Refined Selmer equations for the thrice-punctured line in depth two

Best, Alex J.; Betts, L. Alexander; Kumpitsch, Theresa; Lüdtke, Martin; McAndrew, Angus W.; Qian, Lie; Studnia, Elie; Xu, Yujie

REFINED SELMER EQUATIONS FOR THE THRICE-PUNCTURED LINE IN DEPTH TWO

ALEX J. BEST, L. ALEXANDER BETTS, THERESA KUMPITSCH, MARTIN LÜDTKE, ANGUS W. MCANDREW, LIE QIAN, ELIE STUDNIA, AND YUJIE XU

Abstract. In [Kim05], Kim gave a new proof of Siegel's Theorem that there are only finitely many S-integral points on $\mathbb{P}^1_{\mathbb{Z}} \setminus \{0, 1, \infty\}$. One advantage of Kim's method is that it in principle allows one to actually find these points, but the calculations grow vastly more complicated as the size of S increases. In this paper, we implement a refinement of Kim's method to explicitly compute various examples where S has size 2 which has been introduced in [BD19]. In so doing, we exhibit new examples of a natural generalisation of a conjecture of Kim.

Contents

0. Introduction

Let S be a finite set of primes and let $\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0, 1, \infty\}$ where $\mathbb{Z}_S$ denotes the ring of S-integers. By *Siegel's Theorem*, the set $\mathcal{X}(\mathbb{Z}_S)$ is finite, but Siegel's proof is not constructive. One procedure to in principle compute the set $\mathcal{X}(\mathbb{Z}_S)$ was introduced by Kim [Kim05], who constructed a sequence of subsets, called the *Chabauty–Kim loci*, for each prime $p \notin S$:

$$\mathcal{X}(\mathbb{Z}_p) \supseteq \mathcal{X}(\mathbb{Z}_p)_{S,1} \supseteq \mathcal{X}(\mathbb{Z}_p)_{S,2} \supseteq \ldots \supseteq \mathcal{X}(\mathbb{Z}_S).$$

Kim showed that for $n \gg 0$ the set $\mathcal{X}(\mathbb{Z}_p)_{S,n}$ is finite, thus re-proving Siegel's theorem. The main advantage of Kim's approach is that it is more effective than Siegel's: in many small cases (all with $|S| \leq 1$ and $n \leq 4$) the sets $\mathcal{X}(\mathbb{Z}_p)_{S,n}$ have been computed explicitly [Bal+18; DCW15; CDC20].

2010 *Mathematics Subject Classification.* 14G05,11G55,11Y50.

In this paper we study a refinement of Kim's method introduced by the second author and Netan Dogra, which constructs *refined Chabauty–Kim loci* $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,n} \subseteq \mathcal{X}(\mathbb{Z}_p)_{S,n}$ which still contain the S-integral points. We compute these sets in the case that $n = 2$ and $|S| \leq 2$:

Theorem A (Proposition 3.4)**.** *Let $S = \{\ell\}$, and let $p \neq \ell$ be prime. Then $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ consists of the nontrivial $(p-1)$-st roots of unity $\zeta \in \mathbb{Z}_p$ for which $\mathrm{Li}_2(\zeta) = 0$, up to the natural action of S_3 on $\mathcal{X}$. Here, Li_2 is the p-adic dilogarithm.*

Theorem B (Theorem 3.10)**.** *Let $S = \{\ell, q\}$, and let $p \notin S$ be a prime. Then $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ is equal to the set of points $z \in \mathcal{X}(\mathbb{Z}_p)$ satisfying the equation*

$$a_{\ell,q} \mathrm{Li}_2(z) = a_{q,\ell} \mathrm{Li}_2(1-z)\,,$$

up to the natural action of S_3 on $\mathcal{X}$. Here, $a_{\ell,q}$ and $a_{q,\ell}$ are certain computable p-adic numbers. (See §2.3 for the definition of the constants $a_{\ell,q}$ and a description of an algorithm to compute them; this algorithm has been implemented in SageMath [KLS21].)

These results should be understood in the context of Kim's Conjecture[1] [Bal+18, Conjecture 3.1], which asserts that $\mathcal{X}(\mathbb{Z}_p)_{S,n} = \mathcal{X}(\mathbb{Z}_S)$ for $n \gg 0$. This has been verified in several small cases:

- when $S = \emptyset$ and $p \leq 10^5$, $n = 2$ suffices [Bal+18, §6];
- when $S = \{2\}$ and $3 \leq p \leq 29$, $n = 4$ suffices [DCW16, §8];
- when $S = \{3\}$ and $p \in \{5, 7\}$, $n = 4$ suffices [CDC20, Theorem 1.3].

It is natural in this context to formulate a refined version[2] of Kim's Conjecture: that

$$\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,n} = \mathcal{X}(\mathbb{Z}_S)$$

for $n \gg 0$. Our results provide strong evidence in favour of this refined conjecture in the case $|S| \leq 2$.

In the case $S = \{\ell\}$, we have that $\mathcal{X}(\mathbb{Z}_S) = \{2, -1, \frac{1}{2}\}$ if $\ell = 2$, and $\mathcal{X}(\mathbb{Z}_S) = \emptyset$ if ℓ is odd. Using Theorem A, we have verified computationally that $\mathcal{X}(\mathbb{Z}_p)^{\min}_{\{\ell\},2} = \{2, -1, \frac{1}{2}\}$ for all odd primes $p \leq 1000$ (for any $\ell \neq p$). So we have verified our refined version of Kim's Conjecture in the case $S = \{2\}$, $n = 2$ and $3 \leq p \leq 1000$.

In the case $S = \{\ell, q\}$ for primes $\ell < q$, the set $\mathcal{X}(\mathbb{Z}_S)$ can again be determined by elementary means. It is empty if $\ell \neq 2$, and when $\ell = 2$:

- if q is neither a Mersenne nor a Fermat prime, then $\mathcal{X}(\mathbb{Z}_S) = \{2, -1, \frac{1}{2}\}$ consists of the S_3-orbit of 2;
- if $q \neq 3$ is a Mersenne prime, then $\mathcal{X}(\mathbb{Z}_S)$ consists of the S_3-orbits of 2 and $q + 1$;

[1] Kim's method applies not just to the thrice-punctured line, but more generally to any S-integral model of a hyperbolic curve, and Kim's Conjecture is formulated for all such $\mathcal{X}$.

[2] The logical relation between these two conjectures is that Kim's Conjecture implies our refined version, but not conversely.

- if $q \neq 3$ is a Fermat prime, then $\mathcal{X}(\mathbb{Z}_S)$ consists of the S_3-orbits of 2 and q; and
- if $q = 3$, then $\mathcal{X}(\mathbb{Z}_S)$ consists of the S_3-orbits of 2, 3, 4 and 9.

Regarding the refined Chabauty–Kim loci $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ on the other hand, we can deduce the following from Theorem B.

Proposition (Proposition 3.12)**.** *Let $S = \{\ell, q\}$ be two primes different from 3, and let $p = 3$. Then the refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_3)^{\min}_{S,2}$ contains $\{2, -1, \frac{1}{2}\}$ and at most one more S_3-orbit of points. The second orbit is present if and only if*

$$\min\{v_3(a_{\ell,q}), v_3(a_{q,\ell})\} = v_3(\log(\ell)) + v_3(\log(q))\,. \tag{$\dagger$}$$

In particular, we have verified our refined version of Kim's Conjecture for $S = \{2, q\}$, $n = 2$ and $p = 3$ whenever $q \geq 5$ is either a Mersenne or Fermat prime. Additionally, we have also verified the conjecture for $S = \{2, q\}$, $n = 2$ and $p = 3$ in the cases $q = 19, 37, 53$, by showing that the criterion (†) fails for these values of q. This uses the code in [KLS21].

Let us now say a few words about the refined Chabauty–Kim method. The usual Chabauty–Kim method, which in fact applies to a general hyperbolic curve $\mathcal{X}$, revolves around the study of two objects: the *global Selmer scheme* $\mathrm{Sel}_{S,n}$ and the *local Selmer scheme* $H^1_f(G_p, U_n^{\text{ét}})$, both defined in terms of the $\mathbb{Q}_p$-pro-unipotent étale fundamental group truncated in depth n. These are both affine schemes of finite type over $\mathbb{Q}_p$, and when the inequality

$$\dim \mathrm{Sel}_{S,n} < \dim H^1_f(G_p, U_n^{\text{ét}})$$

holds, then the Chabauty–Kim locus $\mathcal{X}(\mathbb{Z}_p)_{S,n}$ is finite. Moreover, given a sufficiently explicit description of the local and global Selmer schemes, one can write down defining equations for the Chabauty–Kim locus $\mathcal{X}(\mathbb{Z}_p)_{S,n}$, in the form of Coleman analytic functions on $\mathcal{X}(\mathbb{Z}_p)$ which vanish on $\mathcal{X}(\mathbb{Z}_p)_{S,n}$.

This theory was studied in detail in the case of $\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0, 1, \infty\}$ and $n = 2$ in work of Dan-Cohen and Wewers [DCW15]. There, they showed that $\dim H^1_f(G_p, U_2^{\text{ét}}) = 3$, while $\dim \mathrm{Sel}_{S,2} = 2|S|$. So the usual Chabauty–Kim method applies for this $\mathcal{X}$ whenever $|S| \leq 1$, and in the case $|S| = 1$, Dan-Cohen and Wewers found that the Chabauty–Kim locus $\mathcal{X}(\mathbb{Z}_p)_{S,2}$ is cut out by the equation

$$2\,\mathrm{Li}_2(z) = \log(z)\log(1-z)$$

(independent of S) [DCW15, §12].

The refined Chabauty–Kim method of [BD19] replaces the global Selmer scheme by a *refined global Selmer scheme* $\mathrm{Sel}^{\min}_{S,n}$ which is a closed subscheme of $\mathrm{Sel}_{S,n}$, and when the inequality

$$\dim \mathrm{Sel}^{\min}_{S,n} < \dim H^1_f(G_p, U_n^{\text{ét}})$$

holds, then the refined Chabauty–Kim locus $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,n}$ is finite. In the particular case that $\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0, 1, \infty\}$ and $n = 2$, we have $\dim \mathrm{Sel}^{\min}_{S,2} = |S|$,

so the refined Chabauty–Kim method applies now whenever $|S| \leq 2$. Moreover, using the explicit descriptions from [DCW15], we can obtain explicit descriptions of the refined Chabauty–Kim loci, as in our Theorems A and B. Notably, refined Chabauty–Kim allows us to deal with the case $|S| = 2$ already in depth $n = 2$. And even in the case $|S| = 1$, refined Chabauty–Kim provides more stringent constraints than usual Chabauty–Kim: the refined locus $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ for $|S| = 1$ is, up to the S_3-action, cut out by the two equations

$$\log(z) = \mathrm{Li}_2(z) = 0$$

(the equation $\log(z) = 0$ just says that z is a $(p-1)$st root of unity). The fact that we get two defining equations rather than one is significant in the context of Kim's conjecture: a generic pair of Coleman functions on a curve have no common zeroes, so heuristically one would expect any common zero of $\log(z)$ and $\mathrm{Li}_2(z)$ to be there for a reason. More specifically, it seems reasonable to conjecture that the only solution to $\log(z) = \mathrm{Li}_2(z) = 0$ in $\mathcal{X}(\mathbb{Z}_p)$ is $z = -1$: this would imply the refined version of Kim's Conjecture for $S = \{2\}$ and $n = 2$.

Acknowledgements. This project was started during the 2020 Arizona Winter School as part of a project group guided by Minhyong Kim and the second author. The authors would like to thank Minhyong for his support and guidance throughout the different stages of this project, as well as the organizers of the Arizona Winter School for making this collaboration possible in the first place.

1. The S-Unit Equation and Classification of Solutions

Before we begin the paper proper, let us recall a few elementary facts about S-integral points on the thrice-punctured line

$$\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0, 1, \infty\} = \mathrm{Spec}\left(\mathbb{Z}_S[u^{\pm 1}, v^{\pm 1}]/(1-u-v)\right) .$$

S-integral points on $\mathcal{X}$ are the same thing as solutions to the *S-unit equation*, i.e. they are elements $u \in \mathbb{Z}_S^\times$ such that $1 - u \in \mathbb{Z}_S^\times$ also. Equivalently, S-integral points on $\mathcal{X}$ correspond to solutions (a, b, c) of the equation

$$a + b = c \tag{1.1}$$

with $a, b, c \in \mathbb{Z}$ coprime and divisible only by primes in S (up to identifying $(a, b, c) \sim (-a, -b, -c)$).

The solutions to the S-unit equation can be determined by elementary means when $|S| \leq 2$.

Assume firstly that $S = \{\ell\}$. Then in any solution to (1.1), one of a, b, c must be $\pm\ell^n$ for some $n \geq 0$, and the other two must be ± 1. Thus, if ℓ is odd, there are no solutions for parity reasons, while if $\ell = 2$ then the only solution, up to signed permutation of a, b, c, is $1 + 1 = 2$. This says that $\mathcal{X}(\mathbb{Z}_S) = \emptyset$ if $S = \{\ell\}$ with ℓ odd, and is $\{2, -1, \frac{1}{2}\}$ if $S = \{2\}$.

Now assume instead that $S = \{\ell, q\}$ for $\ell < q$. Then there are two possibilities for solutions to (1.1): either one of a, b, c is $\pm\ell^n q^m$ and the other two are ± 1, or one is $\pm\ell^n$, another is $\pm q^m$, and the third is ± 1. In the first case, the only possible solution, up to signed permutation of a, b, c, is $1 + 1 = 2$ in the case $\ell = 2$. In the second case, up to signed permutation we are looking for solutions to

$$q^m = \ell^n \pm 1$$

with $n, m > 0$. Again, this equation has no solutions for parity reasons unless $\ell = 2$. And when $\ell = 2$, the solutions can be classified as follows:

(i) Fermat prime solutions: $q = 2^n + 1$;
(ii) Mersenne prime solutions: $q = 2^n - 1$;
(iii) Catalan solutions: $q^m = 2^n \pm 1$ with $m \geq 2$.

As the terminology suggests, Fermat and Mersenne prime solutions exist only when q is a Fermat or Mersenne prime, respectively. Moreover, by the Catalan Conjecture (proved by Mihăilescu), the only possible Catalan solution is $9 = 8 + 1$ in the case $q = 3$. This special case of the Catalan Conjecture can also be proved directly:

Proposition 1.1. *Let q be an odd prime. If $q \neq 3$, then the equations*

$$q^m = 2^n \pm 1$$

have no solutions with $m \geq 2$. For $q = 3$, the only solution with $m \geq 2$ is $3^2 = 2^3 + 1$.

Proof. Assume that (m, n) is a solution of the equation

$$q^m = 2^n + 1.$$

with $m \geq 2$. Then we have

$$2^n = q^m - 1 = (q - 1)(q^{m-1} + \ldots + q + 1),$$

so the second factor must be a power of two, in particular even since $m \geq 2$. We get another factorization

$$2^n = q^m - 1 = (q^{m/2} - 1)(q^{m/2} + 1).$$

The two factors are powers of two which differ by two, hence they are equal to 2 and 4. It follows that $q = 3$, $m = 2$ and $n = 3$, i.e. the solution is $3^2 = 2^3 + 1$.

For the second case, assume that (m, n) is a solution of the equation

$$q^m = 2^n - 1.$$

Observe that $n \geq 2$ since $m \geq 2$. Reducing modulo 4, we get

$$q^m \equiv -1 \bmod 4,$$

hence m is odd. We have

$$q^m \equiv -1 \bmod 2^n,$$

so that q^m has multiplicative order 2 modulo 2^n. Since $(\mathbb{Z}/2^n\mathbb{Z})^\times$ has order 2^{n-1}, raising to the m-th power is an automorphism of that group, hence q

itself has multiplicative order 2. Then $2^n = q^m + 1$ divides $q^2 - 1$, which is impossible since $m \geq 2$. □

Thus we have seen that when $S = \{\ell, q\}$ with $\ell < q$, then $\mathcal{X}(\mathbb{Z}_S)$ is empty unless $\ell = 2$. And when $\ell = 2$, $\mathcal{X}(\mathbb{Z}_S)$ consists of $\{2, -1, \frac{1}{2}\}$, plus the S_3-orbit of q when q is Fermat, the S_3-orbit of $q+1$ when q is Mersenne, and the S_3-orbit of 9 when $q = 3$. The case $q = 3$ is particularly special, since it is both Fermat and Mersenne: the full set $\mathcal{X}(\mathbb{Z}_S)$ for $S = \{2, 3\}$ is
$\{2, \frac{1}{2}, -1\} \cup \{3, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, -\frac{1}{2}, -2\} \cup \{4, \frac{1}{4}, \frac{3}{4}, \frac{4}{3}, -\frac{1}{3}, -3\} \cup \{9, \frac{1}{9}, \frac{8}{9}, \frac{9}{8}, -\frac{1}{8}, -8\}$.

2. Refined Selmer Schemes and the S_3-Action

2.1. **The Chabauty–Kim method.** Let S be a finite set of primes. Let $\mathbb{Z}_S$ denote the ring of S-integers, and let $\mathcal{X} \to \mathrm{Spec}(\mathbb{Z}_S)$ be a model of a hyperbolic curve over $\mathbb{Z}_S$ with generic fibre X. Assume for simplicity that $\mathcal{X}$ has good reduction outside S, i.e. is the complement of an étale divisor in a smooth proper curve over $\mathbb{Z}_S$. We choose a place $p \notin S$, a basepoint b, either S-integral or tangential (as introduced by Deligne in [Del89]), and denote by $U^{\text{ét}}$ and U^{dR} the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $(X_{\overline{\mathbb{Q}}}, b)$ and the pro-unipotent de Rham fundamental group of $(X_{\mathbb{Q}_p}, b)$, respectively. The Galois action on $U_n^{\text{ét}}$ factors through the maximal quotient G_T of the absolute Galois group unramified outside T, where T is any finite set of primes containing $S \cup \{p\}$. Let $U_n^{\text{ét}}$ and U_n^{dR} be the nth quotients along the lower central series. Following Kim, we consider the subspace

$$H^1_f(G_p, U_n^{\text{ét}}) \subseteq H^1(G_p, U_n^{\text{ét}})$$

consisting of G_p-equivariant $U_n^{\text{ét}}$-torsors which are crystalline. Such $U_n^{\text{ét}}$-torsors are equivalent, via a Dieudonné functor, to admissible U_n^{dR}-torsors, which are parametrized by the right coset space $F^0\backslash U_n^{\text{dR}}$, see [Kim09]. (Here, $F^0 = F^0 U_n^{\text{dR}}$ refers to the Hodge subgroup of U_n^{dR}.) The resulting isomorphism $H^1_f(G_p, U_n^{\text{ét}}) \cong F^0\backslash U_n^{\text{dR}}$ is a non-abelian analogue of the Bloch–Kato logarithm.[3]

Furthermore, we consider the *global S-Selmer scheme* of $\mathcal{X}$ in depth n as the subspace

$$\mathrm{Sel}_{S,n} = \mathrm{Sel}_{S,n}(\mathcal{X}) \subseteq H^1(G_T, U_n^{\text{ét}}),$$

consisting of $U_n^{\text{ét}}$-torsors that are crystalline at p, and unramified at all places not equal to p outside S, following the definition given in [Kim09][Bal+18][4].

[3]Kim uses the left coset space U_n^{dR}/F^0 rather than the right coset space $F^0\backslash U_n^{\text{dR}}$. The two are equivalent via the inversion map. We prefer the latter, so that $H^1_f(G_p, U_n^{\text{ét}}) \cong F^0\backslash U_n^{\text{dR}}$ specializes to the classical abelian Bloch–Kato logarithm for $n = 1$ (see also Remark A.3).

[4]In the general case ($\mathcal{X}$ not necessarily of good reduction outside S), these two definitions of the Selmer scheme disagree, with the Selmer scheme of [Bal+18] being a closed subscheme of the Selmer scheme of [Kim09]. Since we are mainly interested in the case $\mathcal{X} = \mathbb{P}^1_{\mathbb{Z}_S} \setminus \{0, 1, \infty\}$, both definitions are equivalent for us.

This gives rise to the following diagram, sometimes referred to as Kim's cutter,

$$\begin{array}{ccccc} \mathcal{X}(\mathbb{Z}_S) & \longrightarrow & \mathcal{X}(\mathbb{Z}_p) & & \\ \downarrow{\scriptstyle j_S} & & \downarrow{\scriptstyle j_p} & \searrow^{j_{\mathrm{dR}}} & \\ \mathrm{Sel}_{S,n} & \xrightarrow{\mathrm{loc}_p} & H^1_f(G_p, U_n^{\text{ét}}) & \xrightarrow{\sim} & F^0\backslash U_n^{\mathrm{dR}} \end{array} \tag{2.1}$$

for all n.[5] Here the vertical arrows j_S, j_p, and j_{dR} denote the global, resp. local, resp. de Rham Kummer map, assigning to each S-integral (respectively, p-adic) point its path torsor relative to the fixed base point b in the respective moduli space of torsors.

The Chabauty–Kim method gives a proof that if

$$\dim \mathrm{Sel}_{S,n} < \dim H^1_f(G_p, U_n^{\text{ét}})$$

then the set of S-integral points is finite. More precisely, if we consider algebraic functions vanishing on the image of the Selmer scheme, using the fact that j_{dR} has dense image, they can be pulled back to a non-zero ideal of functions of $\mathcal{X}(\mathbb{Z}_p)$ which vanish on $\mathcal{X}(\mathbb{Z}_S)$. We can define the vanishing loci, which we will refer to as *Chabauty–Kim sets*,

$$\mathcal{X}(\mathbb{Z}_p)_n \coloneqq j_p^{-1}(\mathrm{loc}_p(\mathrm{Sel}_{S,n}(\mathcal{X})))$$

in each level n, yielding a sequence of subsets

$$\mathcal{X}(\mathbb{Z}_p) \supseteq \mathcal{X}(\mathbb{Z}_p)_1 \supseteq \mathcal{X}(\mathbb{Z}_p)_2 \supseteq \ldots \supseteq \mathcal{X}(\mathbb{Z}_S).$$

In fact, Kim conjectured that equality

$$\mathcal{X}(\mathbb{Z}_p)_n = \mathcal{X}(\mathbb{Z}_S)$$

holds for large enough n (cf. [Bal+18, §1.4]).

2.2. **Chabauty–Kim in depth $n \leq 2$ for $\mathcal{X} = \mathbb{P}^1 \setminus \{0,1,\infty\}$.** Now let $\mathcal{X} = \mathbb{P}^1 \setminus \{0,1,\infty\}$ be the minimal regular model of the thrice punctured line. We briefly sketch what is known for the Chabauty–Kim method for $\mathcal{X}$ in depth $n \leq 2$, where all the maps in (2.1) can be made explicit. For the basic facts, we refer to [Kim05] and [DCW15].

2.2.1. *Depth 1.* Note that the geometric fundamental group $\pi_1(X_{\overline{\mathbb{Q}}})$ of X is the free profinite group in two generators a, b (corresponding to loops around $0, 1$). Hence, we have

$$U_1^{\text{ét}} = (U^{\text{ét}})^{\mathrm{ab}} = (\pi_1(X_{\overline{\mathbb{Q}}})^{\mathrm{ab}} \otimes \mathbb{Q}_p) \cong \mathbb{Q}_p(1) \cdot a \oplus \mathbb{Q}_p(1) \cdot b \cong \mathbb{Q}_p(1) \times \mathbb{Q}_p(1).$$

Kummer theory yields an isomorphism

$$\mathrm{Sel}_{S,1} = H^1_f(G_T, \mathbb{Q}_p(1)^2) = H^1_f(G_T, \mathbb{Q}_p(1))^2 \cong \mathbb{A}^S \times \mathbb{A}^S,$$

[5]Strictly speaking, the vertical arrows in the diagram don't make sense, since their domains are sets but their codomains are $\mathbb{Q}_p$-schemes. These arrows in fact indicate maps from a set to the set of $\mathbb{Q}_p$-points of the codomain, but this is customarily omitted from the notation.

where we choose coordinates $(x_\ell)_{\ell\in S}$, $(y_\ell)_{\ell\in S}$ of $\mathbb{A}^S\times\mathbb{A}^S$ in such a way that the global nonabelian Kummer map j_S is given by

$$z\mapsto((v_\ell(z))_{\ell\in S},(v_\ell(1-z))_{\ell\in S}).$$

The de Rham side has an explicit description in depth 1 as well. Similar to the above, Kummer theory allows us to identify the local Selmer scheme with $\mathbb{A}^2$ and j_{dR} is given by

$$z\mapsto(\log(z),\log(1-z))$$

in depth 1. Here we refer to the p-adic logarithm, defined as the Coleman integral

$$\log(z)=\int_{\vec{01}}^{z}\frac{\mathrm{d}x}{x}.$$

This gives a description of the localization map as

$$\begin{aligned}\mathrm{Sel}_{S,1}=\mathbb{A}^S\times\mathbb{A}^S&\to H^1_f(G_T,\mathbb{Q}_p(1)^2)=\mathbb{A}^2\\((x_\ell)_{\ell\in S},(y_\ell)_{\ell\in S})&\mapsto(\sum\log(\ell)x_\ell,\sum\log(\ell)y_\ell),\end{aligned}$$

and hence we have completely described the fundamental Chabauty–Kim diagram in depth 1.

2.2.2. *Depth 2.* For $*=\text{ét},\mathrm{dR}$ there is an exact sequence of algebraic groups over $\mathbb{Q}_p$

$$\begin{array}{ccccccccc}1&\longrightarrow&(U^*)^{[2]}/(U^*)^{[3]}&\longrightarrow&U_2^*&\longrightarrow&U_1^*&\longrightarrow&1\\&&\cong\downarrow&&&&\downarrow\cong&&\\&&\mathbb{Q}_p(2)&&&&\mathbb{Q}_p(1)\times\mathbb{Q}_p(1),&&\end{array}$$

where the Tate twist is to be interpreted in the respective realization. The corresponding sequence on Lie algebras splits [DCW15, §5]. The construction in [DCW15, §5] goes via the theory of motives, but can be described equivalently without using this theory. The Lie algebra of $U_2^{\text{ét}}$ is unramified away from p and crystalline at p, so its extension class lies in $\mathrm{Ext}^1(\mathbb{Q}_p(1)^2,\mathbb{Q}_p(2))=\mathrm{H}^1_f(G_\mathbb{Q},\mathbb{Q}_p(1))^2=0$. Thus the extension of Lie algebras for $U^{\text{ét}}$ has a unique $G_\mathbb{Q}$-equivariant splitting, and applying the D_{dR} functor gives the corresponding splitting for U^{dR}.

Hence, via these splittings one can identify U_2^* with the *Heisenberg group*

$$H^*=\begin{pmatrix}1&\mathbb{Q}_p(1)&\mathbb{Q}_p(2)\\0&1&\mathbb{Q}_p(1)\\0&0&1\end{pmatrix}.$$

As $H^i(G_T,\mathbb{Q}_p(2))=0$ for $i=1,2$ by Soulé vanishing, the abelianization map π induces an isomorphism

$$\pi_*\colon\mathrm{Sel}_{S,2}\xrightarrow{\sim}\mathrm{Sel}_{S,1}=H^1_f(G_T,\mathbb{Q}_p(1)^2).$$

Note that as $\overline{X} = \mathbb{P}^1$ has no nontrivial unipotent vector bundles (see [Had11]), we have $F^0 U_1^{\mathrm{dR}} = \{1\}$ and hence

$$H^1_f(G_p, U_2^{\text{ét}}) \cong U_2^{\mathrm{dR}} = H^{\mathrm{dR}}.$$

Finally, in the identification $U_2^{\mathrm{dR}} \cong \mathbb{A}^3$, the map j_{dR} is given by locally p-adic analytic functions as

$$z \mapsto (\log(z), \log(1-z), -\operatorname{Li}_2(z)).$$

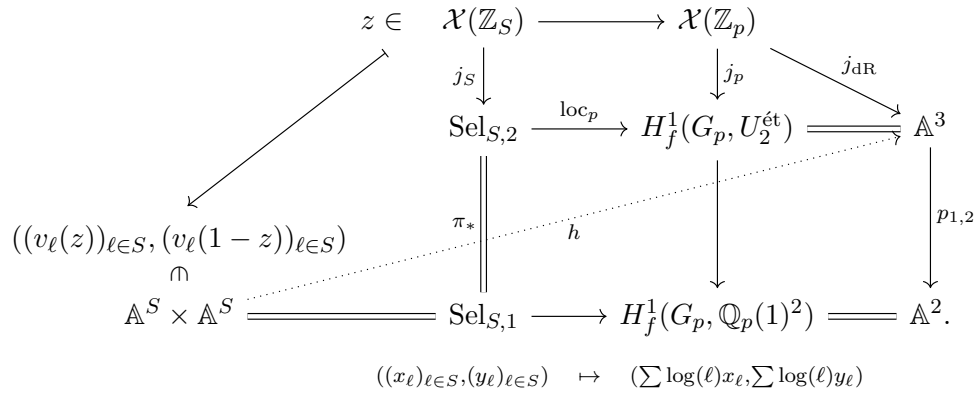
Note that Li_n denotes the p-adic polylogarithm, which is given as an iterated Coleman integral as

$$\operatorname{Li}_n(z) = \int_{\overrightarrow{01}}^{z} \underbrace{\frac{\mathrm{d}x}{x} \cdots \frac{\mathrm{d}x}{x}}_{n-1 \text{ times}} \frac{\mathrm{d}x}{1-x},$$

where we follow Kim's convention that the rightmost integrand is integrated "first". They satisfy several useful identities:

$$\operatorname{Li}_2(z) + \operatorname{Li}_2(1-z) = -\log(z)\log(1-z),$$
$$\operatorname{Li}_2(z) + \operatorname{Li}_2(z^{-1}) = -\frac{1}{2}\log(z)^2.$$

We sum up what is known for the Chabauty–Kim method in depth 2 in the following diagram



2.3. **The localization map in depth 2.**

2.3.1. *Properties.* With above choices of coordinates the localization map

$$h = \mathrm{loc}_p \colon \mathrm{Sel}_{S,2} = \mathbb{A}^S \times \mathbb{A}^S \to U_2^{\mathrm{dR}} = \mathbb{A}^3$$

is of the form

$$((x_\ell)_{\ell\in S}, (y_\ell)_{\ell\in S}) \mapsto \left(\sum_{\ell\in S} \log(\ell) x_\ell, \sum_{\ell\in S} \log(\ell) y_\ell, h_3(x,y) \right).$$

In [DCW15], Dan-Cohen and Wewers study the third term h_3 using mixed Tate motives. They prove that it is bilinear, i.e. of the form

$$h_3 = \sum_{\ell,q\in S} a_{\ell,q} x_\ell y_q.$$

The result of the motivic methods is that all the objects and maps are defined over $\mathbb{Q}$, which is of great advantage in the general theory. For our results we are able to bypass the theory of mixed Tate motives. We provide an elementary proof of the bilinearity of h_3 purely in the language of cocycles in Appendix A.

Given the bilinearity, there are two further pieces of information one needs to fully determine h_3:

(i) For $z \in \mathcal{X}(\mathbb{Z}_S)$ our knowledge of j_{dR} yields

$$h_3((v_\ell(z))_{\ell\in S}, (v_\ell(1-z))_{\ell\in S}) = -\operatorname{Li}_2(z).$$

(ii) The coefficients of this bilinear form satisfy a "twisted antisymmetry relation" ([DCW15, Prop. 10.4])

$$a_{q,\ell} + a_{\ell,q} = \log(\ell)\cdot\log(q).$$

We give a new proof of the second fact in Section 2.5.

Note that when there are sufficiently many global points on $\mathcal{X}$, for instance in the case $S = \{2, q\}$, where q is a Mersenne or Fermat prime, one can directly compute the coefficients by evaluating at these known points and using (i). We do this in Section 3.5. In any other case with $|S| = 2$, this cannot be done. However, this bilinear form is independent of S in a certain sense and in fact comes from a linear form on the infinite dimensional vector space with basis given by pairs of all primes. The independence of S is expressed in the following claim.

Lemma 2.1 (cf. [DCW15, p. 10.2])**.** *Let $S \subseteq S'$ be finite sets of primes not containing p. Then the inclusion $\mathrm{Sel}_{S,2} \subseteq \mathrm{Sel}_{S',2}$ corresponds to the subspace inclusion $\mathbb{A}^S \times \mathbb{A}^S \subseteq \mathbb{A}^{S'} \times \mathbb{A}^{S'}$ with $x_{\ell'} = y_{\ell'} = 0$ for $\ell' \in S' \setminus S$, and the localization map loc_p on $\mathrm{Sel}_{S',2}$ restricts to the localization map on $\mathrm{Sel}_{S,2}$. In particular, the bilinear form coefficients $a_{\ell,q}$ of the third component of loc_p are independent of the set $S \supseteq \{\ell, q\}$ with $p \notin S$.*

Proof. Let $T = S \cup \{p\}$ and $T' = S' \cup \{p\}$. Then we have $T \subseteq T'$ and hence a surjection $G_{T'} \twoheadrightarrow G_T$ between the Galois groups of the maximal extensions of $\mathbb{Q}$ which are unramified outside T' and T, respectively. This induces an injective inflation map

$$H^1(G_T, U_2^{\text{ét}}) \hookrightarrow H^1(G_{T'}, U_2^{\text{ét}})$$

which yields an injection $\mathrm{Sel}_{S,2} \subseteq \mathrm{Sel}_{S',2}$ upon restricting to classes which are crystalline at p. The local Galois group G_p at p has injective maps to G_T and $G_{T'}$, compatible with the surjection $G_{T'} \twoheadrightarrow G_T$. This leads to the

commutative diagram

$$\begin{array}{ccccc} \mathrm{Sel}_{S',2} & \hookrightarrow & H^1(G_{T'}, U_2^{\text{ét}}) & \xrightarrow{\mathrm{loc}_p} & H^1(G_p, U_2^{\text{ét}}) \\ \uparrow & & \uparrow & & \| \\ \mathrm{Sel}_{S,2} & \hookrightarrow & H^1(G_T, U_2^{\text{ét}}) & \xrightarrow{\mathrm{loc}_p} & H^1(G_p, U_2^{\text{ét}}), \end{array}$$

which shows that the localization map on $\mathrm{Sel}_{S',2}$ restricts to that on $\mathrm{Sel}_{S,2}$. For the description of the inclusion of Selmer schemes, we may work in depth one where it boils down to the isomorphisms from Kummer theory

$$\begin{array}{ccccc} H^1(G_{T'}, \mathbb{Q}_p(1)) & \xrightarrow{\sim} & \varprojlim_n \mathbb{Z}_{T'}^\times/p^n \otimes \mathbb{Q}_p & \xrightarrow{\sim} & \mathbb{Q}_p^{T'} \\ \uparrow & & \uparrow & & \uparrow \\ H^1(G_T, \mathbb{Q}_p(1)) & \xrightarrow{\sim} & \varprojlim_n \mathbb{Z}_T^\times/p^n \otimes \mathbb{Q}_p & \xrightarrow{\sim} & \mathbb{Q}_p^T. \end{array} \qquad \square$$

2.3.2. *Computing coefficients.* Using this idea, Dan-Cohen and Wewers give an algorithm for computing the coefficients $a_{\ell,q}$ when $\ell, q < p$ (see [DCW15, §11]). We give a brief sketch of a modified version of this which works for any $\ell, q \neq p$.

Fix an odd prime number p. Let

$$E = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}^\times,$$

which is an infinite-dimensional $\mathbb{Q}$-vector space (written additively), and write $[\cdot]\colon \mathbb{Z}_{(p)}^\times \to E$ for the map $t \mapsto [t] = 1 \otimes t$ (which is a multiplicative-to-additive homomorphism). As $K_2(\mathbb{Z}_{(p)}) \otimes \mathbb{Q}$ vanishes[6], the vector space $E \otimes E$ is spanned by vectors of the form $[t] \otimes [1-t]$ with $t, 1-t \in \mathbb{Z}_{(p)}^\times$, which we refer to as *Steinberg elements*.

Given two prime numbers ℓ, q different from p, we wish to compute a decomposition of $[\ell] \otimes [q]$ as a sum of Steinberg elements and symmetric elements, i.e. generators of the form $[u] \otimes [v] + [v] \otimes [u]$ for $u, v \in \mathbb{Z}_{(p)}^\times$. Hence, we want a decomposition of the form

$$[\ell] \otimes [q] = \sum_i \lambda_i \cdot ([u_i] \otimes [v_i] + [v_i] \otimes [u_i]) + \sum_j \mu_j \cdot [t_j] \otimes [1 - t_j]$$

for some elements $u_i, v_i, t_j \in \mathbb{Z}_{(p)}^\times$ with $1 - t_j \in \mathbb{Z}_{(p)}^\times$ and rational coefficients λ_i, μ_j.

[6]This follows from the vanishing of $K_2(\mathbb{Q}) \otimes \mathbb{Q}$ and the existence of the short exact sequence

$$0 \to K_2(\mathbb{Z}_{(p)}) \to K_2(\mathbb{Q}) \to \bigoplus_{q \neq p} \kappa(q)^\times \to 0.$$

See §11 of [Mil71].

To simplify the expressions, we do this computation in $\bigwedge^2 E$, i.e. first consider a decomposition

$$[\ell] \wedge [q] = \sum_i \lambda_i [t_i] \wedge [1 - t_i]. \tag{2.2}$$

This then yields a decomposition in the tensor-square $E \otimes E$ of the desired form, namely

$$[\ell] \otimes [q] = \frac{1}{2}([\ell] \otimes [q] + [q] \otimes [\ell]) + \frac{1}{2} \sum_i \lambda_i \Big([t_i] \otimes [1 - t_i] - [1 - t_i] \otimes [t_i] \Big).$$

Finally, this yields coefficients of the third component of the localization map, namely

$$a_{\ell,q} = \frac{1}{2} \log(\ell) \log(q) + \frac{1}{2} \sum_i \lambda_i (\mathrm{Li}_2(1 - t_i) - \mathrm{Li}_2(t_i)) \tag{2.3}$$

Remark 2.2 (Differences from [DCW15]). Note that in [DCW15] the authors consider the vector space

$$E = \mathbb{Q} \otimes \mathbb{Q}^\times = \varinjlim_S \mathbb{Q}^S,$$

which is the $\mathbb{Q}$-vector space spanned by all primes, including p, and give an algorithm for a decomposition of $\ell \otimes q$ in $E \otimes E$. If $p > \ell, q$, this yields a description of the coefficient $a_{\ell,q}$ (in our notation). This restriction on p is necessary because the algorithm may otherwise produce values that are divisible by p. This causes a technical problem with the definition of the p-adic (poly)logarithm. It also causes a conceptual problem: If we enlarge the set S by the prime p we no longer have the fundamental Chabauty–Kim diagram (2.1).

Our decomposition on the other hand allows us to specialize to an arbitrary odd prime p as we avoid numbers containing factors of p.

We now describe how to construct a decomposition (2.2) of $[\ell] \wedge [q]$ as a rational linear combination of Steinberg elements $[t] \wedge [1 - t]$ with $t, 1 - t \in \mathbb{Z}_{(p)}^\times$. We may assume that $\ell < q$. We proceed by induction on (q, ℓ), ordered lexicographically. More precisely, we show that $[\ell] \wedge [q]$ can be expressed as a $\mathbb{Q}$-linear combination of Steinberg elements, terms of the form $[\ell'] \wedge [q']$ with $q' < q$, and in the case $\ell > 2$ the particular element $[2] \wedge [q]$. Our algorithm is based on the following observation:

Lemma 2.3. *Let Σ denote the finite set of integers z of absolute value $< q$, together with the even integers z of absolute value $< 2q$. Then for all $z_0 \in \Sigma$, there is a $z_1 \in \Sigma$ such that $q \mid \ell z_0 - z_1$ and neither z_1 nor $r_1 = \frac{\ell z_0 - z_1}{q}$ is divisible by p.*

Proof. There are three values $z_1 \in \Sigma$ such that $q \mid \ell z_0 - z_1$, and these form an arithmetic progression of common difference q. The corresponding values

of r_1 form an arithmetic progression of common difference -1. It follows that at least one of these values has both z_1 and r_1 not divisible by p. $\square$

We use the lemma to find sequences $1 = z_0, z_1, \dots$ and $r_1, r_2, \dots$ of integers, all prime to p, such that $|z_i| < q$ and

$$qr_i = \ell z_{i-1} - z_i \quad \text{or} \quad qr_i = \ell z_{i-1} - 2z_i$$

for all i. (In the case $\ell = 2$ we require $qr_i = \ell z_{i-1} - z_i$ but allow $|z_i| < 2q$ rather than $|z_i| < q$.) Every z_i and every r_i have no prime factor $\geq q$, the latter since $|r_i| \leq \frac{1}{q}\left((q-1)^2 + 2(q-1)\right) < q$.

From this point, we argue as in [DCW15]. Define elements $f_i \in \bigwedge^2 E$ for $i \geq 1$ by

$$f_i \coloneqq [\ell] \wedge [q] + [z_{i-1}] \wedge [q] - [z_i] \wedge [q]\,.$$

Since Σ is finite, there must be indices $m < n$ such that $z_m = \pm z_n$, and hence

$$[\ell] \wedge [q] = \frac{1}{n-m} \cdot \sum_{i=m+1}^{n} f_i\,.$$

We have the identity

$$f_i = \left[\frac{z_i}{\ell z_{i-1}}\right] \wedge \left[\frac{r_i}{\ell z_{i-1}}\right] - \left[\frac{z_i}{\ell z_{i-1}}\right] \wedge \left[1 - \frac{z_i}{\ell z_{i-1}}\right] \quad \text{or} \tag{2.4}$$

$$f_i = \left[\frac{2z_i}{\ell z_{i-1}}\right] \wedge \left[\frac{r_i}{\ell z_{i-1}}\right] - \left[\frac{2z_i}{\ell z_{i-1}}\right] \wedge \left[1 - \frac{2z_i}{\ell z_{i-1}}\right] + [2] \wedge [q]\,, \tag{2.5}$$

according as $\ell z_{i-1} - qr_i$ is equal to z_i or $2z_i$. In any case, f_i can be expressed as a linear combination of smaller basis elements, Steinberg elements, and the particular element $[2] \wedge [q]$. The element $[2] \wedge [q]$ appears only if $\ell \neq 2$ by construction, so that it can be expressed inductively in terms of Steinberg elements.

An implementation of this algorithm in SageMath is provided in [KLS21].

Remark 2.4. This algorithm does not give us any control over the length of the resulting decompositions of prime generators $[\ell] \wedge [q]$ in $\bigwedge^2 E$. However, using some linear algebra, one can easily get a bound on the length of decompositions:

Given a bound b, we consider the subspace V_b of $\bigwedge^2 E$ generated by pairs of primes $[\ell] \wedge [q]$ with $\ell < q < b$ such that $\ell, q \neq p$. This vector space V_b also admits a basis of Steinberg elements $[t] \wedge [1-t]$ where $t, 1-t$ are integers containing only prime factors $< b$. Given such a Steinberg basis, each $[\ell] \wedge [q]$ with $\ell < q < b$ can expressed in terms of this Steinberg basis. Our implementation in Sage essentially uses the above algorithm to produce such a Steinberg basis.

2.3.3. *Examples.* We give some examples of coefficients $a_{\ell,q}$ for primes ℓ, q different from a given odd prime p, as well as the corresponding decomposition of $[\ell] \wedge [q]$ in $\bigwedge^2 E$ where $E = \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}^{\times}$.

Note that if $\ell = 2$ and q is a prime of the form $q = 2^n \pm 1$, i.e. a Mersenne or Fermat prime, we have

$$[2] \wedge [q] = \frac{1}{n} \cdot ([1 \mp q] \wedge [\pm q]),$$

yielding the coefficient

$$a_{2,q} = -\frac{1}{n} \cdot \mathrm{Li}_2(1 \mp q).$$

Remark 2.5. This can also be achieved by using the commutativity of the Chabauty–Kim diagram for the points $z = 1 \mp q = \mp 2^n$ and $z = \pm q$. Identifying $\mathrm{Sel}_{S,2} \cong \mathbb{A}^2 \times \mathbb{A}^2$ via the coordinates (x_2, x_q, y_2, y_q), we have

$$\begin{aligned} j_S(1 \mp q) &= (n, 0, 0, 1), \\ j_S(\pm q) &= (0, 1, n, 0). \end{aligned}$$

By looking at the third component of the localization map loc_p, we find

$$\begin{aligned} -\mathrm{Li}_2(1 \mp q) &= a_{2,q} \cdot n, \\ -\mathrm{Li}_2(\pm q) &= a_{q,2} \cdot n, \end{aligned}$$

so the coefficients are computed as

$$\begin{aligned} a_{2,q} &= -\frac{1}{n} \cdot \mathrm{Li}_2(1 \mp q), \\ a_{q,2} &= -\frac{1}{n} \cdot \mathrm{Li}_2(\pm q). \end{aligned}$$

We give some further examples using the algorithm described above (still fixing $p = 3$):

- Let $\{\ell, q\} = \{2, 11\}$. The algorithm yields

$$[2] \wedge [11] = -\frac{1}{5} \cdot \left[\frac{5}{16}\right] \wedge \left[\frac{11}{16}\right] + \frac{2}{5} \cdot [-4] \wedge [5] + \frac{1}{5} \cdot [-10] \wedge [11].$$

  This determines the coefficient $a_{2,11}$ as

$$\begin{aligned} a_{2,11} = &\frac{1}{2} \cdot \log(2) \log(11) - \frac{1}{10} \cdot \Big(-\mathrm{Li}_2\left(\frac{11}{16}\right) + \mathrm{Li}_2\left(\frac{5}{16}\right) \\ &+2 \cdot (\mathrm{Li}_2(5) - \mathrm{Li}_2(-4)) + \mathrm{Li}_2(11) - \mathrm{Li}_2(-10) \Big). \end{aligned}$$

- Let $\{\ell, q\} = \{2, 13\}$. The algorithm yields

$$\begin{aligned} [2] \wedge [13] = &\frac{1}{6} \cdot [-4] \wedge [5] + \frac{1}{6} \cdot \left[-\frac{5}{2}\right] \wedge \left[\frac{7}{2}\right] - \frac{1}{6} \cdot \left[-\frac{5}{8}\right] \wedge \left[\frac{13}{8}\right] \\ &-\frac{1}{6} \cdot \left[\frac{1}{14}\right] \wedge \left[\frac{13}{14}\right] - \frac{1}{6} \cdot \left[\frac{1}{8}\right] \wedge \left[\frac{7}{8}\right] - \frac{1}{6} \cdot \left[\frac{7}{20}\right] \wedge \left[\frac{13}{20}\right], \end{aligned}$$

determining the coefficient $a_{2,13}$ as

$$\begin{aligned} a_{2,13} =& \frac{1}{2}\cdot\log(2)\log(13)+\frac{1}{12}\cdot\Big(\operatorname{Li}_2(5)-\operatorname{Li}_2(-4)\\ &-\operatorname{Li}_2\left(\frac{7}{2}\right)+\operatorname{Li}_2\left(-\frac{5}{2}\right)-\operatorname{Li}_2\left(\frac{13}{8}\right)+\operatorname{Li}_2\left(-\frac{5}{8}\right)\\ &-\operatorname{Li}_2\left(\frac{13}{14}\right)+\operatorname{Li}_2\left(\frac{1}{14}\right)-\operatorname{Li}_2\left(\frac{1}{8}\right)+\operatorname{Li}_2\left(-\frac{7}{8}\right)\\ &-\operatorname{Li}_2\left(\frac{13}{20}\right)+\operatorname{Li}_2\left(\frac{7}{20}\right)\Big)\Big). \end{aligned}$$

- Let $\{\ell,q\}=\{5,7\}$. The algorithm yields

$$[5]\wedge[7]=-\frac{1}{2}\cdot[-4]\wedge[5]-\left[-\frac{5}{2}\right]\wedge\left[\frac{7}{2}\right]-\frac{1}{3}\cdot\left[-\frac{1}{8}\right]\wedge\left[\frac{7}{8}\right],$$

determining the coefficient $a_{5,7}$ as

$$\begin{aligned} a_{5,7} =& \frac{1}{2}\cdot\log(5)\log(7)-\frac{1}{4}\cdot\left(\operatorname{Li}_2(5)-\operatorname{Li}_2(-4)\right)\\ &-\frac{1}{2}\cdot\left(-\operatorname{Li}_2\left(\frac{7}{2}\right)-\operatorname{Li}_2\left(\frac{5}{2}\right)\right)-\frac{1}{6}\cdot\left(-\operatorname{Li}_2\left(\frac{7}{8}\right)-\operatorname{Li}_2\left(\frac{1}{8}\right)\right). \end{aligned}$$

2.4. **Refined Selmer Schemes.** For $|S|\geq 2$ we see $2|S|=\dim \mathrm{Sel}_{S,2} > \dim U_2^{\mathrm{dR}}=3$. Hence in this case, we cannot directly apply the Chabauty–Kim method, as it is possible that the image of the map loc_p is dense. The following lemma resolves this by showing that the S-integral points in fact land in certain $|S|$-dimensional subspaces of $\mathrm{Sel}_{S,2}$.

Lemma 2.6. *Let $p_i(x,y)$ for $i\in\{/,|,-\}$ denote the condition on $\mathbb{A}^2$ that*

$$\begin{cases} x=y, & \text{if } i=/,\\ x=0, & \text{if } i=|,\\ 0=y, & \text{if } i=-. \end{cases}$$

Then the image of j_S is contained within the union of $3^{|S|}$ linear subspaces

$$\mathrm{Sel}_{S,2}^{\Sigma}=\{((x_\ell)_{\ell\in S},(y_\ell)_{\ell\in S}) : p_{i_\ell}(x_\ell,y_\ell),\ell\in S\}\subseteq \mathbb{A}^S\times\mathbb{A}^S$$

for the $3^{|S|}$ choices of tuples of conditions

$$\Sigma=(i_\ell)_{\ell\in S}\in\{/,|,-\}^S.$$

Each of these subspaces is $|S|$-dimensional.

Proof. We want to prove that for every $\ell\in S$ and every $z\in X(\mathbb{Z}_S)$ we have $v_\ell(z)=0$ or $v_\ell(1-z)=0$ or $v_\ell(z)=v_\ell(1-z)$. The equation

$$z+(1-z)=1$$

gives

$$\min\{v_\ell(z),v_\ell(1-z)\}\leq 0$$

with a strict inequality only if $v_\ell(z) = v_\ell(1-z)$, hence we either have $v_\ell(z) = v_\ell(1-z)$, or that one valuation is larger than the other and the other valuation is zero. □

Remark 2.7. These conditions can be viewed as prescribing for each prime $\ell \in S$ which ray of the tropicalization of $\mathcal{X}$ the tropicalization of the point lies on.

Definition 2.8. Let $\Sigma = (i_\ell)_{\ell \in S} \in \{/, |, -\}^S$ be a choice of refinement conditions for each $\ell \in S$. Denote by $\mathcal{I}^\Sigma_{S,2}$ the ideal defining the image of the refined Selmer scheme $\mathrm{Sel}^\Sigma_{S,2}$ in U_2^{dR} under loc_p. Define

$$\mathcal{X}(\mathbb{Z}_p)^\Sigma_{S,2} \subseteq \mathcal{X}(\mathbb{Z}_p)$$

as the vanishing locus of $j^*_{\mathrm{dR}}(\mathcal{I}^\Sigma_{S,2})$. Taking the union over all refined Selmer conditions, we moreover define

$$\mathrm{Sel}^{\min}_{S,2} = \bigcup_\Sigma \mathrm{Sel}^\Sigma_{S,2},$$
$$\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2} = \bigcup_\Sigma \mathcal{X}(\mathbb{Z}_p)^\Sigma_{S,2}.$$

We refer to these subspaces $\mathrm{Sel}^{\min}_{S,2}$ as *refined Selmer schemes*. This notion is due to Betts and Dogra. In [BD19] a refined Selmer scheme in depth n is defined as a subscheme $\mathrm{Sel}^{\min}_{S,n}(\mathcal{X}) \subseteq H^1(G_{\mathbb{Q}}, U_n)$ consisting of cohomology classes that are everywhere locally geometric.[7] In particular, this object is a subscheme of the usual Selmer scheme $\mathrm{Sel}_{S,n}(\mathcal{X})$ containing the image of the global non-abelian Kummer map j_S. Using Lemma 2.6, one can easily see that what we defined above agrees with their definition for $n = 2$.

We have inclusions

$$\mathcal{X}(\mathbb{Z}_S) \subseteq \mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2} \subseteq \mathcal{X}(\mathbb{Z}_p)_{S,2}.$$

Thus to study the S-integral points we are reduced to analysing the sets $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ when S has size ≤ 2.

2.5. **The S_3-action.** There is a natural action of S_3 on the thrice-punctured line. It is given by the rational functions

$$z,\ 1-z,\ \frac{1}{z},\ \frac{z-1}{z},\ \frac{z}{z-1},\ \frac{1}{1-z},$$

which form the permutation group of $\{0, 1, \infty\}$. When we speak of the group S_3 we will always refer to this permutation group (as opposed to the permutation group on $\{1, 2, 3\}$). In Theorem B.1 of Appendix B (by L.A. Betts and M. Lüdtke) we show that the Chabauty–Kim diagram is functorial in $\mathcal{X}$, so that we get an induced S_3-action on the diagram. This means that we have natural S_3-actions on $\mathrm{Sel}_{S,n}$, on $H^1_f(G_p, U_n^{\text{ét}})$, and on

[7] More precisely, this means that $\xi_i|_{G_{\mathbb{Q}_\ell}} \in j_\ell(\mathcal{X}(\mathbb{Z}_\ell))^{\mathrm{Zar}}$ for all $\ell \notin S$ and $\xi_i|_{G_{\mathbb{Q}_\ell}} \in j_\ell(X(\mathbb{Q}_\ell))^{\mathrm{Zar}}$ for all $\ell \in S$.

U_n^{dR} such that the Kummer maps j_S, j_p, j_{dR} as well as the localization map loc_p and the non-abelian Bloch–Kato logarithm $\log_{\mathrm{BK}}$ are S_3-equivariant. The S_3-equivariance of the localization map in depth 2 is in fact equivalent to the twisted antisymmetry relation mentioned in Section 2.2.2, thus giving an alternative proof of this result (see Proposition 2.14 below). Exploiting the S_3-action also gives an advantage in determining S-integral points, as it allows us to reduce the number of refinement conditions to consider.

We want to describe the S_3-actions on the objects of the Chabauty–Kim diagram in depth 2 explicitly in coordinates. The S_3-action on $\mathbb{P}^1 \setminus \{0,1,\infty\}$ is generated by the two involutions σ and τ given by

$$\sigma(z) = 1 - z, \qquad \tau(z) = \frac{1}{z}.$$

Therefore it suffices to give formulas for these two involutions. Also, it suffices to work with $\mathbb{Q}_p$-points rather than points valued in general $\mathbb{Q}_p$-algebras.

2.5.1. *The Selmer scheme.* Recall that the Selmer scheme $\mathrm{Sel}_{S,2}$ is isomorphic to $\mathbb{A}^S \times \mathbb{A}^S$ with coordinates $(x,y) = ((x_\ell)_{\ell\in S}, (y_\ell)_{\ell\in S})$. In order to obtain formulas for the S_3-action in these coordinates, we first prove a lemma on Galois-invariant paths between certain tangential base points.

Given an automorphism $\rho \in S_3$ of $\mathbb{P}^1_{\mathbb{Z}} \setminus \{0,1,\infty\}$, we can apply ρ to the tangential base point $b = \overrightarrow{01}$ at 0 to obtain a tangential base point $\rho(\overrightarrow{01})$ at $\rho(0)$.

Lemma 2.9. *For all $\rho \in S_3$ there exists a Galois-invariant étale path in depth 2 from $\overrightarrow{01}$ to $\rho(\overrightarrow{01})$.*

Proof. Since the tangential base points $\overrightarrow{01}$ and $\rho(\overrightarrow{01})$ are $\mathbb{Z}$-integral, the torsor $P_2^{\text{ét}}(\overrightarrow{01}, \rho(\overrightarrow{01}))$ is crystalline at p and unramified at all primes $\ell \neq p$. Its class in $H^1(G_{\mathbb{Q}}, U_2^{\text{ét}})$ is therefore contained in the Selmer scheme for the empty set $S = \emptyset$. This is given by

$$\mathrm{Sel}_{\emptyset,2} = \mathbb{A}^{\emptyset} \times \mathbb{A}^{\emptyset} = \{0\},$$

hence the torsor $P_2^{\text{ét}}(\overrightarrow{01}, \rho(\overrightarrow{01}))$ is trivial. This is equivalent to the existence of a Galois-invariant path. □

Given two (possibly tangential) base points b and c of $X = \mathbb{P}^1_{\mathbb{Q}} \setminus \{0,1,\infty\}$, denote by $U_n^{\text{ét}}(b)$ and $U_n^{\text{ét}}(c)$ the étale fundamental groups in depth n at the two respective base points. Given a Galois-invariant étale path $\beta \in P_n^{\text{ét}}(c,b)$ from c to b, the conjugation isomorphism $U_n^{\text{ét}}(b) \cong U_n^{\text{ét}}(c)$ given by $\gamma \mapsto \beta^{-1}\gamma\beta$ is Galois-equivariant. It induces an isomorphism of nonabelian cohomology schemes

$$H^1(G_{\mathbb{Q}}, U_n^{\text{ét}}(b)) \cong H^1(G_{\mathbb{Q}}, U_n^{\text{ét}}(c)) \tag{2.6}$$

which sends a cocycle x to the cocycle $\sigma \mapsto \beta^{-1}x(\sigma)\beta$. Independently of the path β, we have a second isomorphism $t_{b,c}\colon H^1(G_{\mathbb{Q}}, U_n^{\text{ét}}(b)) \cong H^1(G_{\mathbb{Q}}, U_n^{\text{ét}}(c))$ given by twisting by the $(U_n^{\text{ét}}(b), U_n^{\text{ét}}(c))$-path bitorsor $P_n^{\text{ét}}(c,b)$.

Lemma 2.10. *Assume that $\beta \in P_n^{\text{ét}}(c,b)$ is a Galois-invariant path as above. Then the isomorphism* (2.6) *agrees with the isomorphism $t_{b,c}$ given by twisting with the path torsor.*

Proof. The twisting isomorphism $t_{b,c}$ sends a cocycle x to the cocycle $\sigma \mapsto {\beta'}^{-1}x(\sigma)\sigma(\beta')$ for any (not necessarily Galois-invariant) path $\beta' \in P^{\text{ét}}(c,b)$. Choosing $\beta' = \beta$, this agrees with the cocycle description of the isomorphism (2.6). □

Proposition 2.11. *The S_3-action on $\mathrm{Sel}_{S,2}$ is given in the coordinates $x = (x_\ell)_{\ell\in S}$, $y = (y_\ell)_{\ell\in S}$ by*

$$\sigma(x,y) = (y,x),$$
$$\tau(x,y) = (-x, y-x).$$

Proof. We have the isomorphism $\mathrm{Sel}_{S,2} \cong \mathrm{Sel}_{S,1}$ which arises by restriction from the isomorphism

$$H^1(G_T, U_2^{\text{ét}}) \cong H^1(G_T, U_1^{\text{ét}}),$$

where $T \coloneqq S \cup \{p\}$. We may therefore work with the group $U_1^{\text{ét}}$ in depth one. Let $\rho \in S_3$. The action of ρ on $H^1(G_T, U_1^{\text{ét}})$ is given by composing the isomorphism $\rho_*\colon H^1(G_T, U_1^{\text{ét}}(b)) \to H^1(G_T, U_1^{\text{ét}}(\rho(b)))$ induced functorially by the G_T-equivariant isomorphism $\rho_*\colon U_1^{\text{ét}}(b) \to U_1^{\text{ét}}(\rho(b))$ with the isomorphism

$$t_{\rho(b),b}\colon H^1(G_T, U_1^{\text{ét}}(\rho(b))) \to H^1(G_T, U_1^{\text{ét}}(b))$$

given by twisting with the path torsor $P_1^{\text{ét}}(b, \rho(b))$. By Lemma 2.9, there exists a Galois-invariant path $\beta \in P_1^{\text{ét}}(b, \rho(b))$. By Lemma 2.10, $t_{\rho(b),b}$ agrees with the isomorphism induced by the conjugation $\beta^{-1}(-)\beta$ on $U_1^{\text{ét}}$. Hence, the action of ρ on $H^1(G_T, U_1^{\text{ét}})$ is induced by the action $\beta^{-1}\rho_*(-)\beta$ on $U_1^{\text{ét}}$. We are thus reduced to describe the S_3-action on $U_1^{\text{ét}}$.

The embedding

$$\mathbb{P}^1 \setminus \{0, 1, \infty\} \to \mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}}, \quad z \mapsto (z, 1-z)$$

induces an isomorphism

$$U_1^{\text{ét}} \cong \pi_1^{\text{ét},\mathbb{Q}_p}(\mathbb{G}_{\mathrm{m}})^{\mathrm{ab}} \times \pi_1^{\text{ét},\mathbb{Q}_p}(\mathbb{G}_{\mathrm{m}})^{\mathrm{ab}} \cong \mathbb{Q}_p(1) \times \mathbb{Q}_p(1).$$

Kummer theory yields an isomorphism

$$H^1(G_T, \mathbb{Q}_p(1)) \cong \varprojlim \mathbb{Z}_T^\times/p^n \otimes \mathbb{Q}_p \cong \mathbb{Q}_p^T,$$

and the elements which are crystalline at p and unramified at places outside S not equal to p form the subspace $\mathbb{Q}_p^S \subseteq \mathbb{Q}_p^T$ with vanishing p-coordinate. This explains the isomorphism $\mathrm{Sel}_{S,2} = \mathrm{Sel}_{S,1} = \mathbb{A}^S \times \mathbb{A}^S$.

The S_3-action on $\mathbb{P}^1 \setminus \{0,1,\infty\}$ extends to $\mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}}$. This is expressed by a commutative diagram

$$\begin{array}{ccc} \mathbb{P}^1 \setminus \{0,1,\infty\} & \underset{\tau}{\overset{\sigma}{\rightrightarrows}} & \mathbb{P}^1 \setminus \{0,1,\infty\} \\ \downarrow{\scriptstyle (z,1-z)} & & \downarrow{\scriptstyle (z,1-z)} \\ \mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}} & \underset{\tilde{\tau}}{\overset{\tilde{\sigma}}{\rightrightarrows}} & \mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}} \end{array}$$

with maps $\tilde{\sigma}$ and $\tilde{\tau}$ given by

$$\begin{aligned} \tilde{\sigma}(a,b) &= (b,a), \\ \tilde{\tau}(a,b) &= (a^{-1}, -a^{-1}b). \end{aligned}$$

The multiplication map $m\colon \mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}$ induces the addition on $\pi_1^{\text{ét},\mathbb{Q}_p}(\mathbb{G}_{\mathrm{m}}) = \mathbb{Q}_p(1)$. In particular, the multiplication by -1 map, $x \mapsto -x$, which factors as

$$\mathbb{G}_{\mathrm{m}} \overset{(-1,\mathrm{id})}{\longrightarrow} \mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}} \overset{m}{\longrightarrow} \mathbb{G}_{\mathrm{m}},$$

induces the identity on $\pi_1^{\text{ét}}(\mathbb{G}_{\mathrm{m}})$ since the constant map $x \mapsto -1$ induces the trivial homomorphism. This shows that the maps $\tilde{\sigma}$, $\tilde{\tau}$ induce on $\pi_1^{\text{ét}}(\mathbb{G}_{\mathrm{m}} \times \mathbb{G}_{\mathrm{m}}) = \mathbb{Q}_p(1) \times \mathbb{Q}_p(1)$ the automorphisms

$$\begin{aligned} \tilde{\sigma}_*(x,y) &= (y,x), \\ \tilde{\tau}_*(x,y) &= (-x, y-x). \end{aligned}$$

This yields the claimed coordinate description of the S_3-action on $\mathrm{Sel}_{S,2}$. □

2.5.2. *The de Rham side.* We now derive explicit formulas for the S_3-action on U_2^{dR}. Define the two differential forms

$$\alpha = \frac{\mathrm{d}z}{z}, \quad \beta = \frac{\mathrm{d}z}{z-1}.$$

Then the three words of differential forms α, β, $\alpha\beta$ define three coordinate functions

$$u = I_b(\alpha), \quad v = I_b(\beta), \quad w = I_b(\alpha\beta)$$

on U_2^{dR} sending a de Rham loop $\gamma \in U_2^{\mathrm{dR}}$ at b (valued in a $\mathbb{Q}_p$-algebra) to the iterated integral over γ of the respective word of differential forms:

$$\begin{aligned} u(\gamma) &= \int_\gamma \frac{\mathrm{d}z}{z}, \\ v(\gamma) &= \int_\gamma \frac{\mathrm{d}z}{z-1}, \\ w(\gamma) &= \int_\gamma \frac{\mathrm{d}z}{z} \frac{\mathrm{d}z}{z-1}. \end{aligned}$$

(The precise definition of Tannakian iterated integrals is reviewed in Section B.5 in the Appendix B.) The coordinates (u,v,w) define the isomorphism of $\mathbb{Q}_p$-schemes $U_2^{\mathrm{dR}} \cong \mathbb{A}^3$ from [DCW15, §5].

Lemma 2.12. *Let $\rho \in S_3$. Then for each word w in $\{\alpha, \beta\}$ of length 1 or 2, the following iterated Coleman integral vanishes:*

$$\int_{\overrightarrow{01}}^{\rho(\overrightarrow{01})} w = 0.$$

Proof. By Lemma 2.9, there exists a G_p-invariant étale path γ on $\mathbb{P}^1_{\overline{\mathbb{Q}}_p} \setminus \{0, 1, \infty\}$ from $\overrightarrow{01}$ to $\rho(\overrightarrow{01})$ in depth 2. The G_p-invariance of γ is equivalent to the associated map of $\mathbb{Q}_p$-algebras

$$\gamma^\sharp \colon \mathcal{O}(P_2^{\text{ét}}(\overrightarrow{01}, \rho(\overrightarrow{01}))) \to \mathbb{Q}_p$$

being G_p-equivariant. Since $\mathcal{O}(P_2^{\text{ét}}(\overrightarrow{01}, \rho(\overrightarrow{01})))$ is de Rham, applying the de Rham Dieudonné functor D_{dR} and using the comparison isomorphism $D_{\mathrm{dR}}(P_2^{\text{ét}}(\overrightarrow{01}, \rho(\overrightarrow{01}))) \cong P_2^{\mathrm{dR}}(\overrightarrow{01}, \rho(\overrightarrow{01}))$ yields a de Rham path $\gamma_{\mathrm{dR}} \coloneqq D_{\mathrm{dR}}(\gamma)$ corresponding to a homomorphism of $\mathbb{Q}_p$-algebras

$$\gamma_{\mathrm{dR}}^\sharp \colon \mathcal{O}(P_2^{\mathrm{dR}}(\overrightarrow{01}, \rho(\overrightarrow{01}))) \to \mathbb{Q}_p$$

which is Hodge-filtered and compatible with the Frobenii. Thus, γ_{dR} is the unique Frobenius-invariant path from $\overrightarrow{01}$ to $\rho(\overrightarrow{01})$, and it sends the Hodge subspace $F^1\mathcal{O}(P_2^{\mathrm{dR}}(\overrightarrow{01}, \rho(\overrightarrow{01})))$ to zero. By Proposition B.15, if w is a word in $\{\alpha, \beta\}$ of length at least 1, then $I_b(w)$ is contained in F^1. Thus we have

$$\int_{\overrightarrow{01}}^{\rho(\overrightarrow{01})} w \coloneqq \int_{\gamma_{\mathrm{dR}}} w = I_b(w)(\gamma_{\mathrm{dR}}) = \gamma_{\mathrm{dR}}^\sharp(I_b(w)) = 0,$$

as claimed. □

Proposition 2.13. *The S_3-action on U_2^{dR} is given in the coordinates (u, v, w) by*

$$\sigma(u, v, w) = (v, u, uv - w),$$
$$\tau(u, v, w) = (-u, v - u, \frac{1}{2}u^2 - w).$$

Proof. Let $\rho \in S_3$. The action of ρ on $U_2^{\mathrm{dR}} = U_2^{\mathrm{dR}}(b)$ is given by composing the isomorphism $\rho_* \colon U_2^{\mathrm{dR}}(b) \to U_2^{\mathrm{dR}}(\rho(b))$ induced via the functoriality of de Rham fundamental groups with the isomorphism $t_{\rho(b),b} \colon U_2^{\mathrm{dR}}(\rho(b)) \to U_2^{\mathrm{dR}}(b)$ given by twisting with the path torsor $P_2^{\mathrm{dR}}(b, \rho(b))$. Denote this composition also by ρ_*. Since the differential forms α and β have logarithmic poles at the cusps, we can use Proposition B.19 to express ρ_* on U_2^{dR} in the coordinates $(u, v, w) = (I_b(\alpha), I_b(\beta), I_b(\alpha\beta))$. Thus, for $w = \alpha, \beta, \alpha\beta$, we have

$$\rho_*^\sharp(I_b(w)) = \sum_{w = w_1 w_2} I_b(\rho^* w_1)\Big(\int_b^{\rho(b)} \rho^* w_2\Big).$$

By Lemma 2.12, the second integral vanishes for nonempty w_2. So we obtain

$$\rho_*^\sharp(I_b(w)) = I_b(\rho^* w) \quad \text{for } w = \alpha, \beta, \alpha\beta.$$

The pullbacks $\sigma^* w$ are calculated as follows:

$$\begin{aligned}\sigma^*(\alpha) &= \frac{\mathrm{d}(1-z)}{1-z} = \frac{\mathrm{d}z}{z-1} = \beta,\\ \sigma^*(\beta) &= \frac{\mathrm{d}(1-z)}{(1-z)-1} = \frac{\mathrm{d}z}{z} = \alpha,\\ \sigma^*(\alpha\beta) &= \sigma^*(\alpha)\sigma^*(\beta) = \beta\alpha.\end{aligned}$$

Using the shuffle relation

$$I_b(\alpha)I_b(\beta) = I_b(\alpha\beta) + I_b(\beta\alpha),$$

or equivalently $I_b(\beta\alpha) = uv - w$, we find

$$\sigma(u,v,w) = (v,u,uv-w).$$

The pullbacks $\tau^* w$ are calculated as follows:

$$\begin{aligned}\tau^*(\alpha) &= \frac{\mathrm{d}(1/z)}{1/z} = z\Big(-\frac{\mathrm{d}z}{z^2}\Big) = -\frac{\mathrm{d}z}{z} = -\alpha,\\ \tau^*(\beta) &= \frac{\mathrm{d}(1/z)}{(1/z)-1} = \frac{\mathrm{d}z}{z(z-1)} = \frac{\mathrm{d}z}{z-1} - \frac{\mathrm{d}z}{z} = \beta - \alpha,\\ \tau^*(\alpha\beta) &= \tau^*(\alpha)\tau^*(\beta) = -\alpha(\beta-\alpha) = \alpha^2 - \alpha\beta.\end{aligned}$$

Using the shuffle relation $I_b(\alpha)^2 = 2I_b(\alpha^2)$, or equivalently, $I_b(\alpha^2) = \frac{1}{2}u^2$, this implies

$$\tau(u,v,w) = (-u, v-u, \frac{1}{2}u^2 - w),$$

as claimed. □

2.5.3. *The twisted anti-symmetry relation.* As recalled in 2.2.2 above, the localization map $\mathrm{loc}_p : \mathrm{Sel}_{S,2} \to U_2^{\mathrm{dR}}$ with respect to the coordinates $(x,y) = ((x_\ell)_{\ell\in S}, (y_\ell)_{\ell\in S})$ on $\mathrm{Sel}_{S,2}$ and the coordinates u,v,w on U_2^{dR} has the form $h : \mathbb{A}^S \times \mathbb{A}^S \to \mathbb{A}^3$,

$$h(x,y) = \begin{pmatrix} h_1(x,y)\\ h_2(x,y)\\ h_3(x,y)\end{pmatrix} = \begin{pmatrix} \sum_{\ell\in S}\log(\ell)x_\ell\\ \sum_{\ell\in S}\log(\ell)y_\ell\\ \sum_{\ell,q\in S} a_{\ell,q}x_\ell y_q\end{pmatrix} \tag{2.7}$$

for certain coefficients $a_{\ell,q} \in \mathbb{Q}_p$ of the bilinear form in the third component. The difficulty in finding explicit equations for S-integral points of $\mathbb{P}^1 \setminus \{0,1,\infty\}$ lies in determining those coefficients. In [DCW15], Proposition 10.4, the authors show that the coefficients satisfy the "twisted anti-symmetry relation" as discussed above in section 2.3. While they work in the motivic framework, we deduce the same relations in our setting from the S_3-equivariance of the localization map.

Proposition 2.14. *The coefficients $a_{\ell,q}$ of the third component of the localization map* (2.7) *satisfy for all $\ell, q \in S$ the twisted anti-symmetry relation*

$$a_{\ell,q} + a_{q,\ell} = \log(\ell)\log(q).$$

In particular, the "diagonal" coefficients $a_{\ell,\ell}$ for $\ell \in S$ are given by

$$a_{\ell,\ell} = \frac{1}{2}\log(\ell)^2.$$

Proof. Using the coordinate description of the S_3-action on $\mathrm{Sel}_{S,2}$ and U_2^{dR} given in Propositions 2.11 and 2.13, the equivariance of the localization map loc_p with respect to σ reads

$$\begin{pmatrix} h_1(y,x) \\ h_2(y,x) \\ h_3(y,x) \end{pmatrix} = \begin{pmatrix} h_2(x,y) \\ h_1(x,y) \\ h_1(x,y)h_2(x,y) - h_3(x,y) \end{pmatrix}.$$

Comparing third components yields

$$\sum_{\ell,q\in S} a_{\ell,q} y_\ell x_q = \Big(\sum_{\ell\in S}\log(\ell)x_\ell\Big)\Big(\sum_{q\in S}\log(q)y_q\Big) - \sum_{\ell,q\in S} a_{\ell,q}x_\ell y_q,$$

which becomes

$$\sum_{\ell,q\in S} a_{q,\ell} x_\ell y_q = \sum_{\ell,q\in S}\Big(\log(\ell)\log(q) - a_{\ell,q}\Big)x_\ell y_q.$$

Comparing coefficients yields the twisted anti-symmetry relation. □

Remark 2.15. In the proof of Proposition 2.14 we used the equivariance of loc_p only with respect to σ rather than the full S_3-action. It turns out, however, that the equivariance with respect to the second generator τ yields no new information: it gives the same twisted anti-symmetry relations as above.

2.5.4. *The S_3-action on the refined Selmer images.* The S_3-action on $\mathbb{P}^1 \setminus \{0,1,\infty\}$ induces an action on the set $\{|,-,\diagup\}$ of refining Selmer conditions. As we have seen, the generators σ and τ act on $\mathbb{A}^2$ via the linear automorphisms

$$\begin{aligned} \sigma(x,y) &= (y,x), \\ \tau(x,y) &= (-x, y-x), \end{aligned}$$

so their effect on the refined Selmer subspaces $| = \{x=0\}$, $- = \{y=0\}$, $\diagup = \{x=y\}$ is

$$\begin{aligned} \sigma:&\quad | \ \leftrightarrow -, \\ \tau:&\quad - \leftrightarrow \diagup. \end{aligned}$$

For a finite set of primes S, let $\Sigma = (i_\ell)_{\ell\in S} \in \{|,-,\diagup\}^S$ be a choice of refinement conditions for each $\ell \in S$, with associated refined Selmer subscheme $\mathrm{Sel}_{S,2}^{\Sigma}$ and refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_p)_{S,2}^{\Sigma}$. By definition of the S_3-action on the refined Selmer conditions, we have for each $\rho \in S_3$:

$$\rho(\mathrm{Sel}_{S,2}^{\Sigma}) = \mathrm{Sel}_{S,2}^{\rho(\Sigma)}. \tag{2.8}$$

Proposition 2.16. *Let S be a finite set of primes and $p \notin S$ a prime. Then the refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ is S_3-stable. More precisely, let $\Sigma \in \{|, -, /\}^S$ be a set of refining Selmer conditions and let $\rho \in S_3$, then*

$$\rho(\mathcal{X}(\mathbb{Z}_p)^{\Sigma}_{S,2}) = \mathcal{X}(\mathbb{Z}_p)^{\rho(\Sigma)}_{S,2}.$$

Proof. Taking images under loc_p in Equation (2.8) and using the S_3-equivariance yields

$$\rho(\mathrm{loc}_p(\mathrm{Sel}^{\Sigma}_{S,2})) = \mathrm{loc}_p(\mathrm{Sel}^{\rho(\Sigma)}_{S,2}).$$

Taking vanishing ideals gives

$$\rho^*\mathcal{I}^{\Sigma}_{S,2} = \mathcal{I}^{\rho(\Sigma)}_{S,2}.$$

The claim follows by pulling back along the S_3-equivariant map j_{dR} and taking the vanishing locus. □

This enables us to make a nice observation about the (refined) Chabauty–Kim locus.

Corollary 2.17. *Let $\Sigma_1, \dots, \Sigma_r$ be orbit representatives of $\{|, -, /\}^S$ under the S_3-action. The full refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$, and hence the set of S-integral points $\mathcal{X}(\mathbb{Z}_S)$, is covered by the S_3-translates of the Chabauty–Kim sets with refinement conditions $\mathcal{X}(\mathbb{Z}_p)^{\Sigma_1}_{S,2}, \dots, \mathcal{X}(\mathbb{Z}_p)^{\Sigma_r}_{S,2}$.*

Thus, we are able to reduce the number of refined subspaces we need to consider. For S of size one, this reduces the number of subspaces from 3 to 1; for S of size two, the number is reduced from 9 to 2.

3. Explicit Equations

Using the above refinements and simplifications, we are now in a position to compute equations for local refined Selmer images in the case $n \leq 2$ and $|S| \leq 2$.

3.1. **Sets S of size one.** Assume that S consists of a single prime ℓ. Fix a prime $p \neq \ell$. If $\ell = 2$, then we have the 2-integral points $2, -1, \frac{1}{2}$, otherwise there are no ℓ-integral points for parity reasons. Since S_3 acts transitively on the set $\{/, |, -\}$ it suffices to consider a single refined Selmer condition, say $|$. We start by working in depth $n = 1$. We have

$$\mathrm{Sel}_{\{\ell\},1} \cong \mathbb{A}^2$$

with localization map $\mathrm{loc}_p : \mathrm{Sel}_{\{\ell\},1} \to \mathbb{A}^2$ given by

$$\mathrm{loc}_p(x_\ell, y_\ell) = \begin{pmatrix} \log(\ell) x_\ell \\ \log(\ell) y_\ell \end{pmatrix}.$$

Since the image is Zariski dense, the unrefined Chabauty–Kim method does not apply. However, the refined Selmer subspace $\mathrm{Sel}^{|}_{\{\ell\},1} \subseteq \mathrm{Sel}_{\{\ell\},1}$ is one-dimensional, and the localization map restricts as

$$\mathrm{loc}_p(0, y_\ell) = \begin{pmatrix} 0 \\ \log(\ell) y_\ell \end{pmatrix}.$$

In the coordinates u, v, the image is cut out by the equation $u = 0$, which becomes

$$\log(z) = 0$$

after pulling back along j_{dR}. We conclude:

Proposition 3.1. *Let ℓ and $p \neq \ell$ be primes. Then the refined Chabauty–Kim method in depth 1 shows the finiteness of $\mathcal{X}(\mathbb{Z}[1/\ell])$. More precisely, the refined set $\mathcal{X}(\mathbb{Z}_p)^{\min}_{\{\ell\},1}$ up to S_3-orbits consists of the nontrivial $(p-1)$-st roots of unity, independently of ℓ.* □

Remark 3.2. This is precisely the set of ℓ-integral points if and only if $\ell = 2$ and $p = 3$.

Remark 3.3. If S consists only of odd primes, we can take $p = 2$. Since $\mathcal{X}(\mathbb{Z}_2) = \emptyset$ by reducing modulo 2, the inclusion $\mathcal{X}(\mathbb{Z}_S) \hookrightarrow \mathcal{X}(\mathbb{Z}_2)$ trivially shows the non-existence of S-integral points of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. In this sense, the Chabauty–Kim method with $p = 2$ yields the complete set of S-integral points in "depth 0".

Now we go to depth $n = 2$. We have $\mathrm{Sel}_{\{\ell\},2} \cong \mathrm{Sel}_{\{\ell\},1} \cong \mathbb{A}^2$ and the localization map $\mathrm{loc}_p : \mathrm{Sel}_{\{\ell\},2} \to \mathbb{A}^3$ is given by

$$\mathrm{loc}_p(x_\ell, y_\ell) = \begin{pmatrix} \log(\ell) x_\ell \\ \log(\ell) y_\ell \\ \dfrac{1}{2}\log(\ell)^2 x_\ell y_\ell \end{pmatrix}.$$

On the refined Selmer subspace $\mathrm{Sel}^{|}_{\{\ell\},2}$, the localization map restricts as

$$\mathrm{loc}_p(0, y_\ell) = \begin{pmatrix} 0 \\ \log(\ell) y_\ell \\ 0 \end{pmatrix},$$

so that the set $\mathcal{X}(\mathbb{Z}_p)^{|}_{\{\ell\},2}$ is cut out by the two equations

$$\log(z) = 0, \quad \mathrm{Li}_2(z) = 0.$$

This shows:

Proposition 3.4. *Let ℓ and $p \neq \ell, 2$ be primes. The refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_p)^{\min}_{\{\ell\},2}$ in depth 2, up to S_3-orbits, consists of the nontrivial $(p-1)$-st roots of unity $\zeta \in \mathbb{Z}_p$ for which $\mathrm{Li}_2(\zeta) = 0$.* □

Remark 3.5. Work of Besser [Bes02b, Prop. 2.1, 2.2] shows that for any $(p-1)$-st root of unity $\zeta \neq 1$ in $\mathbb{Q}_p$ we have

$$\frac{p^2-1}{p^2}\operatorname{Li}_2(\zeta) \in \mathbb{Z}_p$$

and that this is congruent mod p to

$$(1-\bar{\zeta}^p)^{-1}\operatorname{li}_2(\bar{\zeta})$$

where $\operatorname{li}_2(z)$ is a *finite polylogarithm* function

$$\begin{aligned}\operatorname{li}_n\colon \mathbb{F}_p &\to \mathbb{F}_p\\ z &\mapsto \sum_{k=1}^{p-1}\frac{z^k}{k^n}.\end{aligned}$$

Hence a sufficient condition for $\operatorname{Li}_2(\zeta)$ to be non-zero is that the finite polylogarithm $\operatorname{li}_2(\bar{\zeta})$ is non-zero. Using this one may quickly check if a $(p-1)$-st root of unity $\zeta \in \mathbb{Q}_p$ can possibly have $\operatorname{Li}_2(\zeta) = 0$, and if necessary then compute $\operatorname{Li}_2(\zeta)$ to higher p-adic precision using the work of Besser–de Jeu [BDJ08].

We can use this to verify that the solution set cut out by Prop. 3.4 is just $\{2, -1, \frac{1}{2}\}$ for all odd primes $p \leq 1000$, for instance.

Remark 3.6. Already the unrefined Chabauty–Kim method in depth 2 proves the finiteness of ℓ-integral points of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, since the image of loc_p is a two-dimensional subspace in $\mathbb{A}^3$. As in [DCW15, §12] , the set $\mathcal{X}(\mathbb{Z}_p)_{\{\ell\},2}$ is the vanishing locus of the function

$$2\operatorname{Li}_2(z) - \log(z)\log(1-z),$$

independently of ℓ. If $\ell = 2$, this cuts out precisely the set $\{2, -1, \frac{1}{2}\}$ of 2-integral points for $p = 3, 5, 7$, but for $p = 11$ one gets additionally the S_3-orbit of the point $\frac{1}{2}(1 \pm \sqrt{5})$. The refined Chabauty–Kim method is able to rule out this point already in depth one.

3.2. **Sets S of size two.** Assume now that $|S| = 2$. Then each refined Selmer scheme $\operatorname{Sel}_{S,2}^{i,j}$ has dimension 2, hence the image in $\mathbb{A}^3$ under loc_p is non-dense, so that the corresponding vanishing ideal $\mathcal{I}_{S,2}^{i,j} \neq 0$.

Let $S = \{\ell, q\}$. The localization map with respect to the coordinates $x = (x_\ell, x_q)$, $y = (y_\ell, y_q)$ on $\operatorname{Sel}_{S,2} = \mathbb{A}^4$ has the form

$$\operatorname{loc}_p(x,y) = \begin{pmatrix} \log(\ell)x_\ell + \log(q)x_q \\ \log(\ell)y_\ell + \log(q)y_q \\ \frac{1}{2}\log(\ell)^2 x_\ell y_\ell + a_{\ell,q}x_\ell y_q + a_{q,\ell}x_q y_\ell + \frac{1}{2}\log(q)^2 x_q y_q \end{pmatrix}$$

with unknown coefficients $a_{\ell,q}$, $a_{q,\ell} \in \mathbb{Q}_p$.

We start by determining the equations for $\mathcal{X}(\mathbb{Z}_p)_{S,2}^{|\cdot|}$. This yields the same equations as in case $|S| = 1$ in depth 2 since we are considering the images

under the Kummer map of solutions in which only one prime factor appears. The restriction of loc_p to the subspace $\mathrm{Sel}_{S,2}^{|,|}$ is given by

$$\mathrm{loc}_p(0,0,y_\ell,y_q) = \begin{pmatrix} 0 \\ \log(\ell)y_\ell + \log(q)y_q \\ 0 \end{pmatrix}.$$

In the coordinates u, v, w on $\mathbb{A}^3$, the image of $\mathrm{Sel}_{S,2}^{|,|}$ is therefore cut out by the two equations

$$u = 0, \quad w = 0.$$

Pulling back these equations along j_{dR}, we obtain the following:

Proposition 3.7. *The set $\mathcal{X}(\mathbb{Z}_p)_{S,2}^{|,|}$ is cut out in $\mathcal{X}(\mathbb{Z}_p)$ by the two equations*

$$\log(z) = 0, \quad \mathrm{Li}_2(z) = 0. \tag{3.1}$$

As in the case of one prime above, the vanishing locus $\mathcal{X}(\mathbb{Z}_p)_{S,2}^{|,|}$ consists of the nontrivial $(p-1)$-st roots of unity ζ for which $\mathrm{Li}_2(\zeta) = 0$. This includes in particular -1, which is only a solution of the S-unit equation if $2 \in S$. Note that the set $\mathcal{X}(\mathbb{Z}_p)_{S,2}^{|,|}$ does not depend on the specific set S and in particular not on the coefficients $a_{\ell,q}$ and $a_{q,\ell}$.

We turn to the points of type $(|,-)$. The restriction of loc_p to the subspace $\mathrm{Sel}_{S,2}^{|,-}$ is given by

$$\mathrm{loc}_p(0,x_q,y_\ell,0) = \begin{pmatrix} \log(q)x_q \\ \log(\ell)y_\ell \\ a_{q,\ell}x_q y_\ell \end{pmatrix}.$$

In the coordinates u, v, w on $\mathbb{A}^3$, the image of $\mathrm{Sel}_{S,2}^{|,-}$ is therefore cut out by the equation

$$a_{q,\ell}uv - \log(\ell)\log(q)w = 0.$$

Pulling back along j_{dR} gives the following equation for $\mathcal{X}(\mathbb{Z}_p)_{S,2}^{|,-}$:

$$a_{q,\ell}\log(z)\log(1-z) + \log(\ell)\log(q)\,\mathrm{Li}_2(z) = 0. \tag{3.2}$$

Using the twisted anti-symmetry relation $\log(\ell)\log(q) = a_{\ell,q} + a_{q,\ell}$ and the functional equation relating $\mathrm{Li}_2(z)$ and $\mathrm{Li}_2(1-z)$, this can be written in a more symmetric form as follows:

Proposition 3.8. *The set $\mathcal{X}(\mathbb{Z}_p)_{S,2}^{|,-}$ is cut out in $\mathcal{X}(\mathbb{Z}_p)$ by the equation*

$$a_{\ell,q}\,\mathrm{Li}_2(z) = a_{q,\ell}\,\mathrm{Li}_2(1-z). \tag{3.3}$$

Remark 3.9. Since $\mathrm{Li}_2(-1) = \mathrm{Li}_2(2) = 0$, equation (3.3) is always satisfied for $z = -1$ and $z = 2$, independently of ℓ and q, even when ℓ and q are both odd and these points are not solutions of the S-unit equation.

Observe that the equations $\log(z) = \mathrm{Li}_2(z) = 0$ for $\mathcal{X}(\mathbb{Z}_p)^{|,|}_{S,2}$ imply the equation (3.2) for $\mathcal{X}(\mathbb{Z}_p)^{|,-}_{S,2}$, so we have the inclusion

$$\mathcal{X}(\mathbb{Z}_p)^{|,|}_{S,2} \subseteq \mathcal{X}(\mathbb{Z}_p)^{|,-}_{S,2}. \tag{3.4}$$

Since the action of S_3 on the set $\{|, -, \diagup\}$ of refining Selmer conditions is 2-transitive, the equations (3.1) and (3.3) are sufficient to find equations for all pairs $\Sigma = (i, j)$ of refining Selmer conditions by Proposition 2.16. For example, using the symmetry σ with equation (3.3), we find that $X(\mathbb{Z}_p)^{-,|}_{S,2}$ is defined by the equation

$$a_{\ell,q} \mathrm{Li}_2(1 - z) = a_{q,\ell} \mathrm{Li}_2(z). \tag{3.5}$$

As a consequence of the 2-transitivity and of the inclusion (3.4), the complete set $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ can be computed from $\mathcal{X}(\mathbb{Z}_p)^{|,-}_{S,2}$ by taking S_3-orbits.

The results are summarized in the following theorem.

Theorem 3.10. *Let $S = \{\ell, q\}$ be a set of primes of size two and let $p \notin S$ be a prime. The refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_p)^{\min}_{S,2}$ up to S_3-orbits is cut out in $\mathcal{X}(\mathbb{Z}_p)$ by the equation*

$$a_{\ell,q} \mathrm{Li}_2(z) = a_{q,\ell} \mathrm{Li}_2(1 - z).$$

3.3. **Power series.** Recall that we have

$$\begin{aligned} j_{\mathrm{dR}} \colon \mathcal{X}(\mathbb{Z}_p) &\to U_2^{\mathrm{dR}} \\ z &\mapsto (\log(z), \log(1 - z), -\mathrm{Li}_2(z)). \end{aligned}$$

To compute our Chabauty–Kim sets we need to find the zeroes of the explicit equations determined in Theorem 3.10 above. For this we will compute power series expansions for our coordinates around a fixed residue disk and bound the zeroes of such by studying their Newton polygons.

We will use the residue disc $]2[(\mathbb{Z}_S)$ for computing the power series expansions in the following as we will mostly use $p = 3$ later where this is the only residue disk. In the case $S = \{2, 3\}$ where we choose $p = 5$ there are three residue discs to consider, namely $-1, 2$ and 3. To obtain an expression for j_{dR} in a neighborhood of 2 we want to find power series expansions when $z \in 2 + p\mathbb{Z}_p$ for $\log(z)$, $\log(1 - z)$ and $\mathrm{Li}_2(z)$.

Recall that the functions $\log(z)$ and $\mathrm{Li}_2(z)$ are defined as[8] the (iterated) Coleman integrals

$$\begin{aligned} \log(z) &= \int_{\overrightarrow{01}}^{z} \frac{\mathrm{d}x}{x} \\ \mathrm{Li}_2(z) &= \int_{\overrightarrow{01}}^{z} \frac{\mathrm{d}x}{x} \frac{\mathrm{d}x}{1 - x}. \end{aligned}$$

[8]It is more customary to define $\log(z)$ as a Coleman integral from 1 to z, rather than from $\overrightarrow{01}$. However, it makes no difference which start point we use to define log, since $\int_{\overrightarrow{01}}^{1} \frac{\mathrm{d}x}{x} = 0$, e.g. by a similar argument to Lemma 2.12.

Using additivity of abelian Coleman integrals, we thus find that for $z \in 2 + p\mathbb{Z}_p$, the logarithm $\log(z)$ is given by

$$\log(z) = \underbrace{\int_{\overrightarrow{01}}^{2} \frac{\mathrm{d}x}{x}}_{=\log(2)} + \underbrace{\int_{2}^{z} \frac{\mathrm{d}x}{x}}_{\text{tiny integral}} = \log(2) - \sum_{k=1}^{\infty} \frac{(2-z)^k}{k2^k}.$$

Similarly, for $z \in 2 + p\mathbb{Z}_p$ (so $1 - z \in -1 + p\mathbb{Z}_p$) the logarithm of $1 - z$ is given by

$$\mathrm{Li}_1(z) = \log(1-z) = \underbrace{\int_{\overrightarrow{01}}^{-1} \frac{\mathrm{d}x}{x}}_{=\log(-1)=0} + \underbrace{\int_{-1}^{1-z} \frac{\mathrm{d}x}{x}}_{\text{tiny integral}} = -\sum_{k=1}^{\infty} \frac{(2-z)^k}{k}. \tag{3.6}$$

For $\mathrm{Li}_2(z)$, using the path composition rule for iterated Coleman integrals, we get

$$\mathrm{Li}_2(z) = \mathrm{Li}_2(2) + \left(\int_2^z \frac{\mathrm{d}x}{x}\right) \cdot \mathrm{Li}_1(2) + \int_2^z \frac{\mathrm{d}x}{x}\frac{\mathrm{d}x}{1-x}. \tag{3.7}$$

Since $\mathrm{Li}_2(2) = 0$ (from $\mathrm{Li}_2(z)+\mathrm{Li}_2(1-z) = -\log(z)\log(1-z)$ and $\mathrm{Li}_2(z)+\mathrm{Li}_2(z^{-1}) = -\frac{1}{2}(\log(z))^2$), and $\mathrm{Li}_1(2) = 0$ (from $\mathrm{Li}_1(z) = -\log(1-z)$), we have

$$\mathrm{Li}_2(z) = -\int_{t=0}^{z-2} \frac{\mathrm{d}t}{t+2}\frac{\mathrm{d}t}{t+1}.$$

This can be calculated to be

$$\mathrm{Li}_2(z) = -\sum_{k>i\geq 1} \frac{1}{k}\frac{1}{i2^{k-i}}(2-z)^k. \tag{3.8}$$

In concrete terms,

$$\begin{aligned}\mathrm{Li}_2(z) = &-\frac{1}{4}(2-z)^2 - \frac{1}{6}(2-z)^3 - \frac{5}{48}(2-z)^4 \\ &- \frac{1}{15}(2-z)^5 - \frac{2}{45}(2-z)^6 + O((2-z)^7),\end{aligned} \tag{3.9}$$

where $O((2-z)^7)$ represents all terms of the form $\alpha(2-z)^k$ for $k \geq 7$.

It will be useful to calculate also the power series expansion of $\mathrm{Li}_2(1-z)$ on the residue disk $2 + p\mathbb{Z}_p$. Then $1 - z$ lies in the same residue disk as -1, so by using the path composition rule similarly to (3.7) we obtain

$$\mathrm{Li}_2(1-z) = \mathrm{Li}_2(-1) + \left(\int_{t=0}^{2-z} \frac{\mathrm{d}t}{t-1}\right) \cdot \mathrm{Li}_1(-1) - \int_{t=0}^{2-z} \frac{\mathrm{d}t}{1-t}\frac{\mathrm{d}t}{2-t}.$$

The first summand is $\mathrm{Li}_2(-1) = 0$. In the second summand, we have

$$\mathrm{Li}_1(-1) = -\log(1-(-1)) = -\log(2),$$

and the integral equals

$$\int_{t=0}^{2-z} \frac{\mathrm{d}t}{t-1} = \log(1-z) - \log(-1) = \log(1-z),$$

for which we have already calculated the power series in (3.6) above. For the final summand we calculate the tiny iterated integral as

$$\int_{t=0}^{2-z} \frac{\mathrm{d}t}{1-t}\frac{\mathrm{d}t}{2-t} = \int_{t=0}^{2-z} \frac{\mathrm{d}t}{1-t}\sum_{i=1}^{\infty}\frac{t^i}{i2^i} = \int_{t=0}^{2-z}\sum_{i=1}^{\infty}\sum_{j=1}^{\infty}\frac{t^{i+j-1}\,\mathrm{d}t}{i2^i}$$
$$= \sum_{i=1}^{\infty}\sum_{j=1}^{\infty}\frac{(2-z)^{i+j}}{(i+j)i2^i} = \sum_{k=2}^{\infty}\sum_{i=1}^{k-1}\frac{(2-z)^k}{ki2^i}.$$

Combining the three summands, we obtain the power series

$$\mathrm{Li}_2(1-z) = \sum_{k=1}^{\infty}\frac{1}{k}\Big(\log(2) - \sum_{i=1}^{k-1}\frac{1}{i2^i}\Big)(2-z)^k. \tag{3.10}$$

3.4. **Newton polygon analysis.** Let $S = \{\ell, q\}$ be a set of two primes, both different from 3, so that we can choose $p = 3$ in the Chabauty–Kim method. In order to calculate the set $\mathcal{X}(\mathbb{Z}_3)^{\min}_{S,2}$ up to S_3-orbits, it suffices to calculate the set $\mathcal{X}(\mathbb{Z}_3)^{|,|}_{S,2}$ – which is done in equation 3.1 independently of S – and one more set $\mathcal{X}(\mathbb{Z}_3)^{|,-}_{S,2}$.

Without loss of generality, assume $v_3(a_{\ell,q}) \geq v_3(a_{q,\ell})$. We consider the subset $\mathcal{X}(\mathbb{Z}_3)^{|,-}_{S,2} \subseteq \mathcal{X}(\mathbb{Z}_3)_{S,2}$ defined by the equation

$$a_{\ell,q}\,\mathrm{Li}_2(z) = a_{q,\ell}\,\mathrm{Li}_2(1-z).$$

Using the power series expansions (3.8) and (3.10) for $\mathrm{Li}_2(z)$ and $\mathrm{Li}_2(1-z)$, respectively, we obtain the power series

$$f(z) \coloneqq \sum_{k=1}^{\infty} c_k(2-z)^k$$

with coefficients

$$c_k = \frac{1}{k}\sum_{i=1}^{k-1}\frac{1}{(k-i)2^i}a_{\ell,q} + \frac{1}{k}\Big(\log(2) - \sum_{i=1}^{k-1}\frac{1}{i2^i}\Big)a_{q,\ell}, \tag{3.11}$$

which converges on $\mathcal{X}(\mathbb{Z}_3) = 2 + 3\mathbb{Z}_3$ and defines the set $\mathcal{X}(\mathbb{Z}_3)^{|,-}_{S,2}$. For instance, the first four coefficients are given by

$$c_1 = \log(2)a_{q,\ell},$$
$$c_2 = \frac{1}{4}a_{\ell,q} + \frac{1}{2}\Big(\log(2) - \frac{1}{2}\Big)a_{q,\ell},$$
$$c_3 = \frac{1}{6}a_{\ell,q} + \frac{1}{3}\Big(\log(2) - \frac{5}{8}\Big)a_{q,\ell},$$
$$c_4 = \frac{5}{48}a_{\ell,q} + \frac{1}{4}\Big(\log(2) - \frac{2}{3}\Big)a_{q,\ell}.$$

Lemma 3.11. *For $z \in 2 + 3\mathbb{Z}_3$, the valuation of $\log(z)$ is given by*

$$v_3(\log(z)) = v_3(z+1).$$

Proof. In the series expansion

$$\log(z) = -\sum_{k=1}^{\infty} \frac{1}{k}(z+1)^k,$$

the first summand dominates, i.e. for all $k \geq 2$ we have

$$v_3\Big(\frac{1}{k}(z+1)^k\Big) - v_3(z+1) = (k-1)v_3(z+1) - v_3(k) \geq (k-1) - \log_3(k) > 0,$$

which shows the claim. □

Returning to the study of the function $f(z)$ defining $\mathcal{X}(\mathbb{Z}_3)^{|,-}_{S,2}$, write $z = 2-3t$, then the coefficients of $f(t)$ as a power series in t are $3^k c_k$. We analyze the Newton polygon of this power series. The 3-adic valuation of the k-th coefficient is given by $k + v_3(c_k)$. For $k = 1$, this is

$$1 + v_3(c_1) = 1 + v_3(\log(2)a_{q,\ell}) = 2 + v_3(a_{q,\ell})$$

by Lemma 3.11. For $k \geq 2$, the difference of valuations between the first and the k-th coefficient is

$$\begin{aligned}(k + v_3(c_k)) - (1 + v_3(c_1)) &= k - 2 - v_3(a_{q,\ell}) + v_3(c_k) \\ &\geq k - 2 - v_3(a_{q,\ell}) - v_3(k) - \max_{1\leq i\leq k-1} v_3(i) + v_3(a_{q,\ell}) \\ &= k - 2 - v_3(k) - \max_{1\leq i\leq k-1} v_3(i).\end{aligned}$$

The last expression satisfies

$$k - 2 - v_3(k) - \max_{1\leq i\leq k-1} v_3(i) \begin{cases} = 0, & \text{for } k = 2, 3, \\ > 0, & \text{for } k \geq 4, \end{cases}$$

as one checks by hand for $k = 4$ and for higher k via the estimate

$$k - 2 - v_3(k) - \max_{1\leq i\leq k-1} v_3(i) \geq k - 2 - \log_3(k) - \log_3(k-1).$$

Let $\nu \coloneqq 2 + v_3(a)$, then the Newton polygon of $f(t)$ has the form

$$(0, \infty),\ (1, \nu),\ (2, \geq \nu),\ (3, \geq \nu),\ (4, > \nu), \ldots$$

The first line segment of slope $-\infty$ belongs to the known root $t = 0$ corresponding to $z = 2$ (cf. Remark 3.9). By the same Remark, we have another known root $z = -1$ which corresponds to $t = 1$, so that there is a segment of slope 0. Hence, the first $\geq$ is actually an equality and the point $(2, \nu)$ belongs to the Newton polygon. There is at most one other root in $\mathbb{Z}_3$ before the Newton polygon continues with positive slopes, and this happens if and only if $3 + v_3(c_3) = \nu$, in which case the root has valuation 0.

Proposition 3.12. *Let $S = \{\ell, q\}$ be two primes different from 3, and let $p = 3$. Then the refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_3)^{\min}_{S,2}$ contains $\{2, -1, \frac{1}{2}\}$ and at most one more S_3-orbit of points. The second orbit is present if and only if*

$$\min\{v_3(a_{\ell,q}), v_3(a_{q,\ell})\} = v_3(\log(\ell)) + v_3(\log(q)).$$

Proof. Again, without loss of generality, assume $v_3(a_{\ell,q}) \geq v_3(a_{q,\ell})$. Everything follows from the previous discussion, except for the criterion for when there is another S_3-orbit of points. By the Newton polygon analysis, this happens if and only if $v_3(c_3) = v_3(a_{q,\ell}) - 1$, with the notation as above. Using the twisted antisymmetry relation $a_{q,\ell} + a_{\ell,q} = \log(\ell)\log(q)$, we have

$$\begin{aligned} c_3 &= \frac{1}{6}a_{\ell,q} + \frac{1}{3}(\log(2) - \frac{5}{8})a_{q,\ell} \\ &= \frac{1}{6}\log(\ell)\log(q) + \frac{1}{3}(\underbrace{\log(2) - \frac{9}{8}}_{\text{valuation } 1})a_{q,\ell}. \end{aligned}$$

The twisted anti-symmetry relation also implies

$$v_3(\log(\ell)) + v_3(\log(q)) \geq \min\{v_3(a_{\ell,q}), v_3(a_{q,\ell})\} = v_3(a_{q,\ell}).$$

Hence, the second summand in the formula for c_3 has valuation $v_3(a_{q,\ell})$, the first summand has valuation $\geq v_3(a_{q,\ell}) - 1$. It follows that we have $v_3(c_3) = v_3(a_{q,\ell}) - 1$ if and only if the inequality is an equality. □

Remark 3.13. For all pairs of primes up to 500, we have checked this criterion. The set $\mathcal{X}(\mathbb{Z}_3)^{\min}_{S,2}$ contains an extra point for 2841 out of the 4371 pairs of primes < 500, which is about 65%. More notably, there are some pairs of primes $S = \{2, q\}$ for which the refined Chabauty–Kim conjecture holds in depth 2, namely for

$$q = 19,\ 37,\ 53,\ 107,\ 109,\ 163,\ 181,\ 199,\ 269,\ 271,\ 379,\ 431,\ 433,\ 487,$$

in which case

$$\mathcal{X}(\mathbb{Z}_3)^{\min}_{S,2} = \mathcal{X}(\mathbb{Z}_S) = \left\{2, -1, \frac{1}{2}\right\},$$

as well as all Fermat and Mersenne primes $q = 2^n \pm 1$, where $X(\mathbb{Z}_3)^{\min}_{S,2} = \mathcal{X}(\mathbb{Z}_S)$ consists precisely of the two S_3-orbits of 2 and $\pm q$. We discuss this in more detail in the next section.

3.5. **Fermat and Mersenne primes.** When q is Mersenne (i.e. of the form $q = 2^n - 1$) or Fermat (i.e. of the form $q = 2^n + 1$), then the extra point in the refined Chabauty–Kim locus mentioned in 3.12 is a genuine extra point, thus verifying the refined conjecture.

To give some more details, we need some notation. To treat both cases simultaneously we write $q = 2^n \pm 1$ and agree that every occurrence of the notation "$\pm$" is to be interpreted as "$+$" in the Fermat case and "$-$" in the Mersenne case. Consequently, "$\mp$" refers to the opposite sign in each case. Note that $1 \mp q = \mp 2^n$, so that $\pm q$ and $\mp 2^n$ are S-integral points of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Proposition 3.14. *Let $q = 2^n \pm 1 \neq 3$ be a Fermat or Mersenne prime. Then the refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_3)^{\min}_{\{2,q\},2}$ consists of $\{2, -1, \frac{1}{2}\}$ and the S_3-orbit of the point $\pm q$.* □

We can give explicit equations cutting out the refined Chabauty–Kim sets $\mathcal{X}(\mathbb{Z}_3)^{\Sigma}_{\{2,q\},2}$ for Σ a set of refining conditions, for general primes q. By Theorem 3.10, this boils down to the calculation of the coefficients $a_{2,q}$ and $a_{q,2}$ of the third component of the localization map. Above these were computed as

$$a_{2,q} = -\frac{1}{n}\operatorname{Li}_2(1 \mp q),$$
$$a_{q,2} = -\frac{1}{n}\operatorname{Li}_2(\pm q).$$

Specializing from Theorem 3.10, we can now write down the explicit equations cutting out the refined Chabauty–Kim sets:

Theorem 3.15. *Let $q = 2^n \pm 1$ be a Fermat or Mersenne prime and $p \neq 2, q$. The refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_p)^{|,-}_{\{2,q\},2}$ is cut out by the equation*

$$\operatorname{Li}_2(1 \mp q)\operatorname{Li}_2(z) = \operatorname{Li}_2(\pm q)\operatorname{Li}_2(1 - z).$$

Remark 3.16. The refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_p)^{|,|}_{\{2,q\},2}$ is cut out by $\log(z) = \operatorname{Li}_2(z) = 0$ according to Theorem 3.10. Together with $\mathcal{X}(\mathbb{Z}_p)^{|,-}_{\{2,q\},2}$, this determines explicit equations for $\mathcal{X}(\mathbb{Z}_p)^{\Sigma}_{\{2,q\},2}$ for all choices of refinement conditions Σ via S_3-equivariance (see Proposition 2.16).

3.6. **The case $q = 3$.** Now consider the set $S = \{2, 3\}$. As discussed in Section 1, the prime $q = 3$ is special in that there are solutions to the $\{2, 3\}$-unit equation of all three kinds: Fermat ($3 - 2 = 1$), Mersenne ($-3 + 4 = 1$) and Catalan ($9-8 = 1$). Together with the $\{2\}$-integral solution ($-1+2 = 1$), this gives four S_3-orbits of $\mathbb{P}^1(\mathbb{Z}[1/6])$, forming 21 solutions in total:

$$\{-1, 1/2, 2\} \cup \{-2, -1/2, 1/3, 2/3, 3/2, 3\} \cup \{-3, -1/3, 1/4, 3/4, 4/3, 4\}$$
$$\cup \{-8, -1/8, 1/9, 8/9, 9/8, 9\}.$$

Let $p \neq 2, 3$ be a prime. The three S-integral points 3, -3, 9 lead to three different formulas for the coefficients $a_{2,3}$ and $a_{3,2}$. Viewing $3 = 2^1 + 1$ as a Fermat prime yields

$$a_{2,3} = -\operatorname{Li}_2(-2), \quad a_{3,2} = -\operatorname{Li}_2(3) \tag{3.12}$$

as in the previous subsection; viewing $3 = 2^2 - 1$ as a Mersenne prime yields

$$a_{2,3} = -\frac{1}{2}\operatorname{Li}_2(4), \quad a_{3,2} = -\frac{1}{2}\operatorname{Li}_2(-3); \tag{3.13}$$

and using the commutativity of the Chabauty–Kim diagram for the Catalan solutions $z = -8$ and $z = 9$, which satisfy $j_S(-8) = (3, 0, 0, 2)$ and $j_S(9) = (0, 2, 3, 0)$, yields

$$a_{2,3} = -\frac{1}{6}\operatorname{Li}_2(-8), \quad a_{3,2} = -\frac{1}{6}\operatorname{Li}_2(9). \tag{3.14}$$

Thus, the Chabauty–Kim diagram yields as a byproduct the following identities of dilogarithms:

$$\mathrm{Li}_2(-2) = \frac{1}{2}\,\mathrm{Li}_2(4) = \frac{1}{6}\,\mathrm{Li}_2(-8),$$
$$\mathrm{Li}_2(3) = \frac{1}{2}\,\mathrm{Li}_2(-3) = \frac{1}{6}\,\mathrm{Li}_2(9).$$

According to Theorem 3.10, the refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_p)^{|,-}_{\{2,3\}}$ is cut out by the equation

$$a_{2,3}\,\mathrm{Li}_2(z) = a_{3,2}\,\mathrm{Li}_2(1-z), \tag{3.15}$$

with the coefficients $a_{2,3}$ and $a_{3,2}$ given by the equivalent equations (3.12), (3.13), (3.14). The points -1, 3, -3, 9 are all of type $(|,-)$ and are therefore solutions of (3.15).

Let us now choose $p = 5$, the smallest possible choice since p has to be different from 2 and 3. According to Theorem 3.10, the refined Chabauty–Kim set $\mathcal{X}(\mathbb{Z}_5)^{|,|}_{\{2,3\}}$ is cut out by the equations $\log(z) = \mathrm{Li}_2(z) = 0$. The simultaneous roots when $p = 5$ are the 4th roots of unity ζ satisfying $\mathrm{Li}_2(\zeta) = 0$. Numerical computation shows that this is not the case for $\pm i$ and the fact that $\mathrm{Li}_2(-1) = 0$ shows that the only root in $\mathcal{X}(\mathbb{Z}_5)$ is $z = -1$. However, computer calculations show that for the set $\mathcal{X}(\mathbb{Z}_5)^{|,-}_{\{2,3\}}$ there is, in addition to the known solutions above, one extra solution of (3.15) in the residue disk $3 + 5\mathbb{Z}_5$ which does not correspond to a solution of the S-unit equation and appears transcendental.

Appendix A. Elementary Proof of Bilinearity (by M. Lüdtke)

In the Chabauty–Kim diagram (2.1) of the thrice-punctured line in depth $n = 2$, the mysterious part is the localization map

$$\mathrm{loc}_p\colon \mathrm{Sel}_{S,2} \xrightarrow{\mathrm{res}_p} H^1_f(G_p, U_2^{\text{ét}}) \xrightarrow[\sim]{\log_{\mathrm{BK}}} U_2^{\mathrm{dR}}. \tag{A.1}$$

Using the calculations of the Selmer scheme and the de Rham fundamental group, the localization map is identified with a map of affine $\mathbb{Q}_p$-spaces

$$\mathrm{loc}_p\colon \mathbb{A}^S \times \mathbb{A}^S \longrightarrow \mathbb{A}^3 \tag{A.2}$$

whose projection onto the first two components is given by

$$(x, y) \mapsto \begin{pmatrix} \sum_{\ell\in S} \log(\ell) x_\ell \\ \sum_{\ell\in S} \log(\ell) y_\ell \end{pmatrix}$$

with coordinates $x = (x_\ell)_{\ell\in S}$, $y = (y_\ell)_{\ell\in S}$ on $\mathbb{A}^S \times \mathbb{A}^S$. The difficult part is the third component.

Theorem A.1. *The third component of the localization map* (A.2) *is bilinear.*

The bilinearity is proved in [DCW15], Section 10, in the setting of mixed Tate motives. We give here an elementary proof in terms of Galois cohomology calculations. The proof is split into two parts according to the factorization (A.1) of the localization map. As an algebraic map between affine $\mathbb{Q}_p$-schemes, the bilinearity can be checked on $\mathbb{Q}_p$-points.

A.1. **A cocycle lifting.** Consider first the map

$$\mathrm{Sel}_{S,2}(\mathbb{Q}_p) \to H^1_f(G_p, U_2^{\text{ét}}(\mathbb{Q}_p)),$$

which arises from the restriction map along $G_p \hookrightarrow G_T$

$$\mathrm{res}_p \colon H^1(G_T, U_2^{\text{ét}}(\mathbb{Q}_p)) \to H^1(G_p, U_2^{\text{ét}}(\mathbb{Q}_p))$$

via restricting to cohomology classes which are crystalline at p. The group $U_2^{\text{ét}}(\mathbb{Q}_p)$ is a Heisenberg group

$$U_2^{\text{ét}}(\mathbb{Q}_p) = \begin{pmatrix} 1 & \mathbb{Q}_p(1) & \mathbb{Q}_p(2) \\ & 1 & \mathbb{Q}_p(1) \\ & & 1 \end{pmatrix},$$

with abelianization $U_1^{\text{ét}}(\mathbb{Q}_p) = \mathbb{Q}_p(1) \times \mathbb{Q}_p(1)$ via projection to the $(1,2)$ and $(2,3)$ entries, with central kernel $\mathbb{Q}_p(2)$. Write $Z^1(-,-)$ for continuous (nonabelian) 1-cocycle sets, and denote by $Z^1_f(-,-)$ the subset of cocycles whose classes are crystalline at p.

Lemma A.2. *The restriction map admits a lifting φ to the level of cocycles*

$$\begin{array}{ccc} & & Z^1_f(G_p, U_2^{\text{ét}}(\mathbb{Q}_p)) \\ & \overset{\varphi}{\dashrightarrow} & \big\downarrow \\ \mathbb{Q}_p^S \times \mathbb{Q}_p^S \cong H^1_f(G_T, U_2^{\text{ét}}(\mathbb{Q}_p)) & \xrightarrow{\mathrm{res}_p} & H^1_f(G_p, U_2^{\text{ét}}(\mathbb{Q}_p)) \end{array}$$

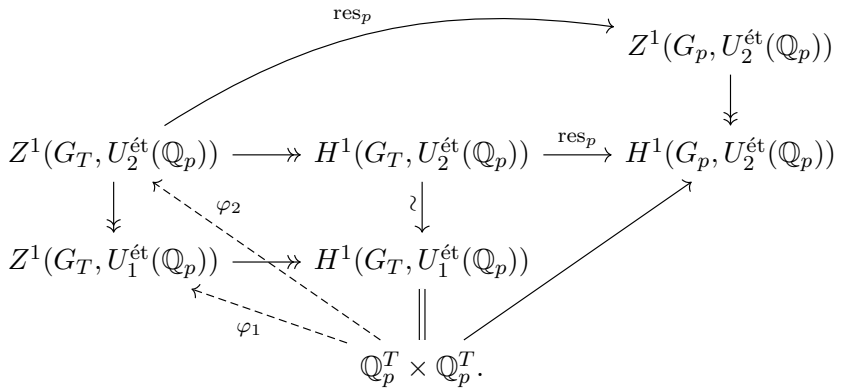
of the form

$$\varphi(x,y) = \begin{pmatrix} 1 & \alpha(x) & \gamma(x,y) \\ & 1 & \beta(y) \\ & & 1 \end{pmatrix}$$

such that

(i) $\alpha(x) \colon G_p \to \mathbb{Q}_p(1)$ *is linear in* x*;*
(ii) $\beta(y) \colon G_p \to \mathbb{Q}_p(1)$ *is linear in* y*;*
(iii) $\gamma(x,y) \colon G_p \to \mathbb{Q}_p(2)$ *is bilinear in* (x,y)*.*

Proof. Consider the following diagram:



The cocycle set $Z^1(G_T, U_1^{\text{ét}}(\mathbb{Q}_p))$ is naturally a $\mathbb{Q}_p$-vector space, so that the isomorphism $H^1(G_T, U_1^{\text{ét}}(\mathbb{Q}_p)) \cong \mathbb{Q}_p^T \times \mathbb{Q}_p^T$ admits a $\mathbb{Q}_p$-linear splitting to the level of cocycles:

$$\varphi_1 \colon \mathbb{Q}_p^T \times \mathbb{Q}_p^T \to Z^1(G_T, U_1^{\text{ét}}(\mathbb{Q}_p)). \tag{A.3}$$

Concretely, choose for every prime $\ell \in T$ a compatible system of p^n-th roots $\sqrt[p^n]{\ell}$ in the maximal extension of $\mathbb{Q}$ which is unramified outside T, giving rise to a Kummer cocycle

$$\kappa_\ell \colon G_T \to \mathbb{Q}_p(1) = (\varprojlim_n \mu_{p^n}) \otimes \mathbb{Q}_p,$$
$$\sigma \mapsto \left(\sigma(\sqrt[p^n]{\ell})/\sqrt[p^n]{\ell}\right)_{n\in\mathbb{N}}.$$

Then a $\mathbb{Q}_p$-linear lift $\kappa \colon \mathbb{Q}_p^T \to Z^1(G_T, \mathbb{Q}_p(1))$ is given by linear extension:

$$\kappa(x) \coloneqq \sum_{\ell\in T} x_\ell \kappa_\ell$$

for $x = (x_\ell)_{\ell\in T}$, and we can define $\varphi_1 \coloneqq \kappa \times \kappa$ in (A.3).

As a next step, one has to lift the obtained cocycles $\varphi_1(x,y) = (\kappa(x), \kappa(y))$ from $U_1^{\text{ét}}$ to $U_2^{\text{ét}}$. The obstruction to the lifting problem is a class in second cohomology $H^2(G_T, \mathbb{Q}_p(2))$, namely the image of $(\kappa(x), \kappa(y)) \in Z^1(G_T, U_1^{\text{ét}}(\mathbb{Q}_p))$ under the nonabelian connecting map arising from the central extension

$$1 \to \mathbb{Q}_p(2) \to U_2^{\text{ét}}(\mathbb{Q}_p) \to U_1^{\text{ét}}(\mathbb{Q}_p) \to 1.$$

Concretely, a lifting cocycle $\varphi_2(x,y)$ has the form

$$\varphi_2(x,y) = \begin{pmatrix} 1 & \kappa(x) & \gamma(x,y) \\ & 1 & \kappa(y) \\ & & 1 \end{pmatrix} \in Z^1(G_T, U_2^{\text{ét}}(\mathbb{Q}_p)) \tag{A.4}$$

for some continuous map $\gamma(x,y)\colon G_T \to \mathbb{Q}_p(2)$. The cocycle condition becomes:

$$\begin{aligned}\varphi_2(x,y)(\sigma\tau) &\overset{!}{=} \varphi_2(x,y)(\sigma)\cdot\sigma\varphi_2(x,y)(\tau)\\ &= \begin{pmatrix} 1 & \kappa(x)(\sigma) & \gamma(x,y)(\sigma)\\ & 1 & \kappa(y)(\sigma)\\ & & 1\end{pmatrix}\begin{pmatrix} 1 & \sigma\kappa(x)(\tau) & \sigma\gamma(x,y)(\tau)\\ & 1 & \sigma\kappa(y)(\tau)\\ & & 1\end{pmatrix}\\ &= \begin{pmatrix} 1 & \kappa(x)(\sigma)+\sigma\kappa(x)(\tau) & \sigma\gamma(x,y)(\tau)+\kappa(x)(\sigma)\cdot\sigma\kappa(y)(\tau)+\gamma(x,y)(\sigma)\\ & 1 & \kappa(y)(\sigma)+\sigma\kappa(y)(\tau)\\ & & 1\end{pmatrix}\end{aligned}$$

for $\sigma,\tau\in G_T$. The equations for the $(1,2)$ and $(2,3)$ entries are satisfied, as they merely express the cocycle property of $\kappa(x)$ and $\kappa(y)$. The equation for the $(1,3)$ entry can be rewritten as

$$\sigma\gamma(x,y)(\tau)-\gamma(x,y)(\sigma\tau)+\gamma(x,y)(\tau)\overset{!}{=}-\kappa(x)(\sigma)\cdot\sigma\kappa(y)(\tau).$$

The left hand side is the coboundary $\partial\gamma(x,y)$ of the 1-cochain $\gamma(x,y)$ and the right hand side is the cup product $-\kappa(x)\smile\kappa(y)$ on the level of cocycles, evaluated at $(\sigma,\tau)\in G_T^2$. Hence, in the terminology of [DCW14][9], a lifting of $(\kappa(x),\kappa(y))$ to $Z^2(G_T,U_2^{\text{ét}}(\mathbb{Q}_p))$ is equivalent to a solution $\gamma(x,y)\colon G_T\to\mathbb{Q}_p(2)$ of the "Heisenberg coboundary equation"

$$\partial\gamma(x,y)=-\kappa(x)\smile\kappa(y). \tag{A.5}$$

By Soulé vanishing, $H^2(G_T,\mathbb{Q}_p(2))=0$, so that the coboundary equation (A.5) admits a solution for all $(x,y)\in\mathbb{Q}_p(1)^2$. Choose a solution $\gamma(e_\ell,e_q)$ for each pair of "basis vectors" $e_\ell,e_q\in\mathbb{Q}_p^T$ and extend bilinearly:

$$\gamma(x,y)\coloneqq\sum_{\ell,q\in T}x_\ell y_q\gamma(e_\ell,e_q).$$

Then the bilinearity of the cup product implies that $\gamma(x,y)$ satisfies the coboundary equation (A.5) for all $x,y\in\mathbb{Q}_p^T$, and hence that $\varphi_2(x,y)$ defined by (A.4) provides a lift of the cocycle $\varphi_1(x,y)=(\kappa(x),\kappa(y))$ to depth 2 with additional the property that its $(1,3)$ component is bilinear in x and y. Then (i)–(iii) are satisfied for φ_2, and hence also for

$$\varphi\coloneqq\operatorname{res}_p\circ\varphi_2|_{\mathbb{Q}_p^S\times\mathbb{Q}_p^S}.$$ □

A.2. **The nonabelian Bloch–Kato logarithm in terms of cocycles.** As a next step, we need to describe the isomorphism

$$H^1_f(G_p,U_2^{\text{ét}}(\mathbb{Q}_p))\xrightarrow[\sim]{\log_{\text{BK}}}U_2^{\text{dR}}(\mathbb{Q}_p).$$

in terms of cocycles. We provide such a description in the following general situation.

Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers R and absolute Galois group $G_K=\operatorname{Gal}(\overline{K}/K)$. Let $\mathcal{X}/R$ be the complement of a smooth

[9]While we follow [Ser94], the authors of [DCW14] use a differing sign convention for coboundary maps in group cohomology, which explains the absence of the minus sign in their Heisenberg coboundary equation.

divisor in a smooth proper curve over R, and let X/K be its generic fibre. Let b be an R-integral point or tangent vector of $\mathcal{X}$. Fix $n \geq 1$ and let $U_n^{\text{ét}}/\mathbb{Q}_p$ be the $\mathbb{Q}_p$-unipotent étale fundamental group of depth n of $X_{\overline{K}}$ with base point $b_{\overline{K}}$. Let U_n^{dR}/K be the de Rham fundamental group of depth n of X with base point b_K. The nonabelian Bloch–Kato logarithm now takes the form of a map

$$H^1_f(G_K, U_n^{\text{ét}}(\mathbb{Q}_p)) \xrightarrow{\log_{\mathrm{BK}}} (F^0\backslash U_n^{\mathrm{dR}})(K). \tag{A.6}$$

The map $\log_{\mathrm{BK}}$ is defined in [Kim09] by interpreting both sides as classifying sets for certain torsors and $\log_{\mathrm{BK}}$ as Fontaine's Dieudonné functor between the corresponding categories:

$$D\colon \begin{pmatrix} \text{crystalline } G_K\text{-equivariant} \\ U_n^{\text{ét}}\text{-torsors over } \mathbb{Q}_p \end{pmatrix} \longrightarrow \begin{pmatrix} \text{admissible } U_n^{\mathrm{dR}}\text{-torsors} \\ \text{over } K \end{pmatrix} \tag{A.7}$$

We recall this definition of $\log_{\mathrm{BK}}$ in terms of torsors in order to extract from it our cocycle description. We only collect the facts we need and refer to [Kim09] for details.

The unipotent group $U_n^{\text{ét}}$ over $\mathbb{Q}_p$ is equipped with an action of G_K by algebraic automorphisms which is continuous in the sense that the G_K-action on $U_n^{\text{ét}}(\mathbb{Q}_p)$ is continuous. A G_K-equivariant $U_n^{\text{ét}}$-torsor over $\mathbb{Q}_p$ is a torsor in the usual sense similarly equipped with a continuous G_K-action such that the action map $P \times U_n^{\text{ét}} \to P$ is G_K-equivariant.

On U_n^{dR}, there are two extra structures: a Hodge filtration $F^\bullet$ by closed subschemes and a Frobenius automorphism φ induced by a comparison isomorphism with the crystalline fundamental group. A U_n^{dR}-torsor is required to be similarly equipped with those two extra structures and the action map has to be compatible with them. Such a U_n^{dR}-torsor T is called *admissible* if it separately trivializable with respect to the Hodge filtration and the Frobenius structure. Every U_n^{dR}-torsor over K is automatically admissible. Indeed, a Hodge trivialization of T is equivalent to the existence of a K-point in F^0T, and the latter is a torsor under the unipotent closed subgroup $F^0U_n^{\mathrm{dR}}$ of U^{dR} and therefore trivial. The Frobenius trivialization is equivalent to a Frobenius-invariant K-point of T. It follows from the arguments of [Bes02a, §3] that there exists even a unique Frobenius-invariant point.

The bijection between $(F^0\backslash U_n^{\mathrm{dR}})(K)$ and isomorphism classes of admissible U_n^{dR}-torsors over K is given as follows. For an admissible U_n^{dR}-torsor T, let $p_T^{\mathrm{H}} \in F^0T(K)$ be a Hodge-trivializing point and $p_T^{\mathrm{cr}} \in T(K)^{\varphi=1}$ the unique Frobenius-invariant point. Then the difference $u_T \coloneqq (p_T^{\mathrm{H}})^{-1}p_T^{\mathrm{cr}}$ of the two trivializations is the well-defined element of $(F^0\backslash U_n^{\mathrm{dR}})(K)$ which represents the admissible torsor T.

Remark A.3. We are differing slightly from [Kim09, Proposition 1]: In loc. cit., the admissible U_n^{dR}-torsor T is represented by the *left* coset $(p_T^{\mathrm{cr}})^{-1}p_T^{\mathrm{H}} \in (U_n^{\mathrm{dR}}/F^0)(K)$ rather than the *right* coset $(p_T^{\mathrm{H}})^{-1}p_T^{\mathrm{cr}}$ in $(F^0\backslash U_n^{\mathrm{dR}})(K)$. Of

course, those two are equivalent to each other via the inversion map. However, it is the map (A.6), using right cosets, which deserves to be called (nonabelian) Bloch–Kato logarithm since it specializes to the classical Bloch–Kato logarithm in the abelian case (see [Sak17, Theorem 1.1 (ii)]). The order "crystalline path followed by inverse of Hodge path" is also what Furusho uses (and to which Dan-Cohen–Wewers refer) in finding explicit equations of the de Rham Kummer map for the thrice-punctured line (see [Fur07, Theorem 2.3], [DCW15, §7.3]).

Let us describe the Dieudonné functor $D \coloneqq D_{\mathrm{dR}}$ in (A.7). If P is a G_K-equivariant $U_n^{\text{ét}}$-torsor, then $D(P)$ is the scheme over $\mathrm{B}_{\mathrm{dR}}^{G_K} = K$ defined by

$$D(P)(\Lambda) = P(B_{\mathrm{dR}} \otimes_K \Lambda)^{G_K} \quad \text{for } K\text{-algebras } \Lambda. \tag{A.8}$$

Here, G_K acts on $P(\mathrm{B}_{\mathrm{dR}} \otimes_K \Lambda)$ via the actions on P and on B_{dR}. With $D(U_n^{\text{ét}})$ similarly defined, there is a canonical isomorphism $D(U_n^{\text{ét}}) \cong U_n^{\mathrm{dR}}$ by the comparison theorems of Olsson's nonabelian p-adic Hodge theory [Ols11]. If P is crystalline (i.e. $\mathrm{B}_{\mathrm{cris}}$-admissible in the sense of [Bet17, (3.4.3)]), then it is also de Rham, and the fact that D commutes with tensor products on B_{dR}-admissible representations [Fon94, §1.5] implies that $D(P)$ is naturally a U_n^{dR}-torsor over K. Here, $D(P)$ inherits a Hodge filtration from B_{dR} and the action map $D(P) \times U_n^{\mathrm{dR}} \to D(P)$ is compatible with it. Similarly, the crystalline Dieudonné functor D_{cris} and the comparison $D_{\mathrm{cris}}(P) \times_{K_0} K \cong D(P)$ (where K_0 is the maximal absolutely unramified subfield of K) equip $D(P)$ with a Frobenius automorphism compatible with the torsor structure. In this way, $D(P)$ becomes an admissible U_n^{dR}-torsor.

Proposition A.4. *Let $c \in Z_f^1(G_K, U_n^{\text{ét}}(\mathbb{Q}_p))$ be a continuous cocycle which represents a crystalline $U_n^{\text{ét}}$-torsor. There exist a point p_c^{H} in $U_n^{\text{ét}}(\mathrm{B}_{\mathrm{dR}}^+)$ and a unique point p_c^{cr} in $U_n^{\text{ét}}(\mathrm{B}_{\mathrm{cris}}^{\varphi=1})$, each realising c as a coboundary in $Z^1(G_K, U_n^{\text{ét}}(\mathrm{B}_{\mathrm{dR}}))$:*

$$c(\sigma) = p_c^{\mathrm{H}} \sigma(p_c^{\mathrm{H}})^{-1} = p_c^{\mathrm{cr}} \sigma(p_c^{\mathrm{cr}})^{-1} \quad \textit{for all } \sigma \in G_K.$$

The difference $u_c \coloneqq (p_c^{\mathrm{H}})^{-1} p_c^{\mathrm{cr}}$ is an element of $U_n^{\text{ét}}(\mathrm{B}_{\mathrm{dR}})^{G_K} \cong U_n^{\mathrm{dR}}(K)$ and the nonabelian Bloch–Kato logarithm (A.6) *is given by*

$$\log_{\mathrm{BK}}([c]) = [u_c] \in (F^0 \backslash U_n^{\mathrm{dR}})(K).$$

Proof. The cocycle c represents the G_K-equivariant $U_n^{\text{ét}}$-torsor P_c over $\mathbb{Q}_p$ whose underlying $U_n^{\text{ét}}$-torsor is trivial (i.e. $P_c = U_n^{\text{ét}}$ acting on itself by right multiplication), but whose G_K-action $\rho_c \colon G_K \to \mathrm{Aut}(U_n^{\text{ét}})$ is twisted by c. On R-points (for $\mathbb{Q}_p$-algebras R), the twisted action is given by

$$\rho_c(\sigma)(u) = c(\sigma)\sigma(u) \quad \text{for } \sigma \in G_K,\ u \in U_n^{\text{ét}}(R).$$

According to (A.8), the K-points of $D(P_c)$ are given by

$$D(P_c)(K) = P_c(\mathrm{B}_{\mathrm{dR}})^{G_K} = \{p \in U_n^{\text{ét}}(\mathrm{B}_{\mathrm{dR}}) : c(\sigma)\sigma(p) = p \ \forall \sigma \in G_K\}.$$

In other words, giving a K-point of $D(P_c)$ is equivalent to realising c as a coboundary in $Z^1(G_K, U_n^{\text{ét}}(\mathrm{B_{dR}}))$. By the discussion above, $D(P_c)$ has a K-point p_c^{H} in the subscheme $F^0D(P_c)$. Since the Hodge filtration on $D(P_c)$ is induced from that on $\mathrm{B_{dR}}$, with $F^0D(P_c)$ corresponding to $F^0\mathrm{B_{dR}} = \mathrm{B_{dR}^+}$, we have

$$p_c^{\mathrm{H}} \in F^0D(P_c)(K) = P_c(\mathrm{B_{dR}^+})^{G_K}.$$

Similarly, by [Bes02a, §3], there exists a unique Frobenius-invariant point

$$p_c^{\mathrm{cr}} \in D_{\mathrm{cris}}(P_c)(K_0)^{\varphi=1} = P_c(\mathrm{B_{cris}^{\varphi=1}})^{G_K}.$$

Since p_c^{H} and p_c^{cr} both realize c as a coboundary, their difference $u_c := (p_c^{\mathrm{H}})^{-1}p_c^{\mathrm{cr}} \in U_n^{\text{ét}}(\mathrm{B_{dR}})$ is G_K-invariant:

$$u_c \in U_n^{\text{ét}}(\mathrm{B_{dR}})^{G_K} = U_n^{\mathrm{dR}}(K).$$

As $F^0D(P_c)$ is an $F^0U_n^{\mathrm{dR}}$-torsor, a different choice of p_c^{H} leads to u_c being multiplied from the right by an element of $F^0U_n^{\mathrm{dR}}(K)$, so that $[u_c]$ is well-defined as an element of $(F^0\backslash U_n^{\mathrm{dR}})(K)$. Comparing with the description of $\log_{\mathrm{BK}}$ in terms of torsors as recalled above, it is clear that $\log_{\mathrm{BK}}([c]) = [u_c]$. □

A.3. **Proof of bilinearity.** We return to the proof of bilinearity of the third component of the localization map (A.2). For a topological $\mathbb{Q}_p$-algebra R with continuous G_p-action, denote by $C^i(G_p, U_2^{\text{ét}}(R))$ the set of continuous (nonabelian) i-cochains $G_p^i \to U_2^{\text{ét}}(R)$ (only $i = 0, 1$ are relevant). Let us call a "parametrized" cochain $f\colon \mathbb{Q}_p^S \times \mathbb{Q}_p^S \to C^i(G_p, U_2^{\text{ét}}(R))$ *homogeneous* if it has the form

$$f(x,y) = \begin{pmatrix} 1 & \alpha(x) & \gamma(x,y) \\ & 1 & \beta(y) \\ & & 1 \end{pmatrix}$$

where

(i) $\alpha(x)\colon G_p^i \to R(1)$ is $\mathbb{Q}_p$-linear in x;
(ii) $\beta(y)\colon G_p^i \to R(1)$ is $\mathbb{Q}_p$-linear in y;
(iii) $\gamma(x,y)\colon G_p^i \to R(2)$ is $\mathbb{Q}_p$-bilinear in (x,y).

Thus, Lemma A.2 can be rephrased as saying that the restriction map $\mathrm{res}_p\colon \mathbb{Q}_p^S \times \mathbb{Q}_p^S \to H_f^1(G_p, U_2^{\text{ét}}(\mathbb{Q}_p))$ admits a lift to $Z_f^1(G_p, U_2^{\text{ét}}(\mathbb{Q}_p))$ which is homogeneous.

Lemma A.5. *Homogeneous cochains are stable under pointwise multiplication and inversion. More precisely: let $f, g\colon \mathbb{Q}_p^S \times \mathbb{Q}_p^S \to C^i(G_p, U_2^{\text{ét}}(R))$ be homogeneous and define fg and f^{-1} for $(x,y) \in \mathbb{Q}_p^S \times \mathbb{Q}_p^S$ and $\underline{\sigma} \in G_p^i$ by*

$$(fg)(x,y)(\underline{\sigma}) = f(x,y)(\underline{\sigma}) \cdot g(x,y)(\underline{\sigma}),$$
$$f^{-1}(x,y)(\underline{\sigma}) = f(x,y)(\underline{\sigma})^{-1}.$$

Then fg and f^{-1} are homogeneous.

Proof. This follows from the formulae for multiplication and inversion of unipotent 3 by 3 matrices. □

Lemma A.6. *If $f\colon \mathbb{Q}_p^S \times \mathbb{Q}_p^S \to U_2^{\text{ét}}(R)$ is homogeneous, then so is the image ∂f of f along the coboundary map $\partial\colon U_2^{\text{ét}}(R) \to Z^1(G_p, U_2^{\text{ét}}(R))$.*

Proof. The coboundary $\partial f(x,y)$ is given by

$$\partial f(x,y)(\sigma) = f(x,y)^{-1} \cdot \sigma(f(x,y)).$$

Since G_p acts on $R(1)$ and $R(2)$ by $\mathbb{Q}_p$-linear automorphisms, the parametrized 1-cochain $(x,y) \mapsto (\sigma \mapsto \sigma(f(x,y)))$ is homogeneous. The claim now follows from Lemma A.5. □

Proof of Theorem A.1. Let $\varphi(x,y)$ be the homogeneous cocycle lifting from Lemma A.2 with components $\alpha(x)$, $\beta(y)$, $\gamma(x,y)$. For all $(x,y) \in \mathbb{Q}_p^S \times \mathbb{Q}_p^S$, let $p^{\mathrm{H}}(x,y) \in U_2^{\text{ét}}(\mathrm{B}_{\mathrm{dR}}^+)$ and $p^{\mathrm{cr}}(x,y) \in U_2^{\mathrm{cr}}(\mathrm{B}_{\mathrm{cris}}^{\varphi=1})$ be elements realizing $\varphi(x,y)$ as a coboundary:

$$\varphi = \partial((p^{\mathrm{H}})^{-1}) = \partial((p^{\mathrm{cr}})^{-1}).$$

By Proposition A.4, the image of (x,y) in $U_2^{\text{ét}}(\mathrm{B}_{\mathrm{dR}})^{G_p} = U_2^{\mathrm{dR}}(\mathbb{Q}_p)$ under the localization map is given by

$$\mathrm{loc}_p(x,y) = \log_{\mathrm{BK}}(\varphi(x,y)) = p^{\mathrm{H}}(x,y)^{-1} p^{\mathrm{cr}}(x,y).$$

The claimed bilinearity follows from Lemma A.5 if we show that $p^{\mathrm{H}}(x,y)$ and $p^{\mathrm{cr}}(x,y)$ are homogeneous.

Since we are working with the punctured line, the groups $F^0U_1^{\mathrm{dR}}$ and $F^0U_2^{\mathrm{dR}}$, which parametrize unipotent vector bundles on the compactification $\mathbb{P}^1_{\mathbb{Q}}$ (cf. [Had11, §3]), are trivial. As a consequence, not only $p^{\mathrm{cr}}(x,y)$ but also $p^{\mathrm{H}}(x,y)$ is uniquely determined.

Write $p^{\mathrm{H}}(x,y)$ in components as

$$p^{\mathrm{H}}(x,y) = \begin{pmatrix} 1 & a^{\mathrm{H}}(x,y) & c^{\mathrm{H}}(x,y) \\ & 1 & b^{\mathrm{H}}(x,y) \\ & & 1 \end{pmatrix}.$$

Then $a^{\mathrm{H}}(x,y)$ realizes $\alpha(x)$ as a coboundary:

$$\alpha(x)(\sigma) = a^{\mathrm{H}}(x,y) - \sigma(a^{\mathrm{H}}(x,y)) \quad \text{for all } \sigma \in G_p,$$

and similarly for $b^{\mathrm{H}}(x,y)$ and $\beta(y)$. Since $F^0U_1^{\mathrm{dR}} = 1$, the elements $a^{\mathrm{H}}(x,y)$ and $b^{\mathrm{H}}(x,y)$ are uniquely determined by this property. This implies that $a^{\mathrm{H}}(x) \coloneqq a^{\mathrm{H}}(x,y)$ depends only on x, that $b^{\mathrm{H}}(y) \coloneqq b^{\mathrm{H}}(x,y)$ depends only on y, and that the maps are linear since $\alpha(x)$ and $\beta(y)$ are linear. Define $\widetilde{p}^{\mathrm{H}}(x,y)$ by linearly extending from the values $p^{\mathrm{H}}(e_\ell, e_q)$ on basis vectors $(\ell, q \in S)$ to form a homogeneous cochain:

$$\widetilde{a}^{\mathrm{H}}(x) = a^{\mathrm{H}}(x), \quad \widetilde{b}^{\mathrm{H}}(x) = b^{\mathrm{H}}(y), \quad \widetilde{c}^{\mathrm{H}}(x,y) = \sum_{\ell,q} x_\ell y_q c^{\mathrm{H}}(e_\ell, e_q).$$

Then, by Lemmas A.5, A.6, $\partial((\widetilde{p}^{\mathrm{H}})^{-1})(x,y)$ is homogeneous. It agrees with the homogeneous cochain $\varphi(x,y)$ on pairs of basis vectors, hence everywhere. By uniqueness, $\widetilde{p}^{\mathrm{H}}(x,y) = p^{\mathrm{H}}(x,y)$ for all $(x,y) \in \mathbb{Q}_p^S \times \mathbb{Q}_p^S$, hence $p^{\mathrm{H}}(x,y)$

is homogeneous as claimed. The same argument shows that also $p^{\mathrm{cr}}(x,y)$ is homogeneous. □

Appendix B. Functoriality of the Chabauty–Kim diagram (by L.A. Betts and M. Lüdtke)

Let F be a number field, S a finite set of primes of F, and R the ring of S-integers in F. Let v be a place of K not contained in S, let p be its residue characteristic, and R_v the completion of R at v. Let T be the set of primes consisting of S together with all primes dividing p. Denote by G_T the Galois group over F of the maximal extension which is unramified outside T, and let $G_v \subseteq G_T$ be the local Galois group at v.

Let X/F be a smooth curve and let $\mathcal{X}/R$ be a model which is the complement of a smooth divisor in a smooth proper curve over R. Let b be an R-integral base point of $\mathcal{X}$, possibly tangential. Denote by $U^{\text{ét}} = U^{\text{ét}}(b)$ the $\mathbb{Q}_p$-pro-unipotent étale fundamental group of $X_{\overline{F}}$ with base point $b_{\overline{F}}$, and by $U^{\mathrm{dR}} = U^{\mathrm{dR}}(b)$ the de Rham fundamental group of X_{F_v} with base point b_{F_v}.

We have a Chabauty–Kim diagram as follows:

$$\begin{array}{ccccc}
\mathcal{X}(R) & \hookrightarrow & \mathcal{X}(R_v) & & \\
\downarrow{\scriptstyle j} & & \downarrow{\scriptstyle j_v} & \searrow^{j_{\mathrm{dR}}} & \\
H^1_f(G_T, U^{\text{ét}}(b))(\mathbb{Q}_p) & \xrightarrow[\mathrm{loc}_v]{} & H^1_f(G_v, U^{\text{ét}}(b))(\mathbb{Q}_p) & \xrightarrow[\log_{\mathrm{BK}}]{\sim} & (F^0\backslash U^{\mathrm{dR}}(b))(F_v).
\end{array}$$

Denote this diagram by $\mathrm{CK}(X,b)$. We want to prove the following:

Theorem B.1. *Given another curve $\mathcal{X}'/R$ as above with base point b', and given a finite morphism $f\colon \mathcal{X} \to \mathcal{X}'$ over R, then we have an induced morphism of Chabauty–Kim diagrams $f_*\colon \mathrm{CK}(X,b) \to \mathrm{CK}(X',b')$.*

Here, the induced morphism of Chabauty–Kim diagrams $f_*\colon \mathrm{CK}(X,b) \to \mathrm{CK}(X',b')$ consists of maps

$$\begin{aligned}
f_*\colon H^1_f(G_T, U^{\text{ét}}(b)) &\to H^1_f(G_T, U'^{\text{ét}}(b')) \text{ of } \mathbb{Q}_p\text{-schemes},\\
f_*\colon H^1_f(G_v, U^{\text{ét}}(b)) &\to H^1_f(G_v, U'^{\text{ét}}(b')) \text{ of } \mathbb{Q}_p\text{-schemes},\\
f_*\colon F^0\backslash U^{\mathrm{dR}}(b) &\to F^0\backslash U'^{\mathrm{dR}}(b') \text{ of } F_v\text{-schemes},
\end{aligned}$$

satisfying the following compatibilities which are expressed by the commutativity of squares:

- compatibility with the global Kummer map:

$$\begin{array}{ccc}
\mathcal{X}(R) & \xrightarrow{j} & H^1_f(G_T, U^{\text{ét}}(b))(\mathbb{Q}_p)\\
\downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f_*}\\
\mathcal{X}'(R) & \xrightarrow{j} & H^1_f(G_T, U'^{\text{ét}}(b'))(\mathbb{Q}_p)
\end{array} \tag{B.1}$$

- compatibility with the local Kummer map:

$$\begin{array}{ccc} \mathcal{X}(R_v) & \xrightarrow{j_v} & H^1_f(G_v, U^{\text{ét}}(b))(\mathbb{Q}_p) \\ \big\downarrow f & & \big\downarrow f_* \\ \mathcal{X}'(R_v) & \xrightarrow{j_v} & H^1_f(G_v, U'^{\text{ét}}(b'))(\mathbb{Q}_p) \end{array} \tag{B.2}$$

- compatibility with the de Rham Kummer map:

$$\begin{array}{ccc} \mathcal{X}(R_v) & \xrightarrow{j_{\text{dR}}} & (F^0\backslash U^{\text{dR}}(b))(F_v) \\ \big\downarrow f & & \big\downarrow f_* \\ \mathcal{X}'(R_v) & \xrightarrow{j_{\text{dR}}} & (F^0\backslash U'^{\text{dR}}(b'))(F_v) \end{array} \tag{B.3}$$

- compatibility with the localization map:

$$\begin{array}{ccc} H^1_f(G_T, U^{\text{ét}}(b)) & \xrightarrow{\text{loc}_v} & H^1_f(G_v, U^{\text{ét}}(b)) \\ \big\downarrow f_* & & \big\downarrow f_* \\ H^1_f(G_T, U'^{\text{ét}}(b')) & \xrightarrow{\text{loc}_v} & H^1_f(G_v, U'^{\text{ét}}(b')) \end{array} \tag{B.4}$$

- compatibility with the Bloch–Kato logarithm:

$$\begin{array}{ccc} H^1_f(G_v, U^{\text{ét}}(b)) & \xrightarrow{\log_{\text{BK}}} & \text{Res}_{F_v/\mathbb{Q}_p}(F^0\backslash U^{\text{dR}}(b)) \\ \big\downarrow f_* & & \big\downarrow f_* \\ H^1_f(G_v, U'^{\text{ét}}(b')) & \xrightarrow{\log_{\text{BK}}} & \text{Res}_{F_v/\mathbb{Q}_p}(F^0\backslash U'^{\text{dR}}(b')) \end{array} \tag{B.5}$$

Theorem B.1 is stated here for the full fundamental groups but it holds verbatim if one works instead with quotients along the descending central series.

The proof of Theorem B.1 breaks down into two steps:

(i) *Functoriality with respect to base-point-preserving maps.*
In other words: $f\colon \mathcal{X} \to \mathcal{X}'$ induces a morphism

$$f_*\colon \text{CK}(\mathcal{X}, b) \to \text{CK}(\mathcal{X}', f(b)).$$

(ii) *Change of base point:*
Given two R-integral base points b and c of $\mathcal{X}$, possibly tangential, there exists a natural isomorphism

$$t_{b,c}\colon \text{CK}(\mathcal{X}, b) \cong \text{CK}(\mathcal{X}, c).$$

The proof of Theorem B.1 follows by composing the two morphisms

$$\text{CK}(\mathcal{X}, b) \xrightarrow{f_*} \text{CK}(\mathcal{X}', f(b)) \cong \text{CK}(\mathcal{X}', b'),$$

where the first one is given by Step 1, and the second by Step 2.

B.1. **Torsors in Tannakian categories.** The three schemes in the bottom row of the Chabauty–Kim diagram are moduli spaces of torsors under various realizations of the fundamental group. An elegant way to define torsors under groups with extra structure uses the language of "algebraic geometry in a Tannakian category" [Del89, §5].

Let $\mathcal{T} = (\mathcal{T}, \otimes, 1)$ be a Tannakian category over some field k. A *ring in* $\mathcal{T}$ is a commutative monoid object of the ind-category ind-$\mathcal{T}$, i.e., an object A of ind-$\mathcal{T}$ together with a multiplication $A \otimes A \to A$ and a unit $1 \to A$ satisfying associativity, unit and commutativity conditions. Homomorphisms of rings in $\mathcal{T}$ are defined in the obvious way. Reversing arrows yields the category of *affine* $\mathcal{T}$*-schemes* (or *affine schemes in* $\mathcal{T}$), whose objects are denoted $\mathrm{Spec}(A)$ for A a ring in $\mathcal{T}$. An A*-module in* $\mathcal{T}$ is an object M in ind-$\mathcal{T}$ with a multiplication map $A \otimes M \to M$ satisfying an associativity and unit condition. Given an A-algebra B in $\mathcal{T}$ and an A-module M in $\mathcal{T}$, we can form the tensor product $B \otimes_A M = \mathrm{coker}(B \otimes A \otimes M \to B \otimes M)$, where the map is given by $b \otimes a \otimes m \mapsto ba \otimes m - b \otimes am$. This is a B-module in $\mathcal{T}$. If the functor $B \otimes_A -$ is exact (respectively, exact and faithful), B is called flat (respectively, faithfully flat) over A. The category of affine $\mathcal{T}$-schemes has fibre products, which are dual to tensor products of rings in $\mathcal{T}$. An *affine group scheme in* $\mathcal{T}$ is a group object of the category of affine $\mathcal{T}$-schemes, and it is clear how to define actions of affine group schemes in $\mathcal{T}$ on affine $\mathcal{T}$-schemes.

Definition B.2. Let $\mathcal{T}$ be a Tannakian category over a field k, let G be an affine group scheme in $\mathcal{T}$, and R a ring in $\mathcal{T}$. A G*-torsor* over R is a faithfully flat affine R-scheme P in $\mathcal{T}$ with a right group action $P \times G \to P$ over R such that the map $P \times G \to P \times_R P$, $(p, g) \mapsto (pg, p)$ is an isomorphism.

By taking sums of the unit object in $\mathcal{T}$, every k-vector space V gives rise to an object $V_{\mathcal{T}}$ of ind-T. For example, if $\mathcal{T}$ is the category of representations of an affine algebraic group over k on finite-dimensional k-vector spaces, then the functor $V \mapsto V_{\mathcal{T}}$ simply equips the vector space V with the trivial action.

As a consequence of the isomorphism $k \cong \mathrm{End}(1)$, the functor $\mathrm{Vect}(k) \to \mathcal{T}$, $V \mapsto V_{\mathcal{T}}$ is a k-linear, exact, fully faithful tensor functor. For every k-algebra R, we obtain a ring $R_{\mathcal{T}}$ in $\mathcal{T}$. Given an affine group scheme G in $\mathcal{T}$, we have a moduli functor on k-algebras whose R-valued points are the isomorphism classes of G-torsors over $R_{\mathcal{T}}$. By abuse of notation, we also call them G-torsors over R. In our cases of interest this moduli functor of G-torsors is representable by an affine k-scheme.

The three cases of interest in the context of the Chabauty–Kim method are the following (using the notation from above):

(i) $\mathcal{T} = \mathrm{Rep}_{\mathrm{cris}}(G_T)$ = continuous representations of G_T on finite-dimensional $\mathbb{Q}_p$-vector spaces, crystalline at v. This is a Tannakian category over $\mathbb{Q}_p$. The $\mathbb{Q}_p$-pro-unipotent étale fundamental group $U^{\text{ét}}$ is a pro-unipotent affine group scheme in this Tannakian category, and $U^{\text{ét}}$-torsors are parametrized by the global Selmer scheme $H^1_f(G_T, U^{\text{ét}})$.

(ii) $\mathcal{T} = \mathrm{Rep}_{\mathrm{cris}}(G_v)$ = crystalline continuous representations of G_v on finite-dimensional $\mathbb{Q}_p$-vector spaces. This is a Tannakian category over $\mathbb{Q}_p$; the $\mathbb{Q}_p$-pro-unipotent étale fundamental group $U^{\text{ét}}$ is also a pro-unipotent affine group scheme in this Tannakian category, and its torsors are parametrized by the local Selmer scheme $H^1_f(G_v, U^{\text{ét}})$.

(iii) $\mathcal{T} = \mathrm{MF}_K^{\varphi,\mathrm{adm}}$ = admissible filtered φ-modules over $K := F_v$. This is a Tannakian category over $\mathbb{Q}_p$. The crystalline fundamental group U^{cris}, equipped with its Frobenius and with the Hodge filtration coming from the comparison isomorphism with the de Rham fundamental group, is a pro-unipotent affine group scheme in $\mathrm{MF}_K^{\varphi,\mathrm{adm}}$. Torsors under it are parametrized by $\mathrm{Res}_{K/\mathbb{Q}_p}(F^0\backslash U^{\mathrm{dR}})$. This follows indirectly from the equivalence of categories $\mathrm{Rep}_{\mathrm{cris}}(G_K) \simeq \mathrm{MF}_K^{\varphi,\mathrm{adm}}$ from [Fon82, Théorème 5.2], and the isomorphism $H^1_f(G_K, U^{\text{ét}}) \cong \mathrm{Res}_{K/\mathbb{Q}_p}(F^0\backslash U^{\mathrm{dR}})$ from [Kim12, Proposition 1.4].

A more direct description of the bijection

$$(U^{\mathrm{cris}}\text{-torsors in } \mathrm{MF}_K^{\varphi,\mathrm{adm}} \text{ over } R)/\mathrm{iso} \cong (F^0\backslash U^{\mathrm{dR}})(R \otimes_{\mathbb{Q}_p} K)$$

for $\mathbb{Q}_p$-algebras R can be extracted from [Kim09, Proposition 1]: given a U^{cris}-torsor T in $\mathrm{MF}_K^{\varphi,\mathrm{adm}}$ over R, we can form the extension of scalars $T \otimes_{K_0} K$, where $K_0 \subseteq K$ is the fraction field of the Witt ring of the residue field of K. The K_0-semilinear Frobenius automorphism of T becomes a K-linear automorphism of $T \otimes_{K_0} K$ upon taking the f-th power, where f is the degree of the residue field of K over $\mathbb{Q}_p$. In this way, $T \otimes_{K_0} K$ becomes a torsor over $R \otimes_{\mathbb{Q}_p} K$ under the group $U^{\mathrm{cris}} \otimes_{K_0} K = U^{\mathrm{dR}}$. The torsor structure is compatible with the Hodge filtration and Frobenius and, moreover, $T \otimes_{K_0} K$ is admissible in the sense of loc. cit., i.e. admits separate trivializations with respect to the Hodge filtration and the Frobenius. There exist an element p^{H} in $F^0(T \otimes_{K_0} K)(R \otimes_{\mathbb{Q}_p} K)$ and a unique element p^{cr} in $(T \otimes_{K_0} K)(R \otimes_{\mathbb{Q}_p} K)^{\varphi=1}$, and the difference $u_T := (p^{\mathrm{H}})^{-1}p^{\mathrm{cr}}$ is the element of $(F^0\backslash U^{\mathrm{dR}})(R \otimes_{\mathbb{Q}_p} K)$ parametrizing the torsor T.[10]

Recall that for $\mathcal{T}$ a Tannakian category over a field k, a *fiber functor* on $\mathcal{T}$ with values in a k-algebra Λ is a k-linear exact tensor functor $\omega\colon \mathcal{T} \to \mathrm{Mod}(\Lambda)$. If $\Lambda \neq 0$, then ω is faithful [Del07, Cor. 2.10]. A fiber functor has a natural extension to the ind-category, $\omega\colon \text{ind-}\mathcal{T} \to \mathrm{Mod}(\Lambda)$. The extension is still a tensor functor, it sends rings in $\mathcal{T}$ to Λ-algebras, sends modules to modules, and is compatible with (relative) tensor products.

Lemma B.3. *Let $\mathcal{T}$ be a Tannakian category over k and let $A \to B$ be a homomorphism of rings in $\mathcal{T}$.*

(a) If there exist a nonzero k-algebra Λ and a fiber functor $\omega\colon \mathcal{T} \to \mathrm{Mod}(\Lambda)$ such that $\omega A \to \omega B$ is faithfully flat, then $A \to B$ is faithfully flat.

[10] See Remark A.3 on the difference of conventions concerning the left coset of $(p^{\mathrm{cr}})^{-1}p^{\mathrm{H}}$ versus the right coset of $(p^{\mathrm{H}})^{-1}p^{\mathrm{cr}}$ with respect to F^0U^{dR}.

(b) *Suppose that $A = R_{\mathcal{T}}$ for some k-algebra R. If $A \to B$ is faithfully flat, then $\omega A \to \omega B$ is faithfully flat for any k-algebra Λ and any fiber functor $\omega\colon \mathcal{T} \to \mathrm{Mod}(\Lambda)$.*

Proof. Let Λ be a nonzero k-algebra and ω a fiber functor on $\mathcal{T}$ with values in $\mathrm{Mod}(\Lambda)$ such that $\omega A \to \omega B$ is faithfully flat. For every A-module M in $\mathcal{T}$, we have a natural isomorphism

$$\omega B \otimes_{\omega A} \omega M \cong \omega(B \otimes_A M),$$

or equivalently, we have a 2-commutative square as follows:

$$\begin{array}{ccc} \mathrm{Mod}(A) & \xrightarrow{B\otimes_A -} & \mathrm{Mod}(B) \\ \downarrow{\scriptstyle \omega} & & \downarrow{\scriptstyle \omega} \\ \mathrm{Mod}(\omega A) & \xrightarrow{\omega B\otimes_{\omega A} -} & \mathrm{Mod}(\omega B). \end{array}$$

Since $\Lambda \neq 0$, the fiber functor ω is faithful, so the exactness and faithfulness of the functor $B \otimes_A -$ may be checked after composing with ω. Since both ω and, by assumption, the bottom horizontal map are exact and faithful, (a) follows.

For (b), suppose that $A = R_{\mathcal{T}}$, assume that $A \to B$ is faithfully flat and let ω be a fiber functor on $\mathcal{T}$ with values in a k-algebra Λ. We may assume $\Lambda \neq 0$. For a k-vector space V, we have $\omega(V_{\mathcal{T}}) = V \otimes_k \Lambda$. It follows that for $A = R_{\mathcal{T}}$ we have an isomorphism

$$\omega(A)_{\mathcal{T}} = (R \otimes_k \Lambda)_{\mathcal{T}} = R_{\mathcal{T}} \otimes \Lambda_{\mathcal{T}} = A \otimes \Lambda_{\mathcal{T}}$$

of rings in $\mathcal{T}$. Hence, if M is an ωA-module, then $M_{\mathcal{T}}$ is an $A \otimes \Lambda_{\mathcal{T}}$-module in $\mathcal{T}$. We obtain a 2-commutative diagram as follows:

$$\begin{array}{ccccc} \mathrm{Mod}(\omega A) & & \xrightarrow{\qquad\qquad\omega B\otimes_{\omega A} -\qquad\qquad} & & \mathrm{Mod}(\omega B) \\ \downarrow{\scriptstyle (-)_{\mathcal{T}}} & & & & \downarrow{\scriptstyle -\otimes_k \Lambda} \\ \mathrm{Mod}(A \otimes \Lambda_{\mathcal{T}}) & \xrightarrow{(B\otimes\Lambda_{\mathcal{T}})\otimes_{A\otimes\Lambda_{\mathcal{T}}} -} & \mathrm{Mod}(B \otimes \Lambda_{\mathcal{T}}) & \xrightarrow{\omega} & \mathrm{Mod}(\omega B \otimes_k \Lambda). \end{array}$$

We are claiming that the top horizontal functor is exact and faithful. Since $\Lambda \neq 0$, this may be checked after composing with the right vertical functor. Going the other way, we have a composition of $(-)_{\mathcal{T}}$, which is exact and (even fully) faithful, of $(B \otimes \Lambda_{\mathcal{T}}) \otimes_{A\otimes\Lambda_{\mathcal{T}}} -$, which is exact and faithful since $A \to B$ is faithfully flat by assumption, and the fiber functor ω which is exact and, since $\Lambda \neq 0$, also faithful. □

The two maps

$$H^1_f(G_T, U^{\text{ét}}(b))(\mathbb{Q}_p) \xrightarrow{loc_v} H^1_f(G_v, U^{\text{ét}}(b))(\mathbb{Q}_p) \xrightarrow{log_{BK}} (F^0\backslash U^{\mathrm{dR}}(b))(F_v)$$

arise from functors between the underlying Tannakian categories in the following way:

Lemma B.4. *Let $a\colon \mathcal{T}_1 \to \mathcal{T}_2$ be an exact k-linear tensor functor between Tannakian categories over a field k. Let G be an affine group scheme in $\mathcal{T}_1$ and P a G-torsor in $\mathcal{T}_1$ over a k-algebra R. Then $a(P)$ is an $a(G)$-torsor in $\mathcal{T}_2$ over R.*

Proof. Everything is clear except for $a(P)$ being faithfully flat over R (i.e., over $R_{\mathcal{T}_2}$). By the definition of a Tannakian category, there exist a nonzero k-algebra Λ and a fiber functor $\omega\colon \mathcal{T}_2 \to \mathrm{Mod}(\Lambda)$. The composition $\omega \circ a$ is then a fiber functor of $\mathcal{T}_1$. By Lemma B.3 (b), the map $\omega aP \to \omega a R_{\mathcal{T}_1} = \omega R_{\mathcal{T}_2}$ is faithfully flat. By Lemma B.3 (a), $aP \to R_{\mathcal{T}_2}$ is faithfully flat. □

Consider the two functors "localization at v" and "crystalline Dieudonné"

$$\mathrm{Rep}_{\mathrm{cris}}(G_T) \xrightarrow{loc_v} \mathrm{Rep}_{\mathrm{cris}}(G_v) \xrightarrow{D_{cris}} \mathrm{MF}_K^{\varphi,\mathrm{adm}}.$$

Both are exact $\mathbb{Q}_p$-linear tensor functors of Tannakian categories over $\mathbb{Q}_p$, so that Lemma B.4 applies. By Olsson's comparison theorem for the fundamental group, we have $D_{\mathrm{cris}}(U^{\text{ét}}) = U^{\mathrm{cris}}$. Hence, we obtain morphisms of moduli spaces of torsors under the étale and crystalline fundamental group:

$$H^1_f(G_T, U^{\text{ét}}) \xrightarrow{loc_v} H^1_f(G_v, U^{\text{ét}}) \xrightarrow{D_{cris}} \mathrm{Res}_{F_v/\mathbb{Q}_p}(F^0 \backslash U^{\mathrm{dR}}).$$

The bottom row of the Chabauty–Kim diagram is obtained by taking $\mathbb{Q}_p$-points.

B.2. **Contracted products of torsors.** The map of Chabauty–Kim diagrams which is functorially induced by a base-point-preserving morphism of curves, as well as the change-of-base point isomorphism which we are constructing, have an interpretation in terms of contracted products of torsors, as we are going to explain.

Let $\mathcal{T}$ be a Tannakian category over a field k. Let G be an affine group scheme in $\mathcal{T}$ which acts from the right on an affine $\mathcal{T}$-scheme X and from the left on a second affine $\mathcal{T}$-scheme Y.

Definition B.5. The *contracted product* $X \overset{G}{\times} Y$ is the quotient of the product $X \times Y$ by the right G-action given by $(x, y).g = (xg, g^{-1}y)$. More generally, if X and Y are affine $\mathcal{T}$-schemes over another affine $\mathcal{T}$-scheme S and G acts by S-morphisms, then $X \overset{G}{\times}_S Y$ is defined as the quotient of $X \times_S Y$ by the G-action. This relative contracted product is again an affine $\mathcal{T}$-scheme over S.

To see why $X \overset{G}{\times} Y$ exists as an affine $\mathcal{T}$-scheme, note that the contracted product is equivalently described as the coequalizer of the two maps $X \times G \times Y \rightrightarrows X \times Y$ given by $(x, g, y) \mapsto (xg, y)$ and $(x, g, y) \mapsto (x, gy)$, respectively. The underlying ring of the contracted product is thus given as an equalizer

$$\mathcal{O}(X \overset{G}{\times} Y) = \mathrm{eq}(\mathcal{O}(X) \otimes \mathcal{O}(Y) \rightrightarrows \mathcal{O}(X) \otimes \mathcal{O}(G) \otimes \mathcal{O}(Y)),$$

which exists as a ring in $\mathcal{T}$. The argument for the relative contracted product $X \overset{G}{\times}_S Y$ is similar.

Lemma B.6. *Let $a\colon \mathcal{T}_1 \to \mathcal{T}_2$ be an exact k-linear tensor functor between Tannakian categories. Then a preserves contracted products: if G is an affine group scheme in $\mathcal{T}_1$ acting on affine $\mathcal{T}_1$-schemes X/S from the right and Y/S from the left, then there is a natural isomorphism*

$$a(X \overset{G}{\times}_S Y) \cong aX \overset{aG}{\times}_{aS} aY.$$

Proof. The functor a preserves equalizers and tensor products. □

Lemma B.7. *Contracted products commute with flat base change: if $T \to S$ is a flat morphism of affine $\mathcal{T}$-schemes, G acts on X/S from the right and on Y/S from the left, then setting $X_T \coloneqq X \times_S T$ and $Y_T \coloneqq Y \times_S T$, the natural map is an isomorphism*

$$X_T \overset{G}{\times}_T Y_T \cong (X \overset{G}{\times}_S Y) \times_S T.$$

Proof. We have natural isomorphisms

$$\begin{aligned} X_T \overset{G}{\times}_T Y_T &= (X_T \times_T Y_T)/G \\ &= ((X \times_S Y) \times_S T)/G \\ &\to (X \times_S Y)/G \times_S T \\ &= (X \overset{G}{\times}_S Y) \times_S T. \end{aligned}$$

The arrow is an isomorphism because base change from affine S-schemes to affine T-schemes commutes with finite colimits by flatness. □

Assume that Y over S carries additionally a right action by another affine group scheme H in $\mathcal{T}$ which is compatible with the left G-action: $(gy)h = g(hy)$. Then the contracted product $X \overset{G}{\times}_S Y$ carries a well-defined right action of H by S-morphisms.

Proposition B.8. *In the situation above, assume that X/S is a G-torsor and Y/S is an H-torsor. Then the contracted product $X \overset{G}{\times}_S Y$ is again an H-torsor over S.*

Proof. Let $T \to S$ be faithfully flat such that X becomes the trivial G-torsor upon base change to T, i.e. $X_T \cong T \times G$ with canonical right G-action. One such choice is $T \coloneqq X$ by the definition of a torsor. The property of $X \overset{G}{\times}_S Y$ being an H-torsor can be checked after the faithfully flat base change to T. Using Lemma B.7, we have

$$(X \overset{G}{\times}_S Y) \times_S T = X_T \overset{G}{\times}_T Y_T \cong (T \times G) \overset{G}{\times}_T Y_T \cong Y_T$$

since taking the contracted product with the trivial G-torsor is the identity. Since Y is a torsor over S by assumption, Y_T is a torsor over T. □

Proposition B.9. *Let Q/S be a right H-torsor with compatible left G-action. Then the functor $P \mapsto P \overset{G}{\times}_S Q$ on G-torsors P/S commutes with base change along arbitrary morphisms $T \to S$.*

Proof. We have a well-defined morphism of H-torsors

$$P_T \overset{G}{\times}_T Q_T \to (P \overset{G}{\times}_S Q) \times_S T$$

given by $[(p,t),(q,t)] \mapsto ([p,q],t)$, where $P_T \coloneqq P \times_S T$ and $Q_T \coloneqq Q \times_S T$. Any morphism of torsors is automatically an isomorphism, as can be checked on a trivializing faithfully flat cover. □

As a special case of Proposition B.8, consider a homomorphism $f\colon G \to G'$ of affine group schemes in $\mathcal{T}$. Then $S \times G'$ is a trivial right G'-torsor over S and has a left action by G via f. By Proposition B.8, for every G-torsor P over S, the contracted product $P \overset{G}{\times}_S (S \times G') = P \overset{G}{\times} G'$ is a G'-torsor over S. Hence, f induces a functor

$$f_*\colon (G\text{-torsors over } S) \longrightarrow (G'\text{-torsors over } S)$$

given by $P \mapsto P \overset{G}{\times} G'$. It commutes with base change in S by Proposition B.9.

B.3. **Functoriality for base-point-preserving maps.** Consider an R-morphism $f\colon \mathcal{X} \to \mathcal{X}'$ as in Theorem B.1. This induces morphisms of fundamental groups $f_*\colon U^{\text{ét}}(b) \to U'^{\text{ét}}(f(b))$ (in the Tannakian categories $\mathrm{Rep}_{\text{cris}}(G_T)$ and $\mathrm{Rep}_{\text{cris}}(G_v)$) and $f_*\colon U^{\text{cris}}(b) \to U'^{\text{cris}}(f(b))$ (in the Tannakian category $\mathrm{MF}_{F_v}^{\varphi,\text{adm}}$). By the previous discussion, f_* induces morphisms between moduli spaces of torsors

$$f_*\colon H^1_f(G_T, U^{\text{ét}}(b)) \to H^1_f(G_T, U'^{\text{ét}}(f(b))),$$
$$f_*\colon H^1_f(G_v, U^{\text{ét}}(b)) \to H^1_f(G_v, U'^{\text{ét}}(f(b))),$$
$$f_*\colon \mathrm{Res}_{F_v/\mathbb{Q}_p}(F^0\backslash U^{\mathrm{dR}}(b)) \to \mathrm{Res}_{F_v/\mathbb{Q}_p}(F^0\backslash U'^{\mathrm{dR}}(f(b))).$$

By construction, the three maps are morphisms of $\mathbb{Q}_p$-schemes.

Proposition B.10. *The third morphism arises via Weil restriction from a morphism $f_*\colon F^0\backslash U^{\mathrm{dR}}(b) \to F^0\backslash U'^{\mathrm{dR}}(f(b))$ over F_v.*

Proof. According to [Kim09, Proposition 1], $F^0\backslash U^{\mathrm{dR}}$ is the moduli space over F_v of admissible U^{dR}-torsors (those with separate trivializations for the Hodge filtration and Frobenius automorphism). There is no Tannakian category over F_v such that admissible torsors can be described as torsors in this category. Nevertheless, given an admissible torsor P over an F_v-algebra Λ, we can form the contracted product $f_*(P) \coloneqq P \overset{U^{dR}(b))}{\times} U'^{\mathrm{dR}}(f(b))$, which is an admissible $U'^{\mathrm{dR}}(f(b))$-torsor over Λ. Its coordinate ring is given as an equalizer

$$\mathrm{eq}(\mathcal{O}(P) \otimes_{F_v} \mathcal{O}(U'^{\mathrm{dR}}(f(b))) \rightrightarrows \mathcal{O}(P) \otimes_{F_v} U^{\mathrm{dR}}(b) \otimes_{F_v} \mathcal{O}(U'^{\mathrm{dR}}(f(b))))$$

and carries an induced Hodge filtration and Frobenius automorphism. After identifying U^{cris}-torsors in $\mathrm{MF}_{F_v}^{\varphi,\mathrm{adm}}$ over $\mathbb{Q}_p$-algebras R with admissible U^{dR}-torsors over $R \otimes_{\mathbb{Q}_p} F_v$ (see (iii) at the end of section B.1), we have a 2-commutative diagram as follows:

$$\begin{array}{ccc}
(U^{\mathrm{cris}}(b)\text{-torsors over } R \text{ in } \mathrm{MF}_{F_v}^{\varphi,\mathrm{adm}}) & \xrightarrow{f_*} & (U'^{\mathrm{cris}}(f(b))\text{-torsors over } R \text{ in } \mathrm{MF}_{F_v}^{\varphi,\mathrm{adm}}) \\
\downarrow\simeq & & \downarrow\simeq \\
(\text{adm. } U^{\mathrm{dR}}(b)\text{-torsors over } R\otimes_{\mathbb{Q}_p} F_v) & \dashrightarrow^{f_*} & (\text{adm. } U'^{\mathrm{dR}}(f(b))\text{-torsors over } R\otimes_{\mathbb{Q}_p} F_v),
\end{array}$$

where the bottom horizontal functor is given by contracted products of admissible torsors. Since the latter functor is defined on all F_v-algebras (not just on those base changed from $\mathbb{Q}_p$), the map on moduli spaces is induced via Weil restriction from a map $f_*\colon F^0\backslash U^{\mathrm{dR}}(b) \to F^0\backslash U'^{\mathrm{dR}}(f(b))$ over F_v. □

Having constructed the three required maps for a morphism of Chabauty–Kim diagrams $\mathrm{CK}(\mathcal{X}, b) \to \mathrm{CK}(\mathcal{X}', f(b))$, it remains to show the compatibilities expressed by the commutative diagrams (B.1)–(B.5).

Proposition B.11. *The three maps above induced by $f\colon \mathcal{X} \to \mathcal{X}'$ satisfy the compatibilities* (B.1)–(B.5) *and hence define a morphism of Chabauty–Kim diagrams $f_*\colon \mathrm{CK}(\mathcal{X}, b) \to \mathrm{CK}(\mathcal{X}', f(b))$.*

Proof. The compatibility with the global (respectively, local) Kummer map amounts to an isomorphism of $U'^{\text{ét}}(f(b))$-torsors

$$P^{\text{ét}}(b,x) \overset{U^{\acute{e}t}(b)}{\times} U'^{\text{ét}}(f(b)) \cong P'^{\text{ét}}(f(b), f(x))$$

in $\mathrm{Rep}_{\mathrm{cris}}(G_T)$ (respectively, $\mathrm{Rep}_{\mathrm{cris}}(G_v)$) for every $x \in \mathcal{X}(R)$. There is a well-defined map $(\alpha, \gamma') \mapsto f_*(\alpha)\gamma'$. Being a morphism between torsors, it is automatically an isomorphism.

The compatibility with the de Rham Kummer map follows similarly from the isomorphism of $U'^{\mathrm{cris}}(f(b))$-torsors

$$P^{\mathrm{cris}}(b,x) \overset{U^{cris}(b)}{\times} U'^{\mathrm{cris}}(f(b)) \cong P'^{\mathrm{cris}}(f(b), f(x))$$

in $\mathrm{MF}_{F_v}^{\varphi,\mathrm{adm}}$.

The compatibilities with the localization map and the Bloch–Kato logarithm follow abstractly from the fact that the maps are given by mapping torsors along an exact $\mathbb{Q}_p$-linear tensor functor between the underlying Tannakian categories, and those functors preserve contracted products by Lemma B.6. □

This finishes the proof of the functoriality of the Chabauty–Kim diagram with respect to base-point-preserving maps.

B.4. **Change of base point.** Assume that c is a second R-integral base point of $\mathcal{X}$ (possibly tangential). We construct a canonical isomorphism of Chabauty–Kim diagrams $\mathrm{CK}(\mathcal{X},b)\cong\mathrm{CK}(\mathcal{X},c)$.

Consider the path space $P^{\text{ét}}(c,b)$ in $\mathrm{Rep}_{\mathrm{cris}}(G_T)$. It is a left $U^{\text{ét}}(b)$-torsor and a right $U^{\text{ét}}(c)$-torsor. Given a $\mathbb{Q}_p$-algebra R and a $U^{\text{ét}}(b)$-torsor P over R, the contracted product $P\overset{U^{ét}(b)}{\times}P^{\text{ét}}(c,b)$ is a $U^{\text{ét}}(c)$-torsor over R by Proposition B.8. The functor

$$(U^{\text{ét}}(b)\text{-torsors over } R)\to(U^{\text{ét}}(c)\text{-torsors over } R)$$

given by $P\mapsto P\overset{U^{ét}(b)}{\times}P^{\text{ét}}(c,b)$ is compatible with base change in R by Proposition B.9. Since we have an isomorphism

$$P^{\text{ét}}(c,b)\overset{U^{ét}(c)}{\times}P^{\text{ét}}(b,c)\cong U^{\text{ét}}(b),$$

the functor $P\mapsto P\overset{U^{ét}(b)}{\times}P^{\text{ét}}(c,b)$ is an equivalence with quasi-inverse given by taking the contracted product with $P^{\text{ét}}(b,c)$ under $U^{\text{ét}}(c)$. As a consequence, we obtain an isomorphism of moduli spaces of torsors

$$t_{b,c}\colon H^1(G_T,U^{\text{ét}}(b))\cong H^1(G_T,U^{\text{ét}}(c)).$$

The same construction for $U^{\text{ét}}(b)$-torsors in $\mathrm{Rep}_{\mathrm{cris}}(G_v)$ and for $U^{\mathrm{cris}}(b)$-torsors in $\mathrm{MF}_{F_v}^{\varphi,\mathrm{adm}}$ yields analogous change-of-base point isomorphisms

$$t_{b,c}\colon H^1(G_v,U^{\text{ét}}(b))\cong H^1(G_v,U^{\text{ét}}(c)),$$
$$t_{b,c}\colon \mathrm{Res}_{F_v/\mathbb{Q}_p}(F^0\backslash U^{\mathrm{dR}}(b))\cong\mathrm{Res}_{F_v/\mathbb{Q}_p}(F^0\backslash U^{\mathrm{dR}}(c)).$$

Proposition B.12. *The last change-of-base point isomorphism is induced via Weil restriction by an isomorphism over F_v:*

$$t_{b,c}\colon F^0\backslash U^{\mathrm{dR}}(b)\cong F^0\backslash U^{\mathrm{dR}}(c). \tag{B.6}$$

Proof. As in the proof of Proposition B.10, we can interpret $F^0\backslash U^{\mathrm{dR}}(b)$ as the moduli space of admissible $U^{\mathrm{dR}}(b)$-torsors over F_v-algebras in the sense of [Kim09]. The contracted product operation $P\mapsto P\overset{U^{dR}(b)}{\times}P^{\mathrm{dR}}(c,b)$ is defined for admissible $U^{\mathrm{dR}}(b)$-torsors over all F_v-algebras (not only those base changed from $\mathbb{Q}_p$). This implies the claim. □

We have constructed the three maps required for an isomorphism of Chabauty–Kim diagrams $\mathrm{CK}(\mathcal{X},b)\cong\mathrm{CK}(\mathcal{X},c)$. It remains to show:

Proposition B.13. *The three maps constructed above satisfy the compatibilities* (B.1)–(B.5) *and hence define a canonical change-of-base point isomorphism $t_{b,c}\colon\mathrm{CK}(\mathcal{X},b)\cong\mathrm{CK}(\mathcal{X},c)$.*

Proof. The compatibility with the global (respectively, local) Kummer map amounts to the isomorphism of $U^{\text{ét}}(c)$-torsors

$$P^{\text{ét}}(b,x)\overset{U^{ét}(b)}{\times}P^{\text{ét}}(c,b)\cong P^{\text{ét}}(c,x)$$

in $\mathrm{Rep}_{\mathrm{cris}}(G_T)$ (respectively, $\mathrm{Rep}_{\mathrm{cris}}(G_v)$).

The compatibility with the de Rham Kummer map follows similarly from the isomorphism of $U^{\mathrm{cris}}(c)$-torsors

$$P^{\mathrm{cris}}(b,x) \overset{U^{cris}(b)}{\times} P^{\mathrm{cris}}(c,b) \cong P^{\mathrm{cris}}(c,x)$$

in $\mathrm{MF}_{F_v}^{\varphi,\mathrm{adm}}$.

The compatibilities with the localization map and the Bloch–Kato logarithm follow abstractly from the fact that the maps are given by mapping torsors along an exact $\mathbb{Q}_p$-linear tensor functor between the underlying Tannakian categories, and those functors preserve contracted products by Lemma B.6. □

This finishes the proof of the change-of-base point isomorphism and hence the proof of Theorem B.1.

B.5. **De Rham functoriality in coordinates.** We now want to consider in more detail the functoriality map on de Rham fundamental groups. Coordinate functions on U^{dR} are given by iterated integrals over de Rham loops, and we seek a description of the map $f_*\colon F^0\backslash U^{\mathrm{dR}}(b) \to F^0\backslash U'^{\mathrm{dR}}(b')$ induced by a morphism $f\colon \mathcal{X} \to \mathcal{X}'$ in terms of those iterated integral coordinates. Since this concerns only the local picture, we work over any finite extension K of $\mathbb{Q}_p$ (such as the completion F_v of a number field at a p-adic valuation) and assume that X is a smooth curve over K. It is clear that the considerations over the local field F_v above remain true in this setting.

Recall the following Tannakian definition of iterated integrals:

Definition B.14. Let $x, y \in X(K)$, let $\gamma \in P^{\mathrm{dR}}(x,y)(K)$ be a de Rham path and let $w = \omega_1 \cdots \omega_r$ be a word of regular differential forms $\omega_i \in H^0(X, \Omega^1_X)$ on X. Let $V(w)$ be the trivial vector bundle $\mathcal{O}_X^{r+1}$, endowed with the unipotent flat connection

$$\nabla = d - \begin{pmatrix} 0 & \omega_1 & & \\ & \ddots & \ddots & \\ & & \ddots & \omega_r \\ & & & 0 \end{pmatrix}.$$

The iterated integral

$$\int_\gamma \omega_1 \cdots \omega_r \in K$$

is defined as the top-right matrix coefficient of the linear map

$$K^{r+1} = V(w)_x \xrightarrow{\gamma} V(w)_y = K^{r+1}.$$

The definition generalizes to tangential end points as follows: write $X = \overline{X} \setminus D$ with the smooth compactification $\overline{X}$ and boundary divisor D. If x or y are K-rational tangent vectors at a point at infinity rather than points in $X(K)$, it follows from the definition of the de Rham fiber functor at a

tangential base point that we still have canonical isomorphisms $V(w)_x \cong K^{r+1} \cong V(w)_y$ provided that the differential forms $\omega_1, \dots, \omega_r$ appearing in w have at most simple poles at these points (see [BF06, §3–4] for details). In particular, the iterated integral $\int_\gamma \omega_1 \cdots \omega_r$ is defined for $\omega_1, \dots, \omega_r \in H^0(X, \Omega^1_X(D))$ even when the end points of γ are tangential points, which we henceforth allow.

The definition of iterated integrals generalizes moreover to de Rham paths $\gamma \in P^{\mathrm{dR}}(x,y)(\Lambda)$ with values in any K-algebra Λ. Thus, the word $w = \omega_1 \cdots \omega_r$ defines an element of the coordinate ring

$$I_{x,y}(w) \in \mathcal{O}(P^{\mathrm{dR}}(x,y)),$$

given by $\gamma \mapsto \int_\gamma w$. In the case $x = y$ we also write $I_x \coloneqq I_{x,x}$. By linear extension, the map $w \mapsto I_{x,y}(w)$ induces a homomorphism

$$I_{x,y} \colon \mathrm{T}_{\sqcup\!\sqcup} H^0(X, \Omega^1_X(D)) \to \mathcal{O}(P^{\mathrm{dR}}(x,y)) \tag{B.7}$$

of K-algebras, where $\mathrm{T}_{\sqcup\!\sqcup} H^0(X, \Omega^1_X(D))$ denotes the tensor algebra on $H^0(X, \Omega^1_X(D))$ with multiplication given by the shuffle product.

Proposition B.15. *The homomorphism $I_{x,y} \colon \mathrm{T}_{\sqcup\!\sqcup} H^0(X, \Omega^1_X(D)) \to \mathcal{O}(P^{\mathrm{dR}}(x,y))$ is filtered with respect to the length filtration on the shuffle algebra and the Hodge filtration on the de Rham path space.*

Proof. Let V_{dR} denote the universal pro-unipotent vector bundle with flat logarithmic connection on $(\overline{X}, D)$, as in [Had11, Theorem 2.1] (where it is denoted $\mathcal{P}_{\mathrm{dR}}$). That is, there is a point $e_x \in V_{\mathrm{dR},x}$ such that (V_{dR}, e_x) pro-represents the functor ω_x^{dR} from unipotent vector bundles with flat logarithmic connection on $(\overline{X}, D)$ to K-vector spaces given by taking the fibre at x. There is a canonical cocommutative coalgebra structure on V_{dR} whose comultiplication $\Delta \colon V_{\mathrm{dR}} \to V_{\mathrm{dR}} \hat{\otimes} V_{\mathrm{dR}}$ and counit $\varepsilon \colon V_{\mathrm{dR}} \to \mathcal{O}_X$ are uniquely determined by the fact that $\Delta(e_x) = e_x \hat{\otimes} e_x$ and $\varepsilon(e_x) = 1$ ($\hat{\otimes}$ here is the natural tensor product on pro-unipotent vector bundles with flat logarithmic connection). So the dual $V_{\mathrm{dR}}^\vee$ is a commutative algebra object in the category of ind-unipotent vector bundles with logarithmic connection on $(\overline{X}, D)$.

For any second K-rational point or tangential point y, the fibre $V_{\mathrm{dR},y}^\vee$ is canonically isomorphic to $\mathcal{O}(P^{\mathrm{dR}}(x,y))$ as commutative K-algebras. This isomorphism can be described explicitly as follows. Given a commutative K-algebra Λ, the isomorphism $P^{\mathrm{dR}}(x,y)(\Lambda) \cong \mathrm{Spec}(V_{\mathrm{dR},y})(\Lambda)$ sends a $\otimes$-natural isomorphism $\gamma \colon \omega_{x,\Lambda}^{\mathrm{dR}} \xrightarrow{\sim} \omega_{y,\Lambda}^{\mathrm{dR}}$ to the K-algebra homomorphism $f_\gamma \colon V_{\mathrm{dR},y}^\vee \to \Lambda$ given by $f_\gamma(\psi) = (1_\Lambda \otimes \psi)(\gamma_{V_{\mathrm{dR}}}(e_x)) \in \Lambda$. There is a Hodge filtration on V_{dR} described in [Had11, Lemma 3.6][11], and the Hodge filtration on $\mathcal{O}(P^{\mathrm{dR}}(x,y))$ is, by definition, the induced filtration on the fibre $V_{\mathrm{dR},y}^\vee$.

[11] There is a minor mistake in the statement of [Had11, Lemma 3.6]. Specifically, in order to ensure uniqueness of the filtration, one should add to the list of conditions the requirement that $e_x \in F^0 V_{\mathrm{dR},x}$. This does not automatically follow from the other conditions, as claimed in [Had11].

Now suppose that $\omega_1, \dots, \omega_r \in H^0(X, \Omega^1_{\overline{X}}(D))$ are logarithmic 1-forms on the curve X. The unipotent vector bundle with flat connection $V(w) = \mathcal{O}_X^{r+1}$ on X from Definition B.14 extends to a unipotent vector bundle with logarithmic flat connection on $\overline{X}$ in an obvious way. Denote this extension again by $V(w)$. Its underlying vector bundle is trivial: $V(w) = \mathcal{O}_{\overline{X}}^{r+1}$. We endow $V(w)$ with the decreasing filtration $F^\bullet$ where $F^{-i}V(w) = \mathcal{O}_{\overline{X}}^{i+1}$ is the span of the last $i+1$ basis vectors for $0 \leq i \leq r$, and $F^1 = 0$. This filtration is Griffiths-transverse, so by [Had11, Proposition 3.7][12] there is a unique morphism $\phi_w \colon V_{\mathrm{dR}} \to V(w)$ which is compatible with connections and filtrations and takes e_x to the point $(0, \dots, 0, 0, 1) \in K^{r+1} = V(w)_x$. The element $I_{x,y}(w) \in \mathcal{O}(P^{\mathrm{dR}}(x,y))$ corresponds under the isomorphism $\mathcal{O}(P^{\mathrm{dR}}(x,y)) \cong V_{\mathrm{dR},y}^\vee$ to the functional $V_{\mathrm{dR},y} \to K$ given as the composite

$$V_{\mathrm{dR},y} \xrightarrow{\phi_{w,y}} V(w)_y = K^{r+1} \to K$$

where the second of these maps is the projection onto the first factor. The first of these maps is filtered since ϕ_w is, and the second of these maps is filtered of degree r by construction. Hence we see that $I_{x,y}(w) \in F^r\mathcal{O}(P^{\mathrm{dR}}(x,y))$, which is what we wanted to show. □

Remark B.16. There is a subtle technical point regarding our use of Hadian's definition of the Hodge filtration in the above proof. The original literature on the Chabauty–Kim method uses an earlier definition of the Hodge filtration on the fundamental group due to Wojtkowiak [Woj93], and it appears that there is no published proof that these two definitions are equivalent. Nonetheless, it is possible to set up the Chabauty–Kim method using Hadian's definition in place of Wojtkowiak's; see [Bet, Remark 4.2.2].

Now assume that we have a model $\mathcal{X}/R$ of X over the valuation ring R of K which is the complement of a smooth divisor in a smooth compactification. Given two R-integral base points b and c (possibly tangential) we want to describe the change-of-base point isomorphism

$$t_{b,c} \colon F^0\backslash U^{\mathrm{dR}}(b) \cong F^0\backslash U^{\mathrm{dR}}(c)$$

from Proposition B.12 in terms coordinates given by iterated integrals.

We have the following description of the change-of-base point isomorphism (B.6):

Proposition B.17. *Let p^{H} be a path in $(F^0P^{\mathrm{dR}}(c,b))(K)$ and let $p^{\mathrm{cr}} \in (P^{\mathrm{dR}}(c,b))(K)^{\phi=1}$ be the unique Frobenius-invariant path. The change of base point isomorphism $t_{b,c} \colon F^0\backslash U^{\mathrm{dR}}(b) \cong F^0\backslash U^{\mathrm{dR}}(c)$ is given by*

$$\gamma \mapsto (p^{\mathrm{H}})^{-1}\gamma p^{\mathrm{cr}}.$$

[12] There are two minor mistakes in the statement of [Had11, Proposition 3.7]. Firstly, the word "strictly" should be removed from the statement. Secondly, [Had11, Proposition 3.7] only holds for those filtered objects which are iterated strict extensions of constant vector bundles with shifts of the trivial filtration: this is slightly more restrictive than the notion of filtered object used in [Had11].

Proof. Let Λ be a K-algebra and let $\gamma \in (U^{\mathrm{dR}}(b))(\Lambda)$. For notational simplicity, we consider only $\Lambda = K$. The admissible $U^{\mathrm{dR}}(b)$-torsor represented by $[\gamma] \in (F^0\backslash U^{\mathrm{dR}}(b))(K)$ is given by $U^{\mathrm{dR}}(b)$ itself with the usual Hodge filtration, but equipped with the twisted Frobenius automorphism

$$\phi_\gamma(\alpha) \coloneqq \gamma\phi(\gamma^{-1}\alpha).$$

Denote this torsor by $U^{\mathrm{dR}}(b)_\gamma$. Twisting $U^{\mathrm{dR}}(b)_\gamma$ by the path torsor $P^{\mathrm{dR}}(c,b)$ results in the path torsor itself with unchanged Hodge filtration but with Frobenius similarly twisted. Denote this torsor by $P^{\mathrm{dR}}(c,b)_\gamma$. The path p^{H} is contained in $(F^0P^{\mathrm{dR}}(c,b)_\gamma)(K)$ because the Hodge filtration on $F^0P^{\mathrm{dR}}(c,b)_\gamma$ agrees with that on $F^0P^{\mathrm{dR}}(c,b)$. The unique element of $P^{\mathrm{dR}}(c,b)_\gamma$ which is invariant under the twisted Frobenius ϕ_γ is given by γp^{cr}. The element of $(F^0\backslash U^{\mathrm{dR}}(c))(K)$ representing $P^{\mathrm{dR}}(c,b)_\gamma$ is the difference of those two paths, namely $(p^{\mathrm{H}})^{-1}\gamma p^{\mathrm{cr}}$, as claimed. □

Recall that the Coleman integral from b to c over a word of differential forms is defined as the iterated integral along the unique Frobenius-invariant path $p^{\mathrm{cr}}(b,c) \in P^{\mathrm{dR}}(b,c)(K)^{\phi=1}$:

$$\int_b^c w \coloneqq \int_{p^{\mathrm{cr}}(b,c)} w.$$

Proposition B.18. *Let w be a word of logarithmic differential forms on X. Then the pullback of $I_c(w)$ along the isomorphism $t_{b,c}\colon F^0\backslash U^{\mathrm{dR}}(b) \cong F^0\backslash U^{\mathrm{dR}}(c)$ from Proposition B.12 is given by*

$$t_{b,c}^\sharp(I_c(w)) = \sum_{w=w_1w_2} I_b(w_1)\Big(\int_c^b w_2\Big).$$

Proof. According to Proposition B.17, the isomorphism $t_{b,c}$ is given by $t_{b,c} = (p^{\mathrm{H}})^{-1}(-)p^{\mathrm{cr}}$ with the Frobenius-invariant path $p^{\mathrm{cr}} \in P^{\mathrm{dR}}(c,b)(K)^{\phi=1}$ and any Hodge path $p^{\mathrm{H}} \in F^0P^{\mathrm{dR}}(c,b)(K)$. Consider a loop $\gamma \in U^{\mathrm{dR}}(b)(\Lambda)$ for some K-algebra Λ. We calculate:

$$\begin{aligned}
t_{b,c}^\sharp(I_c(w))(\gamma) &= I_c(w)(t_{b,c}(\gamma)) \\
&= I_c(w)((p^{\mathrm{H}})^{-1}\gamma p^{\mathrm{cr}}) \\
&= \int_{(p^{\mathrm{H}})^{-1}\gamma p^{\mathrm{cr}}} w \\
&= \sum_{w=w_0w_1w_2} \Big(\int_{(p^{\mathrm{H}})^{-1}} w_0\Big)\Big(\int_\gamma w_1\Big)\Big(\int_{p^{\mathrm{cr}}} w_2\Big) \\
&= \sum_{w=w_1w_2} \Big(\int_\gamma w_1\Big)\Big(\int_{p^{\mathrm{cr}}} w_2\Big) \\
&= \sum_{w=w_1w_2} I_b(w_1)(\gamma)\Big(\int_c^b w_2\Big).
\end{aligned}$$

Here we have used the path composition formula for iterated integrals, the fact that the inverse of a Hodge path from c to b is a Hodge path in the opposite direction, and Proposition B.15 according to which we have $I_{b,c}(w_0) \in F^1\mathcal{O}(P^{\mathrm{dR}}(b,c))$ whenever w_0 has length at least 1, so that the integral of w_0 over a Hodge path vanishes. □

Combining the base-point-preserving functoriality with the change-of-base point isomorphism, we obtain the following formula to express the functoriality of $F^0\backslash U^{\mathrm{dR}}$ in terms of iterated integral coordinates.

Theorem B.19. *Let K be a finite extension of $\mathbb{Q}_p$ and let X/K be a smooth curve. Let $\mathcal{X}/R$ be a model of X over the valuation ring which is the complement of a smooth divisor in a smooth compactification. Let b be an R-integral base point of $\mathcal{X}$ (possibly tangential). Let $(\mathcal{X}', b')$ be a second such curve and let $f\colon \mathcal{X} \to \mathcal{X}'$ be a finite morphism of R-schemes. Let $w = \omega_1 \cdots \omega_r$ be a word of logarithmic differential forms on X'. Then the pullback of $I_{b'}(w)$ along the map $f_*\colon F^0\backslash U^{\mathrm{dR}}(b) \to F^0\backslash U'^{\mathrm{dR}}(b')$ functorially induced by f is given by*

$$f_*^\sharp(I_{b'}(w)) = \sum_{w=w_1w_2} I_b(f^*w_1)\Big(\int_{b'}^{f(b)} f^*w_2\Big).$$

Proof. Let $\gamma \in U^{\mathrm{dR}}(b)(\Lambda)$ for some K-algebra Λ. By the definition of the functoriality map, we have $f_*(\gamma) = t_{f(b),b'}(f(\gamma))$. Using Proposition B.18, we calculate:

$$\begin{aligned} f_*^\sharp(I_{b'}(w))(\gamma) &= \sum_{w=w_1w_2} \Big(\int_{f(\gamma)} w_1\Big)\Big(\int_{b'}^{f(b)} f^*w_2\Big) \\ &= \sum_{w=w_1w_2} \Big(\int_{\gamma} f^*w_1\Big)\Big(\int_{b'}^{f(b)} f^*w_2\Big) \\ &= \sum_{w=w_1w_2} I_b(f^*w_1)\Big(\int_{b'}^{f(b)} f^*w_2\Big). \end{aligned}$$

□

References

[Bal+18] Jennifer S. Balakrishnan, Ishai Dan-Cohen, Minhyong Kim, and Stefan Wewers. "A non-abelian conjecture of Tate–Shafarevich type for hyperbolic curves". In: *Mathematische Annalen* 372.1-2 (2018), pp. 369–428.

[BD19] L. Alexander Betts and Netan Dogra. *The local theory of unipotent Kummer maps and refined Selmer schemes*. 2019. arXiv: 1909.05734 [math.NT].

[BDJ08] Amnon Besser and Rob De Jeu. "$Li^{(p)}$ -Service? An Algorithm for Computing p-Adic Polylogarithms". In: *Mathematics of Computation* 77.262 (2008), pp. 1105–1134. ISSN: 0025-5718. URL: https://www.jstor.org/stable/40234548 (visited on 03/10/2019).

[Bes02a] Amnon Besser. "Coleman integration using the Tannakian formalism". In: *Mathematische Annalen* 322.1 (2002), pp. 19–48.

[Bes02b] Amnon Besser. "Finite and p-adic Polylogarithms". In: *Compositio Mathematica* 130.2 (2002), pp. 215–223. ISSN: 1570-5846, 0010-437X. DOI: 10.1023/A:1013727116183. URL: http://www.cambridge.org/core/journals/compositio-mathematica/article/finite- (visited on 03/30/2019).

[Bet] L. Alexander Betts. *Weight filtrations on Selmer schemes and the effective Chabauty–Kim method*. arXiv: 2106.01218 [math.NT].

[Bet17] L. Alexander Betts. *The motivic anabelian geometry of local heights on abelian varieties*. 2017. arXiv: 1706.04850 [math.NT].

[BF06] Amnon Besser and Hidekazu Furusho. "The double shuffle relations for p-adic multiple zeta values". In: *Primes and knots*. Vol. 416. Contemp. Math. Amer. Math. Soc., Providence, RI, 2006, pp. 9–29. DOI: 10.1090/conm/416/07884.

[CDC20] David Corwin and Ishai Dan-Cohen. "The polylog quotient and the Goncharov quotient in computational Chabauty-Kim theory I". In: *International Journal of Number Theory* 16 (2020), pp. 1859–1905.

[DCW14] Ishai Dan-Cohen and Stefan Wewers. *The Heisenberg coboundary equation: appendix to Explicit Chabauty-Kim theory*. 2014. arXiv: 1403.4414 [math.NT].

[DCW15] Ishai Dan-Cohen and Stefan Wewers. "Explicit Chabauty–Kim theory for the thrice punctured line in depth 2". In: *Proceedings of the London Mathematical Society* 110.1 (2015), pp. 133–171.

[DCW16] Ishai Dan-Cohen and Stefan Wewers. "Mixed Tate motives and the unit equation". In: *International Mathematics Research Notices. IMRN* 17 (2016), pp. 5291–5354. ISSN: 1073-7928. DOI: 10.1093/imrn/rnv239. URL: https://doi-org.ezproxy.bu.edu/10.1093/imrn/rnv239.

[Del07] Pierre Deligne. "Catégories tannakiennes". In: *The Grothendieck Festschrift: A Collection of Articles Written in Honor of the 60th Birthday of Alexander Grothendieck*. Ed. by Pierre Cartier et al. Boston, MA: Birkhäuser Boston, 2007, pp. 111–195. ISBN: 978-0-8176-4575-5. DOI: 10.1007/978-0-8176-4575-5_3.

[Del89] Pierre Deligne. "Le groupe fondamental de la droite projective moins trois points". In: *Galois groups over* **Q**. Vol. 16. Math. Sci. Res. Inst. Publ. Springer, New York, 1989, pp. 79–297. DOI: 10.1007/978-1-4613-9649-9_3.

[Fon82] Jean-Marc Fontaine. "Sur Certains Types de Representations p-adiques du Groupe de Galois d'un Corps Local; Construction d'un Anneau de Barsotti–Tate". In: *Annals of Mathematics* 115.3 (1982), pp. 529–577. ISSN: 0003486X.

[Fon94] Jean-Marc Fontaine. "Exposé III : Représentations p-adiques semi-stables". fr. In: *Périodes p-adiques - Séminaire de Bures, 1988*. Ed. by Jean-Marc Fontaine. Astérisque 223. Société mathématique de France, 1994, pp. 113–184. URL: http://www.numdam.org/item/AST_1994__223__113_0.

[Fur07] Hidekazu Furusho. "p-Adic Multiple Zeta Values II. Tannakian Interpretations". In: *American Journal of Mathematics* 129.4 (2007), pp. 1105–1144. ISSN: 00029327, 10806377.

[Had11] Majid Hadian. "Motivic fundamental groups and integral points". In: *Duke Mathematical Journal* 160.3 (Dec. 2011), pp. 503–565. DOI: 10.1215/00127094-1444296. URL: https://doi.org/10.1215/00127094-1444296.

[Kim05] Minhyong Kim. "The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel". In: *Inventiones mathematicae* 161.3 (2005), pp. 629–656.

[Kim09] Minhyong Kim. "The unipotent Albanese map and Selmer varieties for curves". In: *Kyoto University. Research Institute for Mathematical Sciences. Publications* 45.1 (2009), pp. 89–133. ISSN: 0034-5318. DOI: 10.2977/prims/1234361156.

[Kim12] Minhyong Kim. "Tangential localization for Selmer varieties". In: *Duke Mathematical Journal* 161 (Feb. 2012), pp. 173–199. DOI: 10.1215/00127094-1507332. URL: https://doi.org/10.1215/00127094-1507332.

[KLS21] Theresa Kumpitsch, Martin Lüdtke, and Elie Studnia. *dcw_coefficients: SAGE code for computing Dan-Cohen–Wewers coefficients*. Version v1.0. 2021. DOI: 10.5281/zenodo.4850371. URL: https://doi.org/10.5281/zenodo.4850371.

[Mil71] John Milnor. *Introduction to algebraic K-theory*. 72. Princeton University Press, 1971.

[Ols11] Martin Olsson. "Towards Non-Abelian p-adic Hodge Theory in the Good Reduction Case". In: *Memoirs of the American Mathematical Society* 210.990 (2011). DOI: 10.1090/S0065-9266-2010-00625-2.

[Sak17] Kenji Sakugawa. "On a non-abelian generalization of the Bloch–Kato exponential map". In: *Mathematical journal of Okayama University* 59 (2017), pp. 41–70.

[Ser94] Jean-Pierre Serre. *Cohomologie galoisienne*. Fifth. Vol. 5. Lecture Notes in Math. Springer-Verlag, Berlin, 1994. ISBN: 3-540-58002-6. DOI: 10.1007/BFb0108758.

[Woj93] Zdzisław Wojtkowiak. "Cosimplicial Objects in Algebraic Geometry". In: *Algebraic K-Theory and Algebraic Topology*. Ed. by P.G. Goerss and J.F. Jardine. Vol. 47. NATO ASI Series. Springer Dordrecht, 1993, pp. 287–327.

Mathematics and Statistics Department, Boston University, Boston, MA 02215, USA
Email address: alexjbest@gmail.com
Email address: angusmca@bu.edu

Mathematics Department, Harvard University, Cambridge, MA 02138, USA
Email address: abetts@math.harvard.edu
Email address: yujiex@math.harvard.edu

Institut für Mathematik, Goethe–Universität Frankfurt, Robert-Mayer-Strasse 6–8, 60325
Email address: kumpitsch@math.uni-frankfurt.de
Email address: luedtke@math.uni-frankfurt.de

Department of Mathematics Building 380, Stanford University, Stanford, CA 94305
Email address: lqian@stanford.edu

Ecole Normale Supérieure, 75005 Paris
Email address: studnia@clipper.ens.fr