Q}} \mathrm{gr}_i(\overline{U}_i(X)))$, it will be enough to show that for infinitely many i, the image of $H^1_f(G_{\mathbb{Q}_p}, \mathrm{gr}_i(\overline{U}_i(Z/\mathrm{Res}(X))))$ in $\oplus_{v|w} H^1_f(G_{K_v}, \mathrm{gr}_i(\overline{U}_i))$ is not contained in $M_i := \mathrm{loc}_p H^1_f(G_{\mathbb{Q},S}, \mathrm{Ind}_K^{\mathbb{Q}} \mathrm{gr}_i(\overline{U}_i)) \cap \oplus_{v|w} H^1_f(G_{K_v}, \mathrm{gr}_i(\overline{U}_i))$.

Via the isomorphism $V \simeq \mathrm{Res}_K^{K_0} V_0$, we have an H-action on $H^1_f(G_{\mathbb{Q}}, \mathrm{Ind}_K^{\mathbb{Q}} \mathrm{gr}_i(U_i))$, compatible with the H-action on $\oplus_{v|w} H^1_f(G_{K_v}, \mathrm{gr}_i(U_i))$. In particular, M_i is an H-submodule of $\oplus_{v|w} H^1_f(G_{K_v}, \mathrm{gr}_i(U_i))$. Hence we deduce that it is enough to show that for infinitely many i, the H-module N_i generated by the image of $H^1_f(G_{\mathbb{Q}_p}, \mathrm{gr}_i(\overline{U}_i(Z/\mathrm{Res}(X))))$ in $\oplus_{v|w} H^1_f(G_{K_v}, \mathrm{gr}_i(\overline{U}_i))$ is not contained in M_i. In fact, we show that N_i^H is not contained M_i^H. Note that M_i^H is equal to the intersection of $\mathrm{loc}_p H^1_f(G_{\mathbb{Q}}, \mathrm{gr}_i(L(V_0)))$ with $H^1(G_{K_{0,w}}, \mathrm{gr}_i(L(V_0)))$.

Note that, via the isomorphism $\oplus_{v|w} H^1_f(G_{K_v}, \mathrm{gr}_i(\overline{L}_i)) \simeq \mathbb{Q}_p[H] \otimes H^1_f(G_{K_{0,w}}, \mathrm{gr}_i(\overline{L}_i))$, the subspace M_i^H can be identified with the image of $H^1_f(G_{\mathbb{Q}_p}, \mathrm{gr}_i(\overline{L}_i(Z/\prod_{v|w} X_v)))$ in $H^1_f(G_{K_{0,w}}, \mathrm{gr}_i(\overline{L}_i))$ with respect to the norm map

$$\mathrm{Nm} : \mathbb{Q}_p[H] \otimes H^1_f(G_{K_{0,w}}, \mathrm{gr}_i(\overline{L}_i)) \to H^1_f(G_{K_{0,w}}, \mathrm{gr}_i(\overline{L}_i))$$

induced by the co-unit map $\mathbb{Q}_p[H] \to \mathbb{Q}_p$.

Proposition 6.1 *Let $Z \subset (\mathrm{Res}_{K|\mathbb{Q}} E)_{\mathbb{Q}_p}$ be an irreducible subvariety. Suppose Z dominates a factor above w. Let $W \subset \mathrm{Ind}_K^{K_0} V_0$ denote the image of $V_p \mathrm{Alb}(Z)$. Let $L(W) \subset \mathrm{Ind}_K^{K_0} L(V_0)$ denote the sub-Lie algebra of $L(V)$ generated by W. Then for infinitely many $i > 0$, the norm map, restricted to $\mathrm{gr}_i(L(W))$, surjects onto $\mathrm{gr}_i(L(V_0))_w$.*

Proof In fact we will show this for a positive proportion of $i > 0$. By embedding $\mathbb{Q}_p$ into $\mathbb{C}$, we can descend W to a sub-$\mathbb{Q}$-vector space $W_{\mathbb{Q}}$ of $H_1(\mathrm{Res}_{K|\mathbb{Q}}(E)_{\mathbb{C}}, \mathbb{Q})$. It follows that $W_{\mathbb{Q}}$ is an $F := \mathrm{End}(E_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}$-subspace, hence we may assume it is of the form $(\lambda_1, \ldots, \lambda_m) \cdot H_1(E_{\mathbb{C}}, \mathbb{Q})$ for some $\lambda_i \in F$ not all zero. Fix an embedding of F into $\mathbb{Q}_p$. Then, choosing a basis $e, \overline{e}$ of V_0 such F acts on e by the embedding

and on $\overline{e}$ by its conjugate, it follows that the ith graded piece of $L(W)$ is spanned by elements of the form

$$(\lambda_j^{i-1}\overline{\lambda}_j \cdot e^{i-2}[e, \overline{e}])_{j=1}^m.$$

We see that it will be enough to prove that for a positive proportion of $i \geq 0$,

$$\sum_j \lambda_j^{ei+1}\overline{\lambda}_j \neq 0 \tag{40}$$

(technically, this just shows that the norm is nonzero, but conjugating (40) shows that the map is surjective).

Without loss of generality, we may assume all the λ_i are nonzero. Re-ordering, we may assume that $\lambda_1^e, \ldots, \lambda_k^e$ are pairwise distinct and $\lambda_i^e \in \{\lambda_1^e, \ldots, \lambda_k^e\}$ for all i. If $k = 1$, then it is enough to prove that

$$\sum \lambda_j \overline{\lambda}_j \neq 0,$$

which follows from the fact that $\lambda_j\overline{\lambda}_j > 0$. If $k = 2$, then by the same argument as for $k = 1$, (40) can be rewritten as

$$\sum_{j=1}^2 a_j \lambda_j^{ei} \neq 0.$$

for some rational constants $a_i > 0$. Since $\lambda_1^e \neq \lambda_2^e$, we have that $\lambda_1^{ie} \neq \lambda_2^{ie}$ for all $i > 0$, since distinct eth powers in $F^\times$ cannot differ by a root of unity. Hence (40) holds for all but at most one i.

Now suppose $k \geq 3$. By Szemerédi's theorem [53], it will be enough to prove that the set of i such that (40) does not hold does not contain an arithmetic progression of length k. Let $i_1, \ldots, i_k$ be an arithmetic progression in $e\mathbb{Z}_{>0}$. Let $d = i_2 - i_1$. Then to prove that (40) holds for at least one of the i_j, it is enough to prove that for any positive constants a_i in $\mathbb{Q}$, we have

$$\sum_{j=1}^k a_j \lambda_j^{i_1} v_j \neq 0$$

where $v_j \in F^k$ is the vector $(1, \lambda_j^{de}, \ldots, \lambda_j^{de(k-1)})$. Taking determinants, this follows from the fact that $\lambda_i^{ed} \neq \lambda_j^{ed}$ for $i \neq j$ between 1 and k. □

6.4 Proof of Theorem 1.1, case (4)

As in [13] and [19], the key estimate in the proof of case (4) of Theorem 1.1 is the following theorem of Coates and Kim, coming from Greenberg's generalisation of Iwasawa's theorem to the case of $\mathbb{Z}_p^d$ extensions ([23, Theorem 1]).

Theorem 6.2 (Coates, Kim [13, Theorem 0.1]) *Let Y/L be a curve of genus g whose Jacobian has complex multiplication. Let $\overline{U}_n(Y)$ be the maximal metabelian quotient of $U_n(Y)$. Then, for any finite extension $L'|L$, we have*

$$\sum_{j=1}^{n} \mathrm{h}^2(G_{L',T}, \mathrm{gr}_i(\overline{U}_n(Y))) \leq Bn^{2g-1},$$

for some constant B depending on L' and Y.

As in case (3), by Lemma 5.1 we may enlarge K if necessary to assume that $K|\mathbb{Q}$ is Galois and that all isogenies between $J_{\sigma,\mathbb{C}}$ for different embeddings σ are in fact defined over K. Hence, if $V := V_p J$ and $H < \mathrm{Gal}(K|\mathbb{Q})$ is the subgroup generated by all σ such that $\mathrm{Jac}(X)$ is isogenous (over K or equivalently $\overline{K}$) to $\mathrm{Jac}(X_\sigma)$, then V descends to a Galois representation V_0 of $K_0 := K^H$.

Let $F := \mathrm{End}(J_{\overline{K}}) \otimes \mathbb{Q}$ be the CM field by which J has complex multiplication. Let $e := \#\mu(F')$, where F' is the Galois closure of F. Over a finite extension of $\mathbb{Q}$, V_0 decomposes as a direct sum of characters χ_i for $1 \leq i \leq 2g$. Over K_0, the Galois action permutes the χ_i. In particular, if $S \subset \{1, \ldots, 2g\}^n$ is stable under the action of S_{2g}, then the subspace

$$\oplus_{(i_j)\in S} \otimes \chi_{i_j}$$

of $V_0^{\otimes n}$ is stable under the action of G_K. Let L denote the free metabelian Lie algebra generated by V_0. For n divisible by e, let $V_0[n] \subset \mathrm{gr}_n(L)$ denote the subspace generated by the image of $\prod_{i=1}^{2g} \mathrm{Sym}^{a_i}(\chi_i) \otimes \chi_j \otimes \chi_k$ in L under the nested commutator map, where a_i are such that a_i is in $e \cdot \mathbb{Z}_{\geq 0}$ if $i \neq j, k$, and $a_i + 1 \in e \cdot \mathbb{Z}_{>0}$ otherwise.

Lemma 6.7 *There is a positive constant $c_0 < 1$ with the following property: there is a prime w of K_0 lying above p such that, for a positive proportion of n dividing e, the intersection of $\mathrm{loc}_p H^1_f(G_{\mathbb{Q}}, \mathrm{Ind}_{K_0}^{\mathbb{Q}} V_0[n])$ with $H^1_f(G_{K_{0,w}}, V_0[n])$ is at most c_0 times the dimension of $H^1_f(G_{K_{0,w}}, V_0[n])$.*

Proof It will be enough to show that the dimension of $\mathrm{loc}_p H^1_f(G_{\mathbb{Q}}, \mathrm{Ind}_{K_0}^{\mathbb{Q}} V_0[n])$ is at most $c_0 < 1$ times that of

$$H^1_f(G_{\mathbb{Q}_p}, \mathrm{Ind}_{K_0}^{\mathbb{Q}} V_0[n]) = \oplus_{w|p} H^1_f(G_{K_{0,w}}, V_0[n]).$$

By Lemma 6.1 and Theorem 6.2 is enough to show that $\dfrac{\dim(\mathrm{Ind}_{K_0}^{\mathbb{Q}} V_0[n])^{c=1}}{\dim(\mathrm{Ind}_{K_0}^{\mathbb{Q}} V_0[n])}$ is bounded below by a constant > 0 for n sufficiently large. If K_0 contains one complex place,

then it follows that the dimension is at least $[K_0 : \mathbb{Q}]^{-1} \cdot \dim V_0[n]$. Hence suppose K_0 is totally real. Complex conjugation defines an involution of V_0 which nontrivially permutes the vector subspaces χ_i. Hence $V_1 := \oplus_i \chi_i^{\otimes e} \subset \mathrm{Sym}^e V_0$ is stable under conjugation and the minus eigenspace of V_1 is nontrivial. Via the action of $\mathrm{Sym}^\bullet V_0$ on $[L, L]$, the module $\oplus_{e|n} V_0[n]$ is a module under $\mathrm{Sym}^\bullet V_1$, and by Lemma 5.7, for any nonzero element x of $\mathrm{Sym}^\bullet V_1$, the kernel of the action of x on $\oplus_{e|n} V_0[n]$ is zero. Choosing a nonzero element of V_1 in the minus eigenspace with respect to complex conjugation, we get an injection

$$V_0[n]^{c=-1} \hookrightarrow V_0[n+e]^{c=1}.$$

Since $\dim V_0[n]/V_0[n+e]$ is bounded by a nonzero constant, we see that $V_0[n]^{c=1}$ is a positive proportion of $V_0[n]$. □

For a prime v of K, let L_v denote the free metabelian Lie algebra generated by $V_v := V_p \,\mathrm{Jac}(X_v)$, and $\overline{L}_v$ the associated graded of the Lie algebra of the metabelian quotient of the $\mathbb{Q}_p$-unipotent fundamental group of $X_{v,\overline{\mathbb{Q}}_p}$. Then, by Lemma 5.7, we have an isomorphism of $G_{\mathbb{Q}_p}$-representations

$$\overline{L}_v \simeq L_v / \mathrm{Sym}^\bullet(V_v)(1). \tag{41}$$

Let w be a prime of K_0. The action of G_{K_0} on $\oplus_{v|w} V_v$ induces an action on $\oplus_{v|w} L_v$, giving an isomorphism

$$\mathrm{Ind}_K^{K_0} L \simeq \oplus_{v|w} L_v. \tag{42}$$

For each v, we have a decomposition of V_v as $\oplus_{i=1}^{2g} \chi_{i,v}$, such that the isomorphisms $V_v \simeq \mathrm{Res}\, V_0$ restrict to isomorphisms between $\mathrm{Res}\, \chi_{i,v}$ and $\mathrm{Res}\, \chi_i$ (where the latter restrictions are to a suitably large finite extension of K_0). In the same way as for V_0, we can define subspaces $V_v[n]$ of $\mathrm{gr}_n(L_v)$ for n divisible by e.

Note that we do not assume that the isogenies between $\mathrm{Jac}(X_v)$ for different v above w respect polarisations, and hence we cannot automatically use (41) and (42) to identify $\oplus \overline{L}_v$ with the induction of a quotient Lie algebra of L. However, since we restrict attention to the spaces $V_v[n]$ and $V_0[n]$, we can ignore this subtlety by the following lemma.

Lemma 6.8 *The surjection $L_v \to \overline{L}_v$ restricts to an injection on $\oplus_{e|n} V_v[n]$.*

Proof Let x be an element of $V_v[n] \cap \mathrm{Ker}(L_v \to \overline{L}_v)$. Then there is an element f of $\mathrm{Sym}^{n-2}(V_v)$ such that $x = f \cdot t$, where $t \in \wedge^2 V_v$ is a generator of $\mathrm{Ker}(L_v \to \overline{L}_v)$. Lemma 5.7 implies that x is uniquely determined by its Fox differentials. Let z_i be a generator of $\chi_{i,v}$. We may order the characters $\chi_{i,v}$ so that t is a one-dimensional subspace of $\oplus_{i=1}^{g} \chi_{i,v} \otimes \chi_{g+i,v}$ surjecting onto $\chi_{i,v} \otimes \chi_{g+i,v}$ for all i, hence the Fox differential of x with respect to z_i is given by $\alpha_i \cdot f \cdot z_{g+i}$ (when $i \leq g$) or $\alpha_i \cdot x \cdot z_{i-g}$ (when $i > g$) for some nonzero $\alpha_i \in \mathbb{Q}_p$. Since the Fox differential with respect to z_i

of an element of $V_v[n]$ must necessarily be in

$$\oplus_{(a_i)\in e\cdot\mathbb{Z}^{2g}_{\geq 0}} \mathrm{Sym}^{a_i-1}(\chi_i)\otimes(\otimes_{j\neq i}\mathrm{Sym}^{a_j}(\chi_j)),$$

we see that the congruence conditions force x to be an element of

$$\oplus_{(a_i)\in e\cdot\mathbb{Z}^{2g}_{\geq 0}} \mathrm{Sym}^{a_i-1}(\chi_i)\otimes \mathrm{Sym}^{a_{i+g}-1}(\chi_i)(\otimes_{j\neq i,g+i}\mathrm{Sym}^{a_j}(\chi_j))$$

for all $1\leq i\leq g$. It follows that x must equal zero. □

Let $Z\subset \mathrm{Res}(X)_{\mathbb{Q}_p}$ be an irreducible subvariety which dominates a factor of $\mathrm{Res}(X)$ at a prime lying above w. Let $W\subset \mathrm{Ind}_K^{K_0}(V)$ denote the image of $V_p\,\mathrm{Alb}(Z)$ in $V_p\,\mathrm{Res}\,J$. Let $L(W)$ denote the sub-Lie algebra of L generated by W. For n divisible by e, let $W[n]$ denote the intersection of $\mathrm{gr}_n(L(W))$ with $\oplus_{v|p}V_v[n]$.

By Lemma 6.8 and Theorem 6.2, to complete the proof of case (4) of Theorem 1.1, it will be enough to show that

$$\sum_{i\leq n:e|i}\dim(H^1_f(G_{\mathbb{Q}_p},W[i])/\mathrm{loc}_p\,H^1_f(G_{\mathbb{Q}},\mathrm{Ind}_K^{\mathbb{Q}}V[i])\cap H^1_f(G_{\mathbb{Q}_p},W[i]))\gg n^{2g}$$

(i.e. that it is bounded below by a nonzero constant times n^{2g}). Since

$$\lim_{n\to\infty}\dim V_0[n]/\dim \mathrm{gr}_n L(V_0)>0,$$

it is enough to show that this sum of dimensions makes up a positive proportion of $\sum_{i\leq n:e|i}\dim V_0[i]$.

As in the proof of case (3), we reduce to estimating the size of the image of $H^1_f(G_{\mathbb{Q}_p},W[i])$ in $\oplus_{v|w}H^1_f(G_{K_v},W[i])$ modulo M_i, where

$$M_i:=\mathrm{loc}_p\,H^1_f(G_{\mathbb{Q}},\mathrm{Ind}_K^{\mathbb{Q}}V[i])\cap\oplus_{v|w}H^1_f(G_{K_v},W[i]).$$

The dimension of this image is at least $\frac{1}{\#H}\dim N_i/M_i$, where N_i is the H-module generated by the image of $H^1_f(G_{\mathbb{Q}_p},W[i])$ in $\oplus_{v|w}H^1_f(G_{K_v},V_0[i])$.

We use this to reduce to comparing the subspaces M_i^H and N_i^H of $\mathrm{Ind}_{K_0}^{\mathbb{Q}}V_0[i]\simeq\prod_{v|w}V_v[i]$. As in case (3), we have an isomorphism

$$M_i^H\simeq\mathrm{loc}_p\,H^1_f(G_{\mathbb{Q},S},\mathrm{Ind}_{K_0}^{\mathbb{Q}}V_0[n])\cap H^1_f(G_{K_{0,w}},V_0[n])\subset H^1(G_{\mathbb{Q}_p},\mathrm{Ind}_{K_0}^{\mathbb{Q}}V_0[n]).$$

Hence, by Lemma 6.7, we know that for i sufficiently large, $\dim M_i^H/\mathrm{h}^1_f(G_{K_{0,w}},V_0[i])$ is bounded above by a constant strictly less than 1. Hence it will be enough to prove that $\dim N_i^H/\mathrm{h}^1_f(G_{K_{0,w}},V_0[i])$ tends to 1. Since $\dim F^0(\mathrm{gr}_i(U_i))=O(i^g)$, we have that $\dim F^0W[i]$ and $\dim V_0[i]$ are both $O(i^g)$. Hence, by the p-adic comparison theorem, it is enough to prove that $\dim\widetilde{N}_i^H/\dim V_0[i]$ tends to 1, where $\widetilde{N}_i$ is the

H-module generated by the image of $W[i]$ in $V_0[i]$ with respect to the composite of the projection to $\oplus_{v|w} V_v[i]$ with the norm map

$$\mathrm{Nm} : \oplus_{v|w} V_v[i] \simeq \mathbb{Q}_p[H] \otimes V_0[i] \to V_0[i].$$

Hence to complete the proof of case (4) of Theorem 1.1, it is enough to prove the following lemma regarding the image of $W[n]$ under the composite of the projection to $\oplus_{v|w} V_v[n]$ and the norm map above.

Lemma 6.9 *Let* $\mathrm{Nm}\, W[n] \subset V_0[n]$ *denote the image of* $W[n]$ *with respect to the norm map. Then*

$$\dim \mathrm{Nm}\, W[n] / \dim V_0[n] \to 1$$

as $n \in e \cdot \mathbb{Z}_{>0}$ *tends to infinity.*

Our proof of Lemma 6.9 is rather elaborate. We first need the following result.

Lemma 6.10 *Let* $x_1, \dots, x_n$ *be nonzero elements of a field* F *such that for all* $m > 0$ *and all* $i \neq j$, $x_i^m \neq x_j^m$. *Let* $y_1, \dots, y_n$ *be nonzero elements of* F. *Then, as* m *tends to infinity, the proportion of* i *in* $\{0, \dots, m\}$ *such that* $\sum_j y_j x_j^i \neq 0$ *tends to one uniformly in* m. *More precisely, for any* $\epsilon > 0$, *there is an* m_ϵ *independent of* x_i *and* y_i *such that, for all* $m > m_\epsilon$, $\sum_{j=1}^n y_j x_j^i \neq 0$ *for at least* $(1-\epsilon)m$ *elements of* $\{1, \dots, m\}$.

Proof If $n \leq 2$ the result is clear, so assume $n > 2$. Let $S_m \subset \{0, \dots, m\}$ be the set of i such that $\sum_j y_j x_j^i = 0$. By Szemerédi's theorem, it will be enough to show that S_m does not contain any arithmetic progression of length n. Let $\{i_1, \dots, i_n\} \subset \{1, \dots, m\}$ be an arithmetic progression in $\{1, \dots, m\}$. Let $d := i_2 - i_1$. Let $S_0 \subset S$ Then, since the x_i^d are pairwise distinct by hypothesis, the Vandermonde determinant $\det(x_i^{d\cdot(j-1)})_{1\leq i,j\leq n}$ is nonzero. Hence the vectors $(x_j^{i_1}, \dots, x_j^{i_n}) \in F^n$, for $1 \leq j \leq n$, are linearly independent. It follows that there is a k such that

$$\sum_j y_j x_j^{i_k} \neq 0.$$

□

Now let $F := \mathrm{End}^0(\mathrm{Jac}(X)_{\overline{K}}) \otimes \mathbb{Q}$ be the CM field associated to X, and let $\sigma_1, \dots, \sigma_{2g}$ be the embeddings of F into $\overline{\mathbb{Q}}$.

Lemma 6.11 *Let* $\lambda_1, \dots, \lambda_m$ *be* m *elements of* F *which are not all zero, and are all* e*th powers. Let* $S(n) := \{(a_1, \dots, a_{2g}) \in e \cdot \mathbb{Z}_{\geq 0}^{2g} : \sum a_j = n\}$. *Then, as* $n \in e \cdot \mathbb{Z}_{>0}$ *tends to infinity, the proportion of* (a_i) *in* $S(n)$ *such that*

$$F(a_1, \dots, a_{2g}) := \sum_{i=1}^{m} \prod_{j=1}^{2g} \sigma_j(\lambda_i)^{a_j}$$

is nonzero tends to 1.

Proof Firstly, clearly we can remove all λ_i equal to zero, hence we may assume that all λ_i are nonzero. We may also rescale so that $\lambda_1 = 1$.

We filter the set $\{1, \dots, m\}$ by subsets as follows. For $1 \leq i \leq 2g$, define T_i to be the set of j in $\{1, \dots, m\}$ such that $\sigma_k(\lambda_j) = \sigma_1(\lambda_j)$ for all $1 \leq k \leq i$. We prove, by descending induction on i, that for all $i \leq m$, as N tends to infinity the proportion of (a_j) in $S(n)$ such that

$$F_i(a_1, \dots, a_{2g}) := \sum_{k \in T_i} \prod_{j=1}^{2g} \sigma_j(\lambda_k)^{a_j}$$

is nonzero tends to 1. In the case where $i = 2g$, we see that all the λ_k for k in $T_{2\,g}$ are in fact in $\mathbb{Q}$. Since all the a_i are even and all λ_i are nonzero, each summand is strictly positive (also, since $\lambda_1 = 1$, $T_{2\,g}$ is nonempty).

Now fix a k between 2 and $2\,g$, and suppose that the proportion of (a_i) such that $F_k(a_1, \dots, a_{2\,g})$ is nonzero tends to 1 for (a_i) all divisible by e. If $T_k = T_{k-1}$ there is nothing to prove in the next inductive step, so assume that there is a j in T_{k-1} such that $\sigma_1(\lambda_j) \neq \sigma_k(\lambda_j)$. Let $(b_1, \dots, b_{2\,g})$ be a tuple such that $F_k(b_1, \dots, b_{2g})$ is nonzero. Let $R(b_1, \dots, b_{2\,g})$ be the set of tuples $(a_i) \in e \cdot \mathbb{Z}_{\geq 0}^{2\,g}$ such that $a_i = b_i$ for $i \notin 1, k-1$, and $a_1 + a_{k-1} = b_1 + b_{k-1}$. Let $\mu_1, \dots, \mu_\ell$ be the set of (distinct) possible values of $\sigma_k(\lambda_j^e)/\sigma_1(\lambda_j^e)$ for j in T_{k-1}, such that $\mu_1 = 1$. Then there are constants $c_1, \dots, c_\ell$ such that, for any (a_i) in $R(b_1, \dots, b_{2g})$, we can write

$$F_{k-1}(a_1, \dots, a_{2g}) = \sum_{i=1}^{\ell} c_i \cdot \mu_i^{(a_1 - b_1)/e}.$$

In particular, $c_1 = F_k(b_1, \dots, b_{2g}) \neq 0$, and hence the constants c_i are not all zero. Since the μ_i are all eth powers, for all $i > 0$ and $j_1 \neq j_2$, $\mu_{j_1}^i \neq \mu_{j_2}^i$. Hence the proportion of (a_i) in $R(b_1, \dots, b_{2\,g})$ such that $F_{k-1}(a_1, \dots, a_{2\,g})$ is nonzero tends to 1 uniformly in $b_1 + b_{k-1}$, by Lemma 6.10. Since, for any n_0, the proportion of (b_i) in $S(n)$ such that $b_1 + b_{k-1} \leq n_0$ tends to zero, we deduce that the proportion of (a_i) in $S(n)$ such that $F_{k-1}(a_1, \dots, a_{2\,g})$ is nonzero tends to 1 as required. □

Proof of Lemma 6.9 By embedding $\mathbb{Q}_p$ into $\mathbb{C}$ and viewing Z as a complex subvariety, we can descend the subspace W of $\oplus_{v|w} V_v$ to a subspace $W_{\mathbb{Q}}$ of $\prod H_1(X_{v,\mathbb{C}}, \mathbb{Q})$. Then we may assume W is a subspace of V_0^m of the form $(\lambda_1, \dots, \lambda_m) \cdot V_0$, for some λ_i in $F \subset \mathrm{End}(V_0)$. The action of $\lambda \in F$ on χ_i is given by $\sigma_i(\lambda)$ (after re-ordering the σ_i if necessary). Hence $\mathrm{Nm}\, W[n]$ consists of elements of the form

$$\sum_{i=1}^{m} \sigma_k(\lambda_i)\sigma_\ell(\lambda_i) \left(\prod_{j=1}^{2g} \sigma_j(\lambda_i)^{a_j} \right) \left(\prod_{j=1}^{2g} e_j^{a_j} \right) [e_k, e_\ell] \tag{43}$$

for $a_i \in S(n)$, where e_i is a generator of χ_i. Hence, to show that the kernel of the induced map $V_0[n] \to V_0[n]$ has dimension $o(\dim V_0[n])$, it is enough to show that the

proportion of a_i in $S(n)$ such that (43) is zero is $o(1)$, which follows from Lemma 6.11. □

Acknowledgements The author is very grateful to Nils Bruin, Minhyong Kim, Martin Orr and Samir Siksek for helpful discussions related to this paper. He is also indebted to the anonymous referee for their careful reading of an earlier version of this paper, including the identification of a serious error, as well as Jan Steffen Müller, Pavel Coupek, David Lilienfeldt, Luciena Xiao and Zijian Yao for comments and corrections.

Funding This study was funded by Royal Society (URF\R1\201215).

References

1. Ax, J.: On Schanuel's conjectures. Ann. Math. **93**, 252–268 (1971)
2. Ax, J.: Some topics in differential algebraic geometry I: analytic subgroups of algebraic groups. Am. J. Math. **94**(4), 1195–1204 (1972)
3. Balakrishnan, J., Besser, A., Bianchi, F., Mueller, J.S.: Explicit quadratic Chabauty over number fields. Isr. J. Math. **243**, 185–232 (2020)
4. Balakrishnan, J.S., Dogra, N.: Quadratic Chabauty and rational points, I: p-adic heights. Duke Math. J. **167** (2018). With an appendix by J. Steffen Müller
5. Balakrishnan, J.S., Dogra, N.: Quadratic Chabauty and rational points II: generalised height functions on Selmer varieties. Int. Math. Res. Not. IMRN **15**, 11923–12008 (2021)
6. Balakrishnan, J.S., Dan-Cohen, I., Kim, M., Wewers, S.: A non-abelian conjecture of Tate–Shafarevich type for hyperbolic curves. Math. Ann. **372**(1–2), 369–428 (2018)
7. Blázquez-Sanz, D., Casale, G., Freitag, J., Nagloo, J.: A differential approach to the Ax–Schanuel, I. arXiv preprint arXiv:2102.03384v2 (2021)
8. Bloch, S., Kato, K.: L-functions and Tamagawa numbers of motives. In: The Grothendieck Festschrift, vol. I, pp. 333–400. Birkhäuser, Boston (1990)
9. Borel, A.: Cohomologie réelle stable de groupes S-arithmétiques classiques. C. R. Acad. Sci. Paris Sér. A-B **274**, A1700–A1702 (1972)
10. Bosch, S., Lutkebohmer, W., Raynaud, M.: Néron Models (1990)
11. Carter, R., Segal, G., Macdonald, I.: Lectures on Lie groups and Lie algebras. London Mathematical Society Student Texts, vol. 32. Cambridge University Press, Cambridge (1995)
12. Chiarellotto, B., Le Stum, B.: F-isocristaux unipotents. Compos. Math. **116**, 81–110 (1999)
13. Coates, J., Kim, M.: Selmer varieties for curves with CM Jacobians. Kyoto J. Math. **50**(4), 827–852 (2010)
14. Corwin, D., Dan-Cohen, I.: The polylog quotient and the Goncharov quotient in computational Chabauty–Kim Theory I. Int. J. Number Theory **16**(8), 1859–1905 (2020)
15. Dan-Cohen, I.: Mixed Tate motives and the unit equation II. Algebra Number Theory **14**(5), 1175–1237 (2020)
16. Dan-Cohen, I., Wewers, S.: Mixed Tate motives and the unit equation. Int. Math. Res. Not. IMRN **17**, 5291–5354 (2016)
17. Deligne, P.: Le groupe fondamental de la droite projective moins trois points. In Galois groups over **Q**, Math. Inst. Res. Inst. Publ., vol. 16, pp. 79–297. Springer, Berlin (1989)
18. Dimitrov, M., Ramakrishnan, D.: Arithmetic quotients of the complex ball and a conjecture of Lang. Doc. Math. **20**, 1185–1205 (2015)

19. Ellenberg, J.S., Hast, D.R.: Rational points on solvable curves over $\mathbb{Q}$ via non-abelian Chabauty. Int. Math. Res. Not. IMRN **19**, 14770–14796 (2022)
20. Faltings, G.: Endlichkeitssätze für abelsche varietäten über zahlkörpern. Invent. Math. **73**(3), 349–366 (1983)
21. Faltings, G.: Mathematics around Kim's new proof of Siegel's theorem. Diophantine Geom. CRM Ser. **4**, 173–188 (2007)
22. Fontaine, J.-M., Perrin-Riou, B.: Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L. In: Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, pp. 599–706. Amer. Math. Soc., Providence (1994)
23. Greenberg, R.: The Iwasawa invariants of Γ-extensions of a fixed number field. Am. J. Math. **95**, 204–214 (1973)
24. Grothendieck, A.: Éléments de géométrie algébrique: IV. étude locale des schémas et des morphismes de schémas, première partie. Publ. Math. l'IHES **20**, 5–259 (1964)
25. Grothendieck, A.: Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux. Fasc. I: Exposés 1–8; Fasc. II: Exposés 9–13. Institut des Hautes Études Scientifiques, Paris,: Troisième édition, corrigée, p. 1962. Rédigé par un groupe d'auditeurs, Séminaire de Géométrie Algébrique (1965)
26. Hadian, M.: Motivic fundamental groups and integral points. Duke Math. J. **160**(3), 503–565 (2011)
27. Hain, R.M.: Higher Albanese manifolds. In: Hodge Theory (Sant Cugat, 1985), Lecture Notes in Math., vol. 1246, pp. 84–91. Springer, Berlin (1987)
28. Hain, R.M., Zucker, S.: Unipotent variations of mixed Hodge structure. Invent. Math. **88**(1), 83–124 (1987)
29. Hain, R.: Rational points of universal curves. J. Am. Math. Soc. **24**(3), 709–769 (2011)
30. Hast, D.R.: Rational points and unipotent fundamental groups. PhD Thesis, University of Wisconsin-Madison (2018)
31. Hast, D.R.: Functional transcendence for the unipotent Albanese map. Algebra Number Theory **15**(6), 1565–1580 (2021)
32. Ihara, Y.: On Galois representations arising from towers of coverings of $P^1 - \{0, 1, \infty\}$. Invent. Math. **86**(3), 427–459 (1986)
33. Iwasawa, K.: On $\mathbb{Z}_l$-extensions of algebraic number fields. Ann. Math. **98**, 246–326 (1973)
34. Jannsen, U.: On the l-adic cohomology of varieties over number fields and its Galois cohomology. In: Galois Groups over $\mathbb{Q}$, pp. 315–360. Springer, Berlin (1989)
35. Kim, M.: The motivic fundamental group of $\mathbf{P}^1 - \{0, 1, \infty\}$ and the theorem of Siegel. Invent. Math. **161**(3), 629–656 (2005)
36. Kim, M.: The unipotent Albanese map and Selmer varieties for curves. Publ. Res. Inst. Math. Sci. **45**(1), 89–133 (2009)
37. Kim, M.: p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication. Ann. Math. **172**, 751–759 (2010)
38. Kim, M.: Tangential localization for Selmer varieties. Duke Math. J. **161**(2), 173–199 (2012)
39. Kim, M., Tamagawa, A.: The l-component of the unipotent Albanese map. Math. Ann. **340**(1), 223–235 (2008)
40. Klingler, B.: Hodge loci and atypical intersections: conjectures. arXiv preprint arXiv:1711.09387v2 (2017)
41. Labute, J.P.: Algèbres de Lie et pro-p-groupes définis par une seule relation. Invent. Math. **4**, 142–158 (1967)
42. Labute, J.P.: Free ideals of one-relator graded Lie algebras. Trans. Am. Math. Soc. **347**(1), 175–188 (1995)
43. Mumford, D.: Abelian Varieties, vol. 108. Oxford University Press, Oxford (1974)
44. Nakamura, H., Tsunogai, H.: Some finiteness theorems on Galois centralizers in pro-l mapping class groups. J. Reine Angew. Math. **441**, 115–144 (1993)
45. Namakura, H., Takao, N.: Galois rigidity of pro-l pure braid groups of algebraic curves. Trans. AMS **350**(3), 1079–1102 (1998)
46. Olsson, M.: Towards non-abelian p-adic Hodge theory in the good reduction case. Mem. Am. Math. Soc. **210**, vi+157 (2011)
47. Revêtements étales et groupe fondamental. Lecture Notes in Mathematics, vol. 224. Springer, Berlin, 1971. Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1). Dirigé par A. Grothendieck. Augmenté de deux exposés de M. Raynaud (1971)

48. Serre, J.-P.: Galois cohomology. Springer Monographs in Mathematics. Springer, Berlin (2002). Translated from the French by Patrick Ion and revised by the author
49. Siegel, C.L.: Über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preuss ischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929. In On some applications of Diophantine approximations. Quad./Monogr
50. Siksek, S.: Explicit Chabauty over number fields. Algebra Number Theory **7**(4), 765–793 (2013)
51. Soulé, C.: K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale. Invent. Math. **55**(3), 251–295 (1979)
52. Stix, J.: Trading degree for dimension in the section conjecture: the non-abelian Shapiro lemma. Math. J. Okayama Univ. **52**(1), 29–43 (2010)
53. Szemerédi, E.: On sets of integers containing no k elements in arithmetic progression. Acta Arith. **27**, 199–245 (1975)
54. Triantafillou, N.: Restriction of scalars Chabauty and the S-unit equation. arXiv preprint arXiv:2006.10590v2 (2021)
55. Tsimerman, J.: Ax-Schanuel and o-minimality. O-Minimality Diophantine Geom. **421**, 216 (2015)