FROM CHABAUTY'S METHOD TO KIM'S NON-ABELIAN CHABAUTY'S METHOD

DAVID CORWIN

Contents

This is a draft, so comments (especially on the exposition) and corrections are welcome!

In 1922, Mordell conjectured that every hyperbolic curve has finitely many rational points. The first major progress on this conjecture came from Chabauty in 1941 ([Cha41]). His method, based on an earlier method of Skolem for integral points on non-proper curves, used p-adic analysis to prove finiteness for all curves satisfying a somewhat restrictive condition. While Faltings proved Mordell's conjecture in general in 1983, his proof was not effective. At the same time, Chabauty's method gained a newfound importance when Coleman ([Col85])

Date: August 23, 2021.

showed how to make it effective using his newly developed theory of p-adic integration. This allowed him and others to provably compute the set of rational points on specific curves, and prove general bounds for the number of rational points.

At the same time, Coleman's method worked only for curves satisfying Chabauty's condition. In 2004, Minhyong Kim ([Kim05]) showed how to extend Chabauty's method to prove Siegel's theorem for S-integral points on $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ by making use of non-abelian quotients of its fundamental group. Kim's new method points to a general method for attempting to provably finding the set of rational points on higher genus curves, and some progress has already been made (see especially [BDM+19], the first instance in which Kim's method led to a previously unknown concrete result).

In this article, we explain how Kim's method is a natural generalization of the classical Chabauty-Skolem method.

Notation. For a scheme Y, we let $\mathcal{O}(Y)$ denote its coordinate ring. If R is a ring, we let $Y \otimes R$ or Y_R denote the product (or 'base-change') $Y \times \operatorname{Spec} R$. If Y and $\operatorname{Spec} R$ are over an implicit base scheme S (often $\operatorname{Spec} \mathbb{Q}$), we take the product over S. Similarly, if M is a linear object (such as a module, an algebra, a Lie algebra, or a Hopf algebra), then M_R denotes $M \otimes R$ (again, with the tensor product taken over an implicit base ring, usually $\mathbb{Z}$ or $\mathbb{Z}_p$).

If K is a number field, we let Σ_K denote the set of places of K. If v is a place of K, then K_v denotes the completion of K at v, and if v is a finite place, then $\mathcal{O}_v$ denotes the integer ring of K_v. We say that Z is a ring of S-integers if there is some elements $\alpha \in \mathcal{O}_K$ for which $Z = \mathcal{O}_K[1/\alpha]$. If v is a finite place not dividing α, we write $Z_v = \mathcal{O}_v$.

If A is an abelian group and M a topological space, we denote by $\underline{A}$ the constant sheaf on M with stalk A.

Acknowledgements. Thanks to Bjorn Poonen for some corrections and suggestions.

1. Classical Chabauty-Coleman-Skolem

1.1. **Chabauty's Method.** We recommend [MP12] as a great introduction to Chabauty's method and Coleman's effective version of it. Nonetheless, we give a shorter introduction here, both for completeness and to set some notation.

Let X be a smooth proper hyperbolic curve over a number field K, and let $\mathfrak{p}$ be a finite place of K that is totally split over $\mathbb{Q}$ and such that X has good reduction at $\mathfrak{p}$. Then $K_{\mathfrak{p}} \cong \mathbb{Q}_p$, and X admits a smooth proper model over $Z_{\mathfrak{p}} \cong \mathbb{Z}_p$. We let J be the Jacobian of X. Furthermore,

Important. We suppose that X has a rational point. We fix a point $O \in X(K)$ for Sections 1-4. It will be understood to be the basepoint of all fundamental groups and embeddings into Jacobians in those sections.

From O, we get an embedding $X \hookrightarrow J$ sending O to the identity of J, which we also denote by O.

If $J(K)$ is finite, then it follows that $X(K)$ must be finite, and it is not hard to determine $X(K)$ (c.f. [MP12, §2]). However, $J(K)$, unlike $X(K)$, is not expected to be finite in general; rather, it is proven to be *finitely generated* as an abelian group. Nonetheless, Chabauty observed that even when $J(K)$ is infinite, one might use $J(K)$ to prove finiteness of $X(K)$ *as long as the rank of $J(K)$ as an abelian group is not too large.*

More specifically, Chabauty proved that if

$$r := \operatorname{rank}_{\mathbb{Z}} J(K)$$

is less than the genus g of X, then the intersection

$$X(K_{\mathfrak{p}}) \cap \overline{J(K)}$$

of $X(K_{\mathfrak{p}})$ with the p-adic closure of $J(K)$ in $J(K_{\mathfrak{p}})$ is finite. Later, Coleman showed how to compute this intersection, using his newly developed theory of p-adic integration. The basic intuition is that $\overline{J(K)}$ should be a p-adic manifold of dimension at most r, inside the p-adic manifold $J(K_{\mathfrak{p}})$ of dimension g; then, if $r < g$, its intersection with the one-dimensional p-adic manifold $X(K_{\mathfrak{p}})$ should be discrete, and since $J(K_{\mathfrak{p}})$ is compact, this should be finite.

To make this more precise, one needs a description of the structure of $J(K_{\mathfrak{p}})$. For this, as described in §4.1 of loc. cit., we consider $\omega_J \in H^0(J_{K_{\mathfrak{p}}}, \Omega^1)$, the g-dimensional vector space of regular one-forms on $J_{K_{\mathfrak{p}}}$. Then there is an integration map

$$\begin{aligned} \eta_J \colon J(K_{\mathfrak{p}}) &\to \mathbb{Q}_p \\ Q &\mapsto \int_O^Q \omega_J \end{aligned}$$

characterized uniquely by the fact that it is a homomorphism, and by the fact that for Q sufficiently close to O, it is given by formally taking an anti-derivative of ω_J that vanishes at O and evaluating it at the coordinates of Q.

Letting T denote the dual of $H^0(J_{K_{\mathfrak{p}}}, \Omega^1)$, or equivalently the tangent space to $J_{K_{\mathfrak{p}}}$ at the identity, this gives a homomorphism

$$\log \colon J(K_{\mathfrak{p}}) \to T,$$

which is easily seen to be a local diffeomorphism, hence finite-to-one.

Put together, we now have the diagram:

(A)
$$\begin{tikzcd} X(K) \arrow[r] \arrow[d] & X(K_{\mathfrak{p}}) \arrow[d] \arrow[dr, "\int"] & \\ J(K) \arrow[r] & J(K_{\mathfrak{p}}) \arrow[r, "\log"'] & T \end{tikzcd}$$

The "basic intuition" mentioned above about $\overline{J(Z)}$ can be made precise by noting that the dimension of $\log \overline{J(K)}$ is just the $\mathbb{Z}_p$-rank of the $\mathbb{Z}_p$-span of $\log J(K)$, which must be at most r because $J(K)/(\text{torsion})$ can be generated by $r = \operatorname{rank}_{\mathbb{Z}} J(K)$ elements.

1.1.1. *Coleman Integration.* Finally, the theory of Coleman ([Col85]) allows one to explicitly compute the integration maps in the definition of log. In particular, the diagonal arrow labeled '$\int$' in Diagram A can be expressed as Coleman integration on the p-adic space $X(K_{\mathfrak{p}})$. Therefore, one may explicitly compute a p-adic analytic function on $X(K_{\mathfrak{p}})$ that vanishes on $X(K)$, as follows:

(1) Choose bases of T and $J(K)$
(2) Integrate to find the image of $J(K)$ under log relative to these bases
(3) Find a nonzero element ω_J of $T^\vee = H^0(J_{K_{\mathfrak{p}}}, \Omega^1)$ vanishing on $\log J(K)$
(4) Compute the restriction of η_J to $X(K_{\mathfrak{p}})$

The commutativity of (A) implies that this function vanishes on $X(K)$. Coleman's theory shows that this function is locally analytic and has finitely many zeroes. One may in fact compute local power series expansion for this function, and then use the theory of Newton polygons to approximate the locations of its zeroes.

Remark 1.1. Notice that in applying Chabauty's method, we care only about the span of the image of $J(K)$ in a $\mathbb{Q}_p$-vector space. Therefore, the method doesn't really need knowledge of $J(K)$ itself, but of its tensorization $J(K)_{\mathbb{Q}_p} = J(K) \otimes_{\mathbb{Z}} \mathbb{Q}_p$. This will be important in Section 3.

Remark 1.2. Notice that the line integral $\int_O^Q \omega_J$ does not depend on the choice of a path from O to Q, even up to homotopy. This is a peculiar feature of Coleman integration as opposed to ordinary integration. It may be explained by the notion of Frobenius-invariant path ([Bes02, Corollary 3.2]), also described in Section 5.4.

Remark 1.3. There is a notion of Coleman integration on X itself, and

$$\int_O^Q \omega_J$$

may be computed equivalently as an integral on X or an integral on J. We will return to this point in Section 5.4.

1.2. **Non-Proper Curves and Siegel's Theorem.** We would like to explain how the content of Section 1.1, both Faltings' Theorem and Chabauty's method, fits into a more general fact about integral points on smooth curves of negative Euler characteristic.

Convention: When we say "integral points," we mean points with values in a fixed open subscheme

$$\operatorname{Spec} Z = \operatorname{Spec} \mathcal{O}_K[1/S]$$

of $\operatorname{Spec} \mathcal{O}_K$*; that is, all finiteness results apply equally well to* S*-integral points.*

In 1929, Siegel proved that all affine curves of positive genus have finitely many integral points. For $g > 1$, this is an immediate corollary of Faltings' Theorem (although it was historically proved many years earlier). But for $g = 1$, this gives a result that does not obviously follow, namely that punctured elliptic curves have finitely many integral points (in concrete terms, this implies that a Weierstrass model has finitely many integral solutions). Furthermore, Siegel also proved finiteness of S-integral points for $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, and as a corollary, for any curve of genus 0 with at least three punctures. (Nonetheless, the cases $g = 0, 1$ may be deduced from Faltings' Theorem by a descent argument due to Chevalley and Weil.)

Note that for a proper curve, integral points are the same as rational points, by the valuative criterion of properness. It follows that Faltings' and Siegel's theorems may be jointly summarized by saying that there are finitely many S-integral points on

(1) curves of genus at least 2,
(2) curves of genus 1 with at least one puncture, and
(3) curves of genus 0 with at least three punctures.

In fact, such curves have an important common property that distinguishes them. They are precisely the curves that are *hyperbolic*, which is equivalent to saying that the topological Euler characteristic of their complex points is negative. More importantly for us, they are precisely the smooth curves whose topological fundamental group is non-abelian. We summarize the theorems of Faltings and Siegel as one:

Theorem 1.4 (Faltings-Siegel)**.** *Let X be a smooth curve over a number field K, let Z be an open subscheme of* $\operatorname{Spec}\mathbb{Z}$*, and let $\mathcal{X} \to Z$ be a regular minimal model of X. If the fundamental group of the Betti topological space of $X_{\mathbb{C}}$ is nonabelian (or equivalently if the Euler characteristic is negative) then the set $X(Z)$ of integral points of X is finite.*

Remark 1.5. Just as Siegel's and Faltings' Theorems should be seen as one theorem, there are two other theorems that deserve to be combined in a similar way. Those are Dirichlet's S-Unit Theorem and the Mordell-Weil Theorem. A generalized version of Dirichlet's S-Unit Theorem says that the group of integral points on an algebraic torus is finitely generated. A common generalization of these two theorems then says that

Theorem 1.6 (Dirichlet-Mordell-Weil)*. The group of integral points on a semi-abelian scheme is finitely generated.*

If one wants to make this about curves, one may write it as a statement about the generalized Jacobian of an arbitrary smooth curve (like the one used for Skolem's method in the following section), which is a semi-abelian variety.

1.3. **Skolem's Method.** It turns out that Chabauty's method may be applied to non-proper hyperbolic curves just as well as to proper hyperbolic curves, if one phrases it correctly. In fact, its use for non-proper curves historically predates Chabauty and is known as the method of Skolem, who applied it to Thue equations of the form $f(x, y) = c$ for f a homogeneous binary form of degree at least 3. We briefly describe the more general Chabauty-Skolem method here, as some of the original applications of non-abelian Chabauty involve non-proper curves.

We let X denote a smooth proper curve over a ring $Z = \mathcal{O}_K[1/S]$ of S-integers. While Chabauty-Skolem is very similar to Chabauty, the most subtle point is how to choose J; one wants an embedding from X into a semi-abelian scheme J over Z, such that the embedding is an isomorphism on (geometric) first homology. This may be achieved via a generalized Jacobian. As an example, consider $X = \mathbb{P}^1\backslash\{0, 1, \infty\}$, defined as $\operatorname{Spec}\mathbb{Z}[x, y, x^{-1}, y^{-1}]/(x + y - 1)$. Then $J = \mathbb{G}_m \times \mathbb{G}_m$, and the embedding sends (x, y) satisfying $x+y = 1$ to $(x, y) \in \mathbb{G}_m \times \mathbb{G}_m$. More generally, if X is the complement of a non-split closed reduced subscheme of $\mathbb{A}^1$, then J is a non-split torus of dimension equal to the degree of the subscheme.

To apply Chabauty-Skolem, one chooses a closed point $\mathfrak{p}$ of Z whose completed local ring $Z_{\mathfrak{p}}$ is isomorphic to $\mathbb{Z}_p$. We assume we have a point $O \in X(Z)$, mapping to the identity of J. We let T be the tangent space to $J_{K_{\mathfrak{p}}}$ at O, which is dual to the space of all *translation-invariant* differential 1-forms (not the space of all holomorphic 1-forms unless J is proper). We then have the diagram

(B)
$$\begin{tikzcd} X(Z) \arrow[r] \arrow[d] & X(Z_{\mathfrak{p}}) \arrow[d] \arrow[dr, "\int"] & \\ J(Z) \arrow[r] & J(Z_{\mathfrak{p}}) \arrow[r, "\log"'] & T \end{tikzcd}$$

Then $J(Z)$ is a finitely-generated abelian group (c.f. Theorem 1.6), and the method applies as in the proper case, as long as $\operatorname{rank}_{\mathbb{Z}} J(Z) < \dim J$.

Remark 1.7. In the case that X and J are proper, we have $X(Z) = X(K)$, $J(Z) = J(K)$, $X(Z_\mathfrak{p}) = X(K_\mathfrak{p})$, and $J(Z_\mathfrak{p}) = J(K_\mathfrak{p})$, so the methods of Section 1.1 and of this section are equivalent.

2. The Problem with Abelian Fundamental Groups

This method often does not work, because $J(Z)$ can be too large. Philosophically, the reason why $J(Z)$ can be large while $X(Z)$ remains finite is because the geometric fundamental group of J is abelian, while the fundamental group of X is non-abelian, even center-free.[1] The groundbreaking work of Minhyong Kim ([Kim05]) gets around this fact.

Recall the key properties of J, mentioned in passing in Section 1.3:

(1) J is a semi-abelian scheme over Z.
(2) There is an embedding $X \hookrightarrow J$ that is an isomorphism on (geometric) first homology.

As a clarification about the meaning of "geometric" in (2), note that we can simply require it to be an isomorphism on integral Betti homology for some embedding $Z \hookrightarrow \mathbb{C}$; it then follows that this is the case for Betti cohomology over all embeddings, for algebraic de Rham cohomology over K, and for ℓ-adic cohomology over $\overline{K}$.

Properties (1) and (2) together imply that the embedding induces the abelianization map on fundamental groups (whether Betti, de Rham, crystalline, or geometric étale), because a semi-abelian scheme is in particular a group scheme, so its fundamental group is abelian, hence

$$\pi_1(J) = \pi_1(J)^{ab} = H_1(J) = H_1(X) = \pi_1(X)^{ab}.$$

It might then seem natural to hope for an embedding from X into a variety whose fundamental group is not abelian but *almost abelian*. More specifically, letting $\pi_1(X)$ denote some version (Betti, de Rham, crystalline, or geometric étale) of the fundamental group of X based at O, we define the *descending central series filtration* of $\pi_1(X)$ by

$$\pi_1(X)^{[1]} := \pi_1(X)$$
$$\pi_1(X)^{[n]} := [\pi_1(X)^{[n-1]}, \pi_1(X)]^2,$$

and the corresponding quotients

$$\pi_1(X)_n := \pi_1(X)/\pi_1(X)^{[n+1]},$$

so that $\pi_1(X)_1 = \pi_1(X)^{ab} = \pi_1(J) = H_1(X)$.

We then might hope that for each n, we can find an embedding

$$X \hookrightarrow J_n$$

whose induced map on fundamental groups $\pi_1(X) \to \pi_1(J_n)$ is isomorphic to the quotient map $\pi_1(X) \twoheadrightarrow \pi_1(X)_n$. However, I know of no candidate for the varieties J_n, at least in general.[3]

[1]This is not to say that all varieties with abelian fundamental group have infinitely many integral points, but that in the context of the distinction between a curve and its Jacobian, this principle applies.

[2]If the group has some kind of topology, it is understood that we always take the closure of the commutator.

[3]Since I began writing this, I became aware of work in progress by Edixhoven, Lido, and Schoof, in which they use the Poincaré torsor of the Jacobian of X as an approximation to J_2 and show that non-abelian Chabauty's method may be carried out using its geometry.

To remedy this, the critical insight of Kim was to

(*)

Rewrite the whole of the Chabauty-Skolem method intrinsically in terms of X and its fundamental group.

When we do that, we will see that the Chabauty-Skolem specifically uses $\pi_1(X)_1 = H_1(X)$, which is why classical Chabauty-Skolem is considered "abelian." If the constructions are sufficiently general, one may then replace $\pi_1(X)_1$ by $\pi_1(X)_n$ to arrive at Kim's non-abelian Chabauty's method, as explained in Section 4. Section 3 will be devoted to explaining how to rewrite Chabauty-Skolem in terms of X and its fundamental group.

3. Expressing Chabauty's Method Intrinsically in Terms of X

For simplicity, we assume that X is proper from now until the end of Section 3.2. We then explain the modifications necessary for non-proper X in Section 3.3

In some sense, using J is like using the (abelianization of the) fundamental group of X. From a complex analytic perspective, J not only has the same first (co)homology as X; it is in fact *determined* by (the Hodge structure on) the first (co)homology of X. The Abel-Jacobi Theorem shows that one may construct J as the quotient $H^1(X,\mathbb{R})/H^1(X,\mathbb{Z})$, where the complex structure on $H^1(X,\mathbb{R})$ is determined by the Hodge structure on $H^1(X,\mathbb{C})$. That gives us a first hint as to how to write Chabauty's method in terms of homology.

Of course, for something arithmetic like Chabauty's method, we need to go beyond the complex analytic realm. More specifically, we need to express all the parts of diagram (B) in terms of X:

Goal 3.1. *Express $J(K)$, $J(K_\mathfrak{p})$, T, and the map* log *intrinsically in terms of the first homology of X.*

Remark 3.2. Following Remark 1.1, we really care only about $J(K)_{\mathbb{Q}_p}$ rather than $J(K)$. The same is true of $J(K_\mathfrak{p})$ with respect to its rationalization $J(K_\mathfrak{p})_\mathbb{Q} = J(K_\mathfrak{p}) \otimes_\mathbb{Z} \mathbb{Q}$.

3.1. **Intrinsic Description of the Mordell-Weil Group.**

We first focus on $J(K)$. Recall, for each positive integer m, the Kummer exact sequence

$$0 \to J[m](\overline{K}) \to J(\overline{K}) \xrightarrow{m} J(\overline{K}) \to 0,$$

of G_K-modules, giving rise to the long exact sequence

$$0 \to J[m](K) \to J(K) \to J(K) \to H^1(K, J[m]) \to H^1(K,J) \xrightarrow{m} H^1(K,J) \to \cdots$$

and hence a short exact sequence

$$0 \to J(K)/mJ(K) \xrightarrow{\kappa_m} H^1(K, J[m]) \to H^1(K,J)[m] \to 0, \tag{1}$$

where κ_m is known as the (mod m) *Kummer map.*

The importance of using $J[m]$ is the following: there is a canonical, Galois-equivariant isomorphism

$$J[m] \cong H_1^{\text{ét}}(J_{\overline{K}}, \mathbb{Z}/m\mathbb{Z}) \cong H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/m\mathbb{Z}).[4]$$

[4]For those not familiar with an intrinsic definition of étale homology (of which there are multiple), one may define it simply as the dual of étale cohomology with respect to the chosen coefficients, at least when the cohomology is free.

In other words, the Kummer map is an embedding

$$J(K)/mJ(K) \hookrightarrow H^1(K, H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/m\mathbb{Z})).$$

To get an embedding of $J(K)$ rather than $J(K)/mJ(K)$, one may simply set $m = p^n$ and take an inverse limit. Let

$$T_p := H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \cong H_1^{\text{ét}}(J_{\overline{K}}, \mathbb{Z}_p) \cong \mathrm{T_p}\, J(\overline{K})$$

and

$$V_p := T_p \otimes \mathbb{Q} = H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p),$$

with their associated G_K-actions. Then we get embeddings

$$J(K)_{\mathbb{Z}_p} \hookrightarrow H^1(K, T_p)$$

as well as its rational cousin

$$J(K)_{\mathbb{Q}_p} \hookrightarrow H^1(K, V_p).$$

We now have a 'container' for $J(K)$ defined intrinsically in terms of X, but we need to identify the subspace $J(K)$ inside it (or at least, following Remark 3.2, its $\mathbb{Q}_p$-span) purely in terms of $V_p = H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ (i.e., without reference to J). The vector space V_p has the structure of a G_K-representation, so we want a purely Galois-theoretic way to identify the image of $J(K)_{\mathbb{Q}_p}$ in $H^1(K, V_p)$. As we shall see, this is supplied by the theory of Bloch-Kato Selmer groups, developed in [BK90]. In order to explain what a Bloch-Kato Selmer group is, we first recall the classical theory of Selmer groups.

3.1.1. *Finite Selmer Groups.* We let Σ_K denote the set of all places of K. We consider the short exact sequence 1 both over K and over all completions K_v of K to obtain a diagram:
(C)

$$\begin{tikzcd}
0 \arrow[r] & J(K)/mJ(K) \arrow[r, "\kappa_m"] \arrow[d] & H^1(K, J[m]) \arrow[r] \arrow[d, "\alpha"'] \arrow[dr, "\delta"] & H^1(K, J)[m] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_{v \in \Sigma_v} J(K_v)/mJ(K_v) \arrow[r, "\beta"] & \prod_{v \in \Sigma_K} H^1(K_v, J[m]) \arrow[r, "\gamma"] & \prod_{v \in \Sigma_K} H^1(K_v, J)[m] \arrow[r] & 0
\end{tikzcd}$$

The Selmer group $\mathrm{Sel}_m(J)$ is defined to be the inverse under α of the image of β. As the bottom row is exact, this is just the kernel of $\gamma \circ \alpha = \delta$, implying we have a short exact sequence

$$0 \to J(K)/mJ(K) \to \mathrm{Sel}_m(J) \to Ш_J[m] \to 0,$$

where $Ш_J := \ker(H^1(K, J) \to \prod_{v \in \Sigma_K} H^1(K_v, J)$.

We also have the following conjecture:

Conjecture 3.3 (Tate-Shafarevich)**.** *For any abelian variety J, the group $Ш_J$ is finite.*

3.1.2. *p-adic Selmer Groups.* The map κ_m is unfortunately usually non-injective when viewed as a map from $J(K)$ to $\mathrm{Sel}_m(J)$. To solve this problem, and to make use of the fact that $Ш_J$ is finite, we pass to p-adic Selmer groups.

More precisely, let $\mathrm{T_p}\, Ш_J$ be the p-adic Tate module of $Ш_J$, namely the inverse limit of the groups $Ш_J[p^n]$ taken over the multiplication by p map. Let

$$\mathrm{Sel}_{p^\infty}(J) := \varprojlim \mathrm{Sel}_{p^n}(J).$$

As $J(K)$ is finitely generated, we have $\varprojlim J(K)/p^n J(K) = J(K)_{\mathbb{Z}_p}$, so we have a short exact sequence

$$0 \to J(K)_{\mathbb{Z}_p} \to \mathrm{Sel}_{p^\infty}(J) \to \mathrm{T_p}\,Ш_J \to 0.$$

In particular, if, as conjectured, $Ш_J$ is finite, then $\mathrm{T_p}\,Ш_J = 0$. In fact, as noted in [Sto07, §2], this would follow simply from the weaker claim that the p-divisible part of $Ш_J$ is trivial. By Remark 3.2, Conjecture 3.3 suggests that we may replace $J(K)$ by $\mathrm{Sel}_{p^\infty}(J)$ in Chabauty's method. In practice, one may make the replacement without assuming the conjecture: the standard way to compute $J(K)$ is by computing Selmer groups, and if the $\mathbb{Z}_p$-rank of $\mathrm{Sel}_{p^\infty}(J)$ is less than g, then Chabauty's method works. The conjecture simply shows that we do not expect to lose anything by passing from $J(K)_{\mathbb{Z}_p}$ to $\mathrm{Sel}_{p^\infty}(J)$.

Notice that $\mathrm{Sel}_{p^n}(J) \subseteq H^1(K, H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p^n\mathbb{Z}))$, so

$$\mathrm{Sel}_{p^\infty}(J) \subseteq \varprojlim H^1(K, H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}/p^n\mathbb{Z})) = H^1(K, T_p)$$

Remark 3.4. On the infinite level, the Selmer group is defined by the same kind of local condition as is the finite version. First, we need a definition:

Definition 3.5. For an abelian group M, we define the *p-adic completion*

$$\widehat{M} := \varprojlim M/p^n M.$$

When M is finitely generated, this is the same as $M \otimes \mathbb{Z}_p$. When M is profinite, it surjects onto its p-adic completion.

To understand the local condition for p-adic Selmer groups, we draw the diagram

(D)
$$\begin{tikzcd}
0 \arrow[r] & J(K)_{\mathbb{Z}_p} \arrow[r, "\kappa_{p^\infty}"] \arrow[d] & H^1(K, T_p) \arrow[r] \arrow[d, "\alpha"'] & H^1(K, J)[p^\infty] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_{v \in \Sigma_v} \widehat{J(K_v)} \arrow[r, "\beta"] & \prod_{v \in \Sigma_K} H^1(K_v, T_p) \arrow[r, "\gamma"] & \prod_{v \in \Sigma_K} H^1(K_v, J)[p^\infty] \arrow[r] & 0.
\end{tikzcd}$$

Then the Selmer group $\mathrm{Sel}_{p^\infty}(J)$ is just the inverse under α of the image of β.

Remark 3.6. Following Remark 3.2, we only really care about these things $\mathbb{Q}_p$-linearly. In other words, we care about $J(K)_{\mathbb{Q}_p}$, which is conjecturally isomorphic to

$$\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}} := \mathrm{Sel}_{p^\infty}(J) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{Sel}_{p^\infty}(J) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

We may draw the diagram

(D')
$$\begin{tikzcd}
0 \arrow[r] & J(K)_{\mathbb{Q}_p} \arrow[r, "\kappa_{p^\infty}"] \arrow[d] & H^1(K, V_p) \arrow[d, "\alpha"'] \\
0 \arrow[r] & \prod_{v \in \Sigma_v} \widehat{J(K_v)}_{\mathbb{Q}} \arrow[r, "\beta"] & \prod_{v \in \Sigma_K} H^1(K_v, V_p).
\end{tikzcd}$$

Then by exactness of tensoring with $\mathbb{Q}$, the $\mathbb{Q}_p$-Selmer group $\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}}$ is just the inverse under α of the image of β in Diagram D'.

Remark 3.7. For a given $v \in \Sigma_K$, let ℓ denote its residue characteristic. Then $J(K_v)$ is a compact abelian ℓ-adic Lie group of dimension g, so it's isomorphic to a finite group times $\mathbb{Z}_\ell^g$[5]. It follows that $J(K_v)$ surjects onto its p-adic completion, so we may replace $\prod_{v \in \Sigma_v} \widehat{J(K_v)}$ by $\prod_{v \in \Sigma_v} J(K_v)$ in the diagram without changing the image of β. As explained in Section 3.3, this is no longer always true when X is not compact.

Remark 3.8. When $\ell \neq p$, the p-adic completion of $J(K_v)$ is finite, so the image of β is torsion and therefore zero when working rationally. In particular, its image has an intrinsic definition. In fact, the entire group $H^1(K_v, V_p)$ is trivial (c.f. [Fen16, Example 2.4] or [Bel09, Exercise 2.9]), so one may ignore the local conditions for $\ell \neq p$.

However, when X and J are non-compact, this is not always the case, and one may need the local conditions for $\ell \neq p$, as explained in Section 3.3. This is fundamentally related to the fact that integral points and rational points may be different on non-proper varieties.

We now want a way to determine the image of $J(K)_{\mathbb{Q}_p}$ in $H^1(K, V_p)$ in terms of the Galois representation V_p. We are partway there, as we may replace $J(K)_{\mathbb{Q}_p}$ by $\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}}$; the latter seems more intrinsic, as it is a subgroup of $H^1(K, V_p)$ defined by local conditions.

The problem is that this collection of "local conditions" (by which we mean a certain subgroup of $\prod_{v \in \Sigma_K} H^1(K_v, V_p)$) is still defined using the geometry of J, rather than something intrinsic to the representation T_p. Bloch and Kato solved this problem[6].

3.1.3. *Bloch-Kato Selmer Groups.* References for this section include [BK90, §3], [Bel09, §2], [Fen16].

Bloch and Kato fixed this problem by observing in [BK90] that one could define the image of β by using p-adic Hodge theory, and therefore define $\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}}$ intrinsically in terms of the Galois action on V_p. Their original motivation was to extend the notions of Selmer group and Tate-Shafarevich group (and hence the Birch and Swinnerton-Dyer Conjecture) to motives other than those arising from the H^1 of an abelian variety). But their methods are invaluable in Kim's work, as they will eventually allow us to extend the notion of Selmer group from $T_p = H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \cong \pi_1^{\text{ét}}(X_{\overline{K}})_1 \otimes_{\widehat{\mathbb{Z}}} \mathbb{Z}_p$ to certain non-abelian pro-p quotients of $\pi_1^{\text{ét}}(X_{\overline{K}})$.

By Remark 3.8, because we are assuming X is proper, we need to consider local conditions only for v of residue characteristic p, so we need to determine the image of

$$\kappa_v \colon J(K_v)_{\mathbb{Q}} \to H^1(K_v, V_p).$$

Notice that by considering the case where v is the chosen place $\mathfrak{p}$, this will also solve the second part of Goal 3.1; that is, writing $J(K_{\mathfrak{p}})$ intrinsically.

To explain how Bloch-Kato identified the appropriate subgroup of $H^1(K_v, V_p)$, we need to recall a bit of p-adic Hodge theory. This theory identifies a subcategory

$$\{\text{crystalline representations}\} \subseteq \{\text{all continuous } \mathbb{Q}_p\text{-representations of } G_{K_v}\}.$$

[5]For the reader who wants to know why, here's the sketch of an argument. We assume the fact about p-adic Lie groups, proved in [Bou98] or [Ser06], that the Lie group exponential is defined on a neighborhood of the identity, is a local homeomorphism, and is a group homomorphism for abelian Lie groups. As the identity in a g-dimensional p-adic vector space has a basis of neighborhoods of the identity that are subgroups isomorphic to $\mathbb{Z}_p^g$, we choose such a neighborhood U mapping homeomorphically onto its image under the exponential. Then its image is an open subgroup of $J(K_v)$, which must be finite index by compactness.

[6]Also c.f. the last paragraph of Section 1 in [Fen16, p.4] for a similar description of this "problem."

Crystalline representations are the $\ell = p$ analogue of unramified representations in the $\ell \neq p$ case. More specifically, just as the ℓ-adic cohomology of a variety with good reduction at $p \neq \ell$ is unramified, the p-adic cohomology of such a variety is always crystalline, albeit technically ramified.

We can apply this notion to the group $H^1(K_v, V_p)$, which is the group of extensions of $\mathbb{Q}_p$ (with trivial G_{K_v}-action) by V_p, in the category of continuous p-adic representations of G_{K_v}. That is, every element $\alpha \in H^1(K_v, V_p)$ may be represented as an extension

$$0 \to V_p \to E_\alpha \to \mathbb{Q}_p \to 0.$$

Definition 3.9. We say that $\alpha \in H^1(K_v, V_p)$ is *crystalline* if the representation E_α is crystalline as a representation of G_{K_v}.

Definition 3.10. The subgroup of all crystalline elements of $H^1(K_v, V_p)$ is denoted

$$H^1_f(K_v, V_p)$$

and is known as the *local Bloch-Kato Selmer group at v*.

Just as varieties with good reduction at v give rise to crystalline representations, extensions coming from integral points (elements of $J(\mathcal{O}_v)$) are crystalline. But as J is proper, we have $J(K_v) = J(\mathcal{O}_v)$, so the image of $J(K_v)$ lands in $H^1_f(K_v, V_p)$. The key theorem of Bloch-Kato in this context is:

Theorem 3.11 (Bloch-Kato)**.** *The image of the Kummer map*

$$\kappa_v \colon J(K_v)_{\mathbb{Q}} \to H^1(K_v, V_p)$$

is $H^1_f(K_v, V_p)$.

The proof of the theorem proceeds by noting that the map is injective and then showing that the dimension of the right side is $g[K_v : \mathbb{Q}_p]$, which is the dimension of $J(K_v)$ as a p-adic Lie group, and hence of $J(K_v)_{\mathbb{Q}}$ as a $\mathbb{Q}_p$-vector space.

Finally, we recall what happens globally; i.e., over K.

Definition 3.12. We let $H^1_f(K, V_p)$ denote the subset of $\alpha \in H^1(K, V_p)$ whose image in $H^1(K_v, V_p)$ lies in $H^1_f(K_v, V_p)$ for each $v \mid p$. This is known as the *(global) Bloch-Kato Selmer group.*

We then have:

Corollary 3.13 (of Theorem 3.11)**.** *For any abelian variety J, the group $\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}}$ is naturally identified with $H^1_f(K, V_p)$.*

Proof. As explained in Remark 3.4, the group $\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}}$ is the subset of $H^1(K, V_p)$ that is locally in the image of $J(K_v)_{\mathbb{Q}}$ for each v. By Remark 3.8, the only relevant places are those dividing p, so the result follows by Theorem 3.11. □

Although the equality $J(K)_{\mathbb{Q}_p} = H^1_f(K, V_p)$ is only conjectural (as it follows from Conjecture 3.3), we still have a natural map $X(K) \to H^1_f(K, V_p)$, which means that we may rewrite Chabauty's diagram in the following way:

$$\text{(A')} \qquad \begin{tikzcd} X(K) \arrow[r] \arrow[d, "\kappa"] & X(K_{\mathfrak{p}}) \arrow[d, "\kappa_{\mathfrak{p}}"] \arrow[dr, "\int"] & \\ H^1_f(K, V_p) \arrow[r, "\mathrm{loc}"'] & H^1_f(K_{\mathfrak{p}}, V_p) \arrow[r, "\log"'] & T \end{tikzcd}$$

We have partially achieved our goal, as we have rewritten the diagram in a way that should be equally amenable as Diagram A to proving finiteness of $X(K)$ (that is, as long as Conjecture 3.3 is true), and in which $J(K)$ and $J(K_{\mathfrak{p}})$ were replaced by objects defined purely in terms of X.

The map $\int$ may be defined intrinsically in terms of X by Remark 1.3. However, for the moment, our only way to define log is to compose the logarithm (tensored with $\mathbb{Q}$) associated to the p-adic Lie group $J(K_{\mathfrak{p}})$ with the inverse of $\kappa_{\mathfrak{p}}$ in Theorem 3.11. This reliance on J means that we do not yet have an intrinsic definition of log (or of its target T, for that matter). We now explain how Bloch and Kato's work defines log intrinsically.

3.2. **Intrinsic Definition of the Logarithm.** Before defining log intrinsically, we must define its target T.

3.2.1. *De Rham Homology and its Hodge Filtration.* Recall that, as long as X is proper, T is the dual of $H^0(J_{K_{\mathfrak{p}}}, \Omega^1)$. But $H^0(J_{K_{\mathfrak{p}}}, \Omega^1)$ has a description in terms of cohomology; more precisely, in terms of the Hodge filtration on the de Rham cohomology of $J_{K_{\mathfrak{p}}}$. There is a decreasing filtration F^i on $H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$, with

$$0 = F^2 H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}}) \subseteq H^0(J_{K_{\mathfrak{p}}}, \Omega^1) = F^1 H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}}) \subseteq F^0 H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}}) = H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}}).$$

It is also true that $\mathrm{Gr}^0 H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}}) \cong H^1(J_{K_{\mathfrak{p}}}, \mathcal{O}_{J_{K_{\mathfrak{p}}}})$, but we will not need this fact. Furthermore, when X is not proper, it is still true that $F^1 H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$ is isomorphic to the space of translation-invariant holomorphic differentials on J.

The de Rham homology $H_1^{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$ is isomorphic to the dual of $H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$ (as with étale homology, one can give an intrinsic definition, but this is not needed). It has a decreasing Hodge filtration dual to that of $H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$, defined as an annihilator

$$F^i H_1^{\mathrm{dR}}(J_{K_{\mathfrak{p}}}) := \mathrm{Ann}(F^{-i+1} H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}})).$$

The funny-looking index $-i+1$ ensures that $\mathrm{Gr}^i H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$ is dual to $\mathrm{Gr}^{-i} H_1^{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$.

The upshot is that T, isomorphic to the dual of $H^0(J_{K_{\mathfrak{p}}}, \Omega^1) = \mathrm{Gr}^1 H^1_{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$, is just $\mathrm{Gr}^{-1} H_1^{\mathrm{dR}}(J_{K_{\mathfrak{p}}}) = H_1^{\mathrm{dR}}(J_{K_{\mathfrak{p}}})/F^0 H_1^{\mathrm{dR}}(J_{K_{\mathfrak{p}}})$. In fact, this is intrinsic to X, because the inclusion $X \hookrightarrow J$ induces an isomorphism on first homology and cohomology, so we have

$$T = H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})/F^0 H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}}).$$

This is our desired intrinsic definition of T.

Bloch-Kato were furthermore able to define a logarithm map $H^1_f(K_{\mathfrak{p}}, V_p) \to T$ purely in terms of the representation V_p (i.e., without reference to J). The reader who wishes to take this on faith may safely skip to Section 3.3.

For the interested reader who wishes to see a sketch of this construction, we have to recall how p-adic Hodge theory relates the p-adic étale cohomology of X to the de Rham cohomology of $X_{K_{\mathfrak{p}}}$.

3.2.2. *More p-adic Hodge Theory.* We work only over $K_{\mathfrak{p}} \cong \mathbb{Q}_p$. Fontaine's theory defines a series of $\mathbb{Q}_p$-algebras with $G_{\mathbb{Q}_p}$-action. The two we will need are

$$B_{\mathrm{crys}} \subseteq B_{\mathrm{dR}}.$$

Their actual definitions do not concern us. The important facts are as follows. There is a descending filtration F^i on B_{dR}, for which $B_{\mathrm{dR}}^+ := F^0 B_{\mathrm{dR}}$ is a DVR with fraction field B_{dR} and residue field $\mathbb{C}_p$, the p-adic completion of $\overline{\mathbb{Q}_p}$. There is a Frobenius ϕ acting on B_{crys}, whose fixed subring is denoted $B_{\mathrm{crys}}^{\phi=1}$. We also have $B_{\mathrm{crys}}^{G_{K_{\mathfrak{p}}}} = B_{\mathrm{dR}}^{G_{K_{\mathfrak{p}}}} = K_{\mathfrak{p}}$, and for a continuous p-adic representation V of $G_{\mathbb{Q}_p}$, we define

$$D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_{K_{\mathfrak{p}}}}$$
$$D_{\mathrm{dR}}^+(V) = (B_{\mathrm{dR}}^+ \otimes_{\mathbb{Q}_p} V)^{G_{K_{\mathfrak{p}}}}$$
$$D_{\mathrm{crys}}(V) = (B_{\mathrm{crys}} \otimes_{\mathbb{Q}_p} V)^{G_{K_{\mathfrak{p}}}}$$

The decreasing filtration on B_{dR} induces a filtration on $D_{\mathrm{dR}}(V)$, known as the *Hodge filtration.* If Y is a smooth variety over $\mathbb{Q}_p$ and $V = H^i_{\text{ét}}(Y_{\overline{\mathbb{Q}_p}}, \mathbb{Q}_p)$, then an important theorem in p-adic Hodge theory tells us that there is a natural isomorphism

$$D_{\mathrm{dR}}(V) \to H^i_{\mathrm{dR}}(Y)$$

respecting the Hodge filtrations on each side. In addition, $D_{\mathrm{dR}}^+(V)$ is naturally identified with $F^0 D_{\mathrm{dR}}(V)$.

Similarly, the Frobenius on B_{crys} induces a Frobenius map on $D_{\mathrm{crys}}(V)$, and if $V = H^i_{\text{ét}}(Y_{\overline{\mathbb{Q}_p}}, \mathbb{Q}_p)$, and Y has good reduction with special fiber $\mathcal{Y}_{\mathbb{F}_p}$, then there is a natural isomorphism

$$D_{\mathrm{crys}}(V) \to H^i_{\mathrm{crys}}(\mathcal{Y}_{\mathbb{F}_p}, \mathbb{Q}_p)$$

respecting the Frobenius morphisms on each side. Note that if X is not proper, we may need to replace crystalline cohomology by log-crystalline or rigid cohomology. Finally, note that D_{dR} and D_{crys} commute with taking duals, so the aforementioned results apply equally well to homology.

Let us apply all of that to $Y = X_{K_{\mathfrak{p}}}$ and first homology. Once again, let $V_p = H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$. Then

$$H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}}) \cong D_{\mathrm{dR}}(V_p) \cong D_{\mathrm{crys}}(V_p),$$

and by compatibility with the Hodge filtration, we also have

$$T \cong D_{\mathrm{dR}}(V_p)/D_{\mathrm{dR}}^+(V_p).$$

Remark 3.14. It turns out that we can now give a precise definition of the crystalline condition (as well as the de Rham condition introduced below in Section 3.3.2), although we left out this definition out earlier because we did not explicitly use it. For a general p-adic representation V of $G_{K_{\mathfrak{p}}}$, we always have

$$\dim D_{\mathrm{crys}}(V) \leq \dim D_{\mathrm{dR}}(V) \leq \dim V.$$

We say that V is *crystalline* if

$$\dim D_{\mathrm{crys}}(V) = \dim V$$

and *de Rham* if

$$\dim D_{\mathrm{dR}}(V) = \dim V.$$

The statements above about the cohomology of smooth varieties $Y/\mathbb{Q}_p$ imply that the p-adic cohomology of any variety is de Rham as a representation of $G_{\mathbb{Q}_p}$, and crystalline if the variety has good reduction at p.

3.2.3. *The Bloch-Kato Exponential Map.* Armed with all the background from Section 3.2.2, we are now able to sketch how Bloch-Kato defined the map

$$\log\colon H^1_f(K_\mathfrak{p}, V_p) \to T$$

purely in terms of the representation V_p.

For this, we note that by [BK90, 1.17], there is a short exact sequence

$$0 \to \mathbb{Q}_p \xrightarrow{\alpha} B_{\mathrm{crys}}^{\phi=1} \oplus B_{\mathrm{dR}}^+ \xrightarrow{\beta} B_{\mathrm{dR}} \to 0,$$

defined by $\alpha(x) = (x, x)$ and $\beta(x, y) = x - y$.

Upon tensoring with V over $\mathbb{Q}_p$ and taking Galois cohomology, as well as noting by [BK90, Lemma 3.8.1] that the map $H^1(K_\mathfrak{p}, V \otimes B_{\mathrm{dR}}^+) \to H^1(K_\mathfrak{p}, B_{\mathrm{dR}})$ is injective, we get a long exact sequence

$$0 \to V^{G_{K_\mathfrak{p}}} \to D_{\mathrm{crys}}(V_p)^{\phi=1} \oplus D_{\mathrm{dR}}^+(V_p) \to D_{\mathrm{dR}}(V_p) \to H^1(K_\mathfrak{p}, V_p) \to H^1(K_\mathfrak{p}, V_p \otimes B_{\mathrm{crys}}^{\phi=1})$$

Bloch-Kato also prove that the kernel

$$\ker(H^1(K_\mathfrak{p}, V_p) \to H^1(K_\mathfrak{p}, V_p \otimes B_{\mathrm{crys}}^{\phi=1})),$$

which they denote $H^1_e(K_\mathfrak{p}, V_p)$, is equal to $H^1_f(K_\mathfrak{p}, V_p)$. From this, we get a surjective map

$$T = D_{\mathrm{dR}}(V_p)/D_{\mathrm{dR}}^+(V_p) \to H^1_f(K_\mathfrak{p}, V_p),$$

known as the *Bloch-Kato exponential map.* Bloch-Kato ([BK90, Example 3.10.1-3.11]) show that this coincides with the ordinary exponential map in the case of a p-adic formal Lie group and of an abelian variety, respectively.

The kernel of this map is $D_{\mathrm{crys}}(V_p)^{\phi=1}/V^{G_{K_\mathfrak{p}}}$, which is 0 when V_p is the Tate module of an abelian (or even semi-abelian) variety, essentially by the Weil conjectures (which imply that ϕ has no eigenvalues equal to 1). In that case, it has an inverse

$$\log_{\mathrm{BK}},$$

sometimes called the *Bloch-Kato logarithm*, which is our intrinsically-defined logarithm.

3.3. **Bloch-Kato for Non-Proper X.** The reader wishing to see Kim's method more quickly may take on faith that for a general semi-abelian variety J:

(1) There is a notion of p-adic Selmer group

$$\mathrm{Sel}_{p^\infty}(J) \subseteq H^1(K, T_p)$$

relative to an integer ring $Z = \mathcal{O}_K[1/S]$,

(2) The image of

$$\kappa\colon J(Z)_{\mathbb{Q}_p} \to H^1(K, V_p)$$

is contained in $\mathrm{Sel}_{p^\infty}(J)_\mathbb{Q}$, and they coincide as long as Conjecture 3.3 is true, and

(3) The definition of $\mathrm{Sel}_{p^\infty}(J)_\mathbb{Q}$ is intrinsic to the Galois representation $V_p = H_1^{\text{ét}}(J, \mathbb{Q}_p) = H_1^{\text{ét}}(X, \mathbb{Q}_p)$,

and skip to Section 3.4. We have already explained this when J is an abelian variety; the reader wishing to see the more general case of a semi-abelian variety may continue below.

We suppose we're looking at Z-points for $Z = \mathcal{O}_K[1/S]$, with S a finite set of places not containing $\mathfrak{p}$. The basic modification to Diagram D is that for $v \notin S$, we want to consider the image under β not of $J(K_v)$ (or its $\mathbb{Q}_p$-completion) but of $J(\mathcal{O}_v)$. In other words, we will define $\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}}$ as the preimage under α of the image of β in the diagram:

(D")
$$\begin{tikzcd} J(Z)_{\mathbb{Q}_p} \arrow[rr, "\kappa_{p^\infty}"] \arrow[d] & & H^1(K, V_p) \arrow[d, "\alpha"] \\ \prod_{v\notin S} \widehat{J(\mathcal{O}_v)}_{\mathbb{Q}} \times \prod_{v\in S} \widehat{J(K_v)}_{\mathbb{Q}} \arrow[rr, "\beta"] & & \prod_{v\in\Sigma_K} H^1(K_v, V_p), \end{tikzcd}$$

This establishes (1). As well, (2) follows by combining the case of an abelian variety with Kummer theory for algebraic tori (essentially following the Kummer theory discussed in 3.3.1, with K in place of K_v).

Now, we deal with (3). Write $\beta = \prod_{v\in\Sigma_K} \kappa_v$, where for $v \in S$, we have

$$\kappa_v \colon \widehat{J(K_v)}_{\mathbb{Q}} \to H^1(K_v, V_p),$$

and for $v \notin S$,

$$\kappa_v \colon \widehat{J(\mathcal{O}_v)}_{\mathbb{Q}} \to H^1(K_v, V_p).$$

Definition 3.15. For each place v of K, we refer to the image of κ_v as the *local Bloch-Kato Selmer group*[7] *at* v.

In this terminology, the group $\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}}$ is the preimage under α of the product of all the local Bloch-Kato Selmer groups.

Our goal for the rest of Section 3.3 is to explain why the local Bloch-Kato Selmer group can be defined intrinsically in terms of the representation V_p. This will in turn give an intrinsic definition of $\mathrm{Sel}_{p^\infty}(J)_{\mathbb{Q}}$.

Recall that in Remark 3.8, we mentioned that when X is proper, we may ignore v of residue characteristic ℓ different from p. This is no longer true if we are considering non-proper X. More specifically, we will need local conditions for all $v \notin S$.

As well, Remark 3.7 is no longer quite true. For example, for $J = \mathbb{G}_m$, the group $J(K_v)$ is product of $\mathbb{Z}$ with a compact ℓ-adic Lie group, so it does not surject onto its p-adic completion (whether or not $\ell = p$). Therefore, the p-adic completions in Diagram D" are necessary.

For the previous two reasons, we have to be more careful for non-proper X and J.

3.3.1. *Bloch-Kato for* $\mathbb{G}_m$. For simplicity, we first explain what happens when $J = \mathbb{G}_m$. The case of a general semi-abelian variety will then be a simple combination of what we know for $\mathbb{G}_m$ and what we know for abelian varieties. We let

$$T_p = H_1^{\text{ét}}(J_{\overline{K}}, \mathbb{Z}_p) = \mathbb{Z}_p(1).$$

By Kummer theory, there is an isomorphism

$$\kappa_v \colon \widehat{K_v^\times} \xrightarrow{\sim} H^1(K_v, T_p).$$

[7]Note that this definition of local Bloch-Kato Selmer groups agrees *a posteriori* with the standard one, although it is not *a priori* the same. Usually, one first gives the intrinsic definition of local Bloch-Kato Selmer groups via p-adic Hodge theory, and then proves as a theorem that they are the same as our definition.

Therefore, for $v \notin S$, the local Bloch-Kato Selmer group is the whole group $H^1(K_v, V_p)$.

We now cover $v \in S$. We let ℓ denote the residue characteristic of v.

When $\ell = p$, the group $K_v^\times$ is the product of a compact p-adic Lie group of dimension $[K_v : \mathbb{Q}_p]$ with $\mathbb{Z}$, so $\widehat{K_v^\times} \cong H^1(K_v, T_p)$ is a $\mathbb{Z}_p$-module of rank $1 + [K_v : \mathbb{Q}_p]$. The group $\widehat{\mathcal{O}_v^\times} \subseteq \widehat{K_v^\times}$ has rank $[K_v : \mathbb{Q}_p]$, and its image in $H^1(K_v, T_p)$ consists entirely of crystalline classes. Bloch-Kato show that the group $H^1_f(K_v, T_p)$ of crystalline classes has rank $[K_v : \mathbb{Q}_p]$, which implies that the image of

$$\kappa_v \colon \widehat{\mathcal{O}_v^\times} \otimes \mathbb{Q} \to H^1(K_v, V_p)$$

is precisely $H^1_f(K_v, V_p)$.

When $\ell \neq p$, the group $\mathcal{O}_v^\times$ is a compact ℓ-adic Lie group, so its p-completion is finite, and its $\mathbb{Q}$-tensorization is trivial. Therefore, we may take the local Bloch-Kato Selmer group to be 0.

We summarize the cases as follows:

	$v \in S$	$v \notin S$
$\ell = p$	$H^1(K_v, V_p)$	$H^1_f(K_v, V_p)$
$\ell \neq p$	$H^1(K_v, V_p)$	0

3.3.2. *Bloch-Kato for Semi-abelian Varieties.* Everything in Section 3.3.1 applies whenever J is an algebraic torus, which follows by Galois descent applied to a product of copies of $\mathbb{G}_m$. However, when J is a general semi-abelian variety, we need to combine what we just did for $\mathbb{G}_m$ with what we did in Section 3.1.3.

The trickiest case is when $\ell = p$, but $v \in S$. In that case, we are considering rational points $J(K_v)$. When J is an abelian variety, these are cut out by the crystalline condition. But when J is a torus, the crystalline condition cuts out $J(\mathcal{O}_v)$, not the full group $J(K_v)$. We therefore need a new p-adic Hodge theory condition that corresponds to crystalline classes for an abelian variety but all classes for an algebraic torus.

In addition to the category of crystalline representations, there is an intermediate subcategory

$$\{\text{crystalline representations}\} \subseteq \{\text{de Rham representations}\} \subseteq \{\text{all } \mathbb{Q}_p\text{-representations of } G_{K_v}\},$$

which is the $\ell = p$ analogue of *all* representations in the $\ell \neq p$. In particular, every representation coming from the étale cohomology of a variety is de Rham, but not all continuous $\mathbb{Q}_p$-representation of G_{K_v} is de Rham.

We recall the notation that if $\alpha \in H^1(K_v, V_p)$, there is a corresponding extension

$$0 \to V_p \to E_\alpha \to \mathbb{Q}_p \to 0$$

of representations of G_{K_v}.

Definition 3.16. We say that $\alpha \in H^1(K_v, V_p)$ is *de Rham* if the representation E_α is de Rham as a representation of G_{K_v}.

Definition 3.17. Following [BK90], the subgroup of all de Rham elements of $H^1(K_v, V_p)$ is denoted

$$H^1_g(K_v, V_p).$$

It is a theorem that *any* representation coming from the étale cohomology of a variety is de Rham. Therefore, the image of $\kappa_v \colon \widehat{K_v^\times} \otimes \mathbb{Q} \xrightarrow{\sim} H^1(K_v, \mathbb{Q}_p(1))$ consists entirely of de Rham classes, so

$$H^1_g(K_v, \mathbb{Q}_p(1)) = H^1(K_v, \mathbb{Q}_p(1)).$$

On the other hand, if V_p is the (rational) Tate module of an abelian variety, we have

$$H^1_f(K_v, V_p) = H^1_g(K_v, V_p).$$

The reader should think of this a cohomological manifestation of the fact that integral and rational points are the same on a proper variety.

Combining these two cases, it makes sense to say that when $\ell = p$ and $v \notin S$, our local Bloch-Kato Selmer group is $H^1_g(K_v, V_p)$.

In the $\ell = p$ and $v \in S$ case, we do not need any modifications, as the image of

$$\widehat{J(\mathcal{O}_v)} \otimes \mathbb{Q} \to H^1(K_v, V_p)$$

is just $H^1_f(K_v, V_p)$, the subgroup of crystalline classes.

For $\ell \neq p$ and $v \in S$, we note that

$$\widehat{J(K_v)} \otimes \mathbb{Q} \to H^1(K_v, V_p)$$

is an isomorphism; this is an easy combination of Remark 3.8 with the case $\ell = p\, v \notin S$ for $J = \mathbb{G}_m$.

Finally, for $\ell \neq p$ and $v \notin S$, we note that $J(\mathcal{O}_v)$ is a compact ℓ-adic Lie group, so its p-adic completion is torsion. In this case, the local Bloch-Kato Selmer group is 0.

We summarize the cases as follows:

	$v \in S$	$v \notin S$
$\ell = p$	$H^1_g(K_v, V_p)$	$H^1_f(K_v, V_p)$
$\ell \neq p$	$H^1(K_v, V_p)$	0

3.4. **Summary of Intrinsic Chabauty-Skolem.** We may now rewrite Diagram A in a way that refers only to X and its first homology:

(A")

$$\begin{tikzcd} X(Z) \arrow[r] \arrow[d] & X(Z_{\mathfrak{p}}) \arrow[d] \arrow[dr, "\int"] & \\ H^1_f(K, H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \arrow[r, "\text{loc}"'] & H^1_f(K_{\mathfrak{p}}, H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \arrow[r, "\log_{\text{BK}}"'] & H_1^{\text{dR}}(X_{K_{\mathfrak{p}}})/F^0 H_1^{\text{dR}}(X_{K_{\mathfrak{p}}}) \end{tikzcd}$$

Notice that we've written out $H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p)$ rather than the equivalent shorthand T_p. This is to emphasize the fact that T_p only depends on the first homology (and therefore fundamental group) of X.

Recall from Section 2 that if we let $\pi_1(X)$ denote some version (Betti, de Rham, crystalline, geometric étale, or pro-p geometric étale) of the fundamental group of X based at O, then we define the *descending central series filtration* of $\pi_1(X)$ by

$$\pi_1(X)^{[1]} := \pi_1(X)$$
$$\pi_1(X)^{[n]} := [\pi_1(X)^{[n-1]}, \pi_1(X)],$$

where commutator always denotes the topological closure of the group-theoretic commutator. We have the corresponding quotients

$$\pi_1(X)_n := \pi_1(X)/\pi_1(X)^{[n+1]},$$

so that $\pi_1(X)^{ab} = \pi_1(X)_1 = H_1(X)$.

Our goal is to think of the homology in Diagram A" as the abelianization $\pi_1(X)^{ab} = \pi_1(X)_1$, and then replace $\pi_1(X)_1$ by $\pi_1(X)_n$ for $n > 1$. In the next section, we explain how to do this.

4. Making Sense of Chabauty-Skolem for Non-Abelian Quotients

4.1. **Chabauty-Skolem in terms of the Fundamental Group.** We just mentioned that "we want to replace all instances of first homology of X in Diagram A" by something in the form $\pi_1(X)^{ab} = \pi_1(X)_1$. We must now be precise about what kind of fundamental group we are using.

There are two instances of first homology where we want to do this. The first instance is the p-adic étale homology $H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p)$. Note that $\pi_1^{\text{ét}}(X_{\overline{K}})_1$ is isomorphic to $H_1^{\text{ét}}(X_{\overline{K}}, \widehat{\mathbb{Z}})$. Letting $\pi_1^{\text{ét}}(X_{\overline{K}})^{(p)}$ denote the pro-p completion of $\pi_1^{\text{ét}}(X_{\overline{K}})$, we have

$$H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Z}_p) = \pi_1^{\text{ét}}(X_{\overline{K}})_1^{(p)}.$$

While we may define $\pi_1^{\text{ét}}(X_{\overline{K}})_n^{(p)}$ for $n > 1$, but it is a priori a mystery what one means by the tensorization $\pi_1^{\text{ét}}(X_{\overline{K}})_n^{(p)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. As an approximation, note that

$$\pi_1^{\text{ét}}(X_{\overline{K}})^{(p),[n]}/\pi_1^{\text{ét}}(X_{\overline{K}})^{(p),[n+1]} = \mathrm{Im}(\pi_1^{\text{ét}}(X_{\overline{K}})^{(p),[n]} \to \pi_1^{\text{ét}}(X_{\overline{K}})_n^{(p)})$$

is a free $\mathbb{Z}_p$-module of finite rank, so its $\mathbb{Q}_p$-tensorization is a p-adic representation of G_K. Therefore, whatever we mean by $\pi_1^{\text{ét}}(X_{\overline{K}})_n^{(p)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, the nth subquotient of its descending central series filtration should be naturally isomorphic to

$$(\pi_1^{\text{ét}}(X_{\overline{K}})^{(p),[n]}/\pi_1^{\text{ét}}(X_{\overline{K}})^{(p),[n+1]}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

We explain how to do this in Section 4.2.1.

The second instance of first homology is the de Rham homology $H_1^{\text{dR}}(X_{K_\mathfrak{p}})$. There is a notion of unipotent de Rham fundamental group $\pi_1^{\text{dR}}(X_{K_\mathfrak{p}})$, whose abelianization is the first de Rham homology. We will explain the de Rham fundamental group in more detail in Section 4.2.2.

It turns out that each of $\pi_1^{\text{ét}}(X_{\overline{K}})_n^{(p)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $\pi_1^{\text{dR}}(X_{K_\mathfrak{p}})$ has the structure of a pro-unipotent group over $\mathbb{Q}_p$. We therefore now review the notion of pro-unipotent groups and pro-unipotent completion.

4.2. **Pro-Unipotent Groups.**

Definition 4.1. A *pro-unipotent group* over $\mathbb{Q}_p$ is a group scheme over $\mathbb{Q}_p$ that is a projective limit of unipotent algebraic groups over $\mathbb{Q}_p$.

Any unipotent group over $\mathbb{Q}_p$ is trivially a pro-unipotent group. Furthermore, an abelian unipotent group is the same thing as a finite-dimensional vector space over $\mathbb{Q}_p$, under the identification

$$V \mapsto \mathrm{Spec}(\mathrm{Sym}\, V^\vee).$$
$$U(\mathbb{Q}_p) \leftarrow\!\shortmid U$$

The most natural way to produce a pro-unipotent group that is not an algebraic group (rather, a pro-algebraic group) is by the procedure of *pro-unipotent* or *Malcev*[8] completion of ordinary groups, along with its profinite version in Section 4.2.1. Some references for pro-unipotent completion include [Vez] and [Sui07], and the original source is the appendix to [Qui69].

We now describe the notion of pro-unipotent completion rigorously, as we will need it to define the pro-unipotent completion $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}$ of $\pi_1^{\text{ét}}(X_{\overline{K}})$ in Section 4.2.1. However, in practice, one really needs to know only the existence of the Galois-equivariant universal homomorphism $\pi_1^{\text{ét}}(X_{\overline{K}}) \to \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}(\mathbb{Q}_p)$ and the isomorphism (2) that it induces, so the reader who wishes may now skip to Section 4.2.1.

Let Γ be an abstract group and R a field of characteristic 0. There are three equivalent ways to define the pro-unipotent completion Γ_R of Γ, and each gives a different insight on this completion. We list these three ways as three "Constructions":

Construction 4.2. Let $A \coloneqq R[\Gamma]$ be the group ring of Γ with coefficients in R. Then A is naturally a cocommutative Hopf algebra over R, where each $g \in \Gamma \subseteq A$ is grouplike. There is a counit $\epsilon\colon A \to R$ sending $g \in \Gamma$ to $1 \in R$. Let J denote the augmentation ideal, i.e., the kernel of ϵ.

Let
$$R[\Gamma]_J \coloneqq \varprojlim_m R[\Gamma]/J^m,$$
and let
$$B \coloneqq \mathrm{H}om_R^{\mathrm{cts}}(R[\Gamma]_J, R)$$
be the vector space of continuous (with respect to the J-adic topology) linear functionals on $R[\Gamma]_J$. A functional is continuous if and only if it factors through the quotient by a finite power of J, so we may equivalently write
$$B_R = \varinjlim \mathrm{H}om_R(R[\Gamma]/J^m, R) = \varinjlim \mathrm{H}om_{\mathbb{Q}}(\mathbb{Q}[\Gamma]/J^m, R).$$

The cocommutative Hopf algebra structure on A gives a commutative Hopf algebra structure on B. Then the prounipotent completion Γ_R of Γ is the group scheme
$$\Gamma_R = \operatorname{Spec} B_R.$$

This construction is described in [Hai05, §1.5]

Construction 4.3. Let $\mathbf{Rep}_R(\Gamma)$ denote the category of R-linear representations of Γ. It is an abelian tensor category[9] with unit object $\mathbb{1} = R$, the trivial one-dimensional representation. We recall the notion of a unipotent object of such a category:

Definition 4.4. If V is an object of an abelian tensor category $\mathcal{C}$, then we say that V is *unipotent* if there exists a finite filtration $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_m = V$ such that
$$V_i/V_{i-1} \cong \mathbb{1}$$
for $i = 1, \cdots, m$.

[8]The Russian is Мальцев, so it might make more sense to write Maltsev.

[9]All the reader must know about tensor categories $\mathcal{C}$ is that they have a tensor product functor $\times$ and that tensoring with the unit object $\mathbb{1}$ is isomorphic to the identity functor.

Let $\mathbf{Rep}_R^{\mathrm{un}}(\Gamma)$ denote the subcategory of unipotent R-linear representations of Γ. Then this is a neutral Tannakian category,[10] and by the general theory of Tannakian categories, it is equivalent to the category $\mathbf{Rep}_R^{\mathrm{alg}}(\Gamma_R)$ of R-linear algebraic representations of a pro-unipotent group that we denote Γ_R.

If Γ is a profinite group and R a topological field, one may modify this construction by taking the category of continuous R-linear representations of Γ. We will use this particularly when Γ is profinite and $R = \mathbb{Q}_p$.

Construction 4.5. The pro-unipotent completion U_Γ may be defined by the following universal property. The group U_Γ is a pro-unipotent group with a canonical group homomorphism

$$u\colon \Gamma \to \Gamma_R(R)$$

such that for any unipotent group U over R and group homomorphism

$$f\colon \Gamma \to U(R),$$

there is a unique algebraic group homomorphism

$$f_u\colon \Gamma_R \to U$$

such that after passing to R-points,

$$f = f_u \circ u.$$

If Γ is a topological group and R a topological field, then Γ_R has the same universal property, with "group homomorphism" replaced by "continuous group homomorphism."

Let X be a variety over a subfield $K \subseteq \mathbb{C}$. We write X^{an} for $X(\mathbb{C})$ equipped with its structure as a complex manifold (in particular, with the complex topology). Then the pro-unipotent *Betti* or *topological* fundamental group $\pi_1(X^{\mathrm{an}})_{\mathbb{Q}}$ is defined as the pro-unipotent completion of the topological fundamental group $\Gamma = \pi_1(X^{\mathrm{an}})$ over $\mathbb{Q}$.

4.2.1. *The Unipotent Etale Fundamental Group.* For a variety X over a field K, there is a notion of the $\mathbb{Q}_p$-pro-unipotent completion

$$\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}$$

of the profinite group $\pi_1^{\text{ét}}(X_{\overline{K}})$.

It is defined via Construction 4.3 or 4.5 for the topological group $\Gamma = \pi_1^{\text{ét}}(X_{\overline{K}})$ and topological ring $R = \mathbb{Q}_p$. There is even a version of Construction 4.2, but it involves first taking the completed group ring of the pro-p nilpotent quotient of Γ and then completing with respect to the augmentation ideal.

In either case, one defines $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}$ by applying p-adic pro-unipotent completion to the profinite group $\Gamma = \pi_1^{\text{ét}}(X_{\overline{K}})$. One may define the lower central series quotients

$$\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n} = \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}/\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}^{[n+1]},$$

and in the cases we consider (specifically, when the profinite group in question is topologically finitely generated), these quotients are not only pro-unipotent but actually unipotent algebraic groups (i.e., they are *finite-dimensional varieties*).

[10]A *Tannakian category* is a rigid abelian tensor category, and neutral refers to the existence of a limit-preserving tensor functor to the category of R-vector spaces. The main theorem is that any neutral Tannakian category is equivalent as a tensor category to the category of representations of a unique (up to isomorphism) pro-algebraic group. More details can be found, for example, in [Bre94].

Then $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}$ is the $\mathbb{Q}_p$-pro-unipotent completion of $\pi_1^{\text{ét}}(X_{\overline{K}})_n := \pi_1^{\text{ét}}(X_{\overline{K}})/\pi_1^{\text{ét}}(X_{\overline{K}})^{[n+1]}$. One may show that the continuous homomorphism

$$\pi_1^{\text{ét}}(X_{\overline{K}}) \to \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}(\mathbb{Q}_p)$$

induces the desired isomorphisms

$$\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}^{[n]}/\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}^{[n+1]} \cong (\pi_1^{\text{ét}}(X_{\overline{K}})^{(p),[n]}/\pi_1^{\text{ét}}(X_{\overline{K}})^{(p),[n+1]}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p. \tag{2}$$

In particular, $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}$ has the important property that its abelianization is naturally isomorphic to $H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$.

In either case, it is isomorphic to the group scheme

$$\pi_1(X^{\text{an}})_{\mathbb{Q}_p}$$

over $\mathbb{Q}_p$ when K is a subfield over $\mathbb{C}$, but with the added bonus of having an action of G_K induced by the continuous Galois action of G_K on $\pi_1^{\text{ét}}(X_{\overline{K}})$. The homomorphism $\pi_1^{\text{ét}}(X_{\overline{K}}) \to \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}(\mathbb{Q}_p)$ and hence the isomorphisms (2) are Galois-equivariant for this action.

The action of G_K on $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}$ is a *continuous algebraic* action. The "algebraic" part means that for a fixed $\sigma \in G_K$, the map $\sigma\colon \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p} \to \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}$ is a morphism of group schemes over $\mathbb{Q}_p$.[11] The "continuous part" means that the map

$$G_K \times \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}(\mathbb{Q}_p) \to \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}(\mathbb{Q}_p)$$

is a continuous map of topological spaces, with the profinite topology on G_K and the p-adic topology on p-adic points.

The coordinate ring $\mathcal{O}(\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p})$ is a vector space over $\mathbb{Q}_p$. The continuous algebraic action of G_K on $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}$ is the same as giving the vector space

$$\mathcal{O}(\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p})$$

the structure of a continuous $\mathbb{Q}_p$-linear representation of G_K, for which the multiplication and comultiplication maps are Galois-equivariant. For $v \in \Sigma_K$, we can restrict this representation of G_K to a representation of G_{K_v} and try to do p-adic Hodge theory with it. We note one technical point that allows us to do this:

Remark 4.6. Normally, in p-adic Hodge theory, one works with p-adic Galois representations on finite-dimensional vector spaces. The theory of finite-dimensional p-adic Galois representations still applies to

$$\mathcal{O}(\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}),$$

because it is an inductive limit of finite-dimensional p-adic Galois representations. For example, we say that it is crystalline or de Rham if it is an inductive limit of crystalline or de Rham representations, and we define D_{dR} and D_{crys} so that they commute with inductive limits of finite-dimensional representations.

[11] If this algebraicity seems strange, note that in the abelian case, the condition of being algebraic is equivalent to being linear.

4.2.2. *The Unipotent de Rham Fundamental Group.* Just as the de Rham homology of $X_{K_\mathfrak{p}}$ is D_{dR} of the p-adic étale homology, we may define the unipotent de Rham fundamental group $\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})$ of $X_{K_\mathfrak{p}}$ as

$$\operatorname{Spec} D_{\mathrm{dR}}(\mathcal{O}(\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p})).$$

We may take Spec because D_{dR} is compatible with tensor products, so the Hopf algebra structure on $\mathcal{O}(\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p})$ makes $\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})$ into a group scheme. There is even a Bloch-Kato exponential map, which we will discuss in Section 4.3.3.

This definition of $\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})$ may seem unsatisfying, for it is not intrinsic to de Rham theory and does not give us a pro-unipotent group over K itself. For now, this definition will suffice, as it is the quickest way to define Kim's cutter. We will give a more intrinsic definition in Section 5, as it is necessary in order to relate p-adic Galois cohomology to p-adic integration. More specifically, in order to compute the composition of the logarithm with $\kappa_\mathfrak{p}$ (a.k.a. the diagonal arrow of Diagrams A-A"), we must express this diagonal arrow as some sort of integration, as we did in the abelian case in Section 1.1.1. The more intrinsic definition of $\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})$ in terms of de Rham theory, rather than in terms of D_{dR}, will allow us to do so.

The unipotent de Rham fundamental group $\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})$ has a Hodge filtration on its coordinate ring coming from that on the functor D_{dR} described in Section 3.2.2. The Hodge filtration on its coordinate ring induces one on its Lie algebra, and the 0th filtered piece of its Lie algebra is a Lie subalgebra, which corresponds to a subgroup denoted $F^0\pi_1^{\mathrm{dR}}$.[12]

We assume that p is a prime of good reduction for X, so it is also the same as

$$\operatorname{Spec} D_{\mathrm{crys}}(\mathcal{O}(\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p})),$$

which gives it a Frobenius action. As mentioned in the previous paragraph, we leave non-abelian Coleman integration (i.e., the explicit description of the diagonal arrow) to Section 5.

Finally, just as with $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}$, there is a descending central series filtration, along with corresponding quotients

$$\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n.$$

This is compatible via p-adic Hodge theory with the descending central series filtration on $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}$, in the sense that

$$D_{\mathrm{dR}}\mathcal{O}(\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}) \cong \mathcal{O}(\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n),$$

in a way compatible with the Hopf algebra, Hodge, and Frobenius structures.

4.2.3. *Free Pro-Unipotent Groups.* If Γ is a free group (as in the case for the fundamental group of any smooth affine curve), then its pro-unipotent completion is a free pro-unipotent group (Construction 4.5 easily implies this, for an appropriate definition of the free pro-unipotent group on a set in terms of a universal property). Similarly, the de Rham fundamental group of such a curve is a free

There is in fact a concrete description of the coordinate ring of a free pro-unipotent group as a free shuffle algebra, described as follows. Suppose Γ has free generators $\gamma_1, \cdots, \gamma_r$.

Then B has $\mathbb{Q}$-vector space basis consisting of words w in the γ_i's; in particular, it is isomorphic as a vector space to the non-commutative polynomial algebra

$$\mathbb{Q}\langle\gamma_1, \cdots, \gamma_r\rangle.$$

[12] The subvarieties $F^i\pi_1^{\mathrm{dR}}$ for $i \neq 0$ are not, however, subgroups, as incorrectly stated in [Kim05].

The product of two words w_1, w_2 in the γ_i's is the shuffle product:

$$w_1 ш w_2 := \sum_{\sigma \in ш(\ell(w_1), \ell(w_2))} \sigma(w_1 w_2),$$

where ℓ denotes the length of a word, $ш(\ell(w_1), \ell(w_2)) \subseteq S_{\ell(w_1)+\ell(w_2)}$ denotes the group of shuffle permutations of type $(\ell(w_1), \ell(w_2))$, and $w_1 w_2$ denotes concatenation. The coproduct Δ is given by

$$\Delta w := \sum_{w_1 w_2 = w} w_1 \otimes w_2.$$

More generally, if U is a free pro-unipotent group, let $\gamma_1, \cdots, \gamma_r$ be a set of generators for U^{ab} as a vector space (recall that an abelian unipotent group is the same as a vector space). Then $\mathcal{O}(U)$ has the same description, at least abstractly. However, the exact basis of $\mathcal{O}(U)$ is determined only if one chooses lifts to the γ_i from U^{ab} to U.

We will apply this in the case that U is the de Rham unipotent fundamental group, whence U^{ab} is the first de Rham homology. In this case, a choice of closed differential 1-forms representing cohomology classes dual to the γ_i does determine lifts of each γ_i to U, by associating with a word the corresponding iterated integral described in Section 5.

4.3. **Making sense of the Chabauty-Skolem diagram with Unipotent Fundamental Group.** Armed with our notion of $\mathbb{Q}_p$-unipotent fundamental group $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p}$, we can conjecture a non-abelian version of Diagram A". We choose some level of nilpotency n and simply replace $H_1^{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ by $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}$, and $H_1^{\text{dR}}(X_{K_\mathfrak{p}})$ by $\pi_1^{\text{dR}}(X_{K_\mathfrak{p}})_n$:

(Non-Abelian A)

$$\begin{tikzcd}
X(Z) \arrow[r] \arrow[d] & X(Z_\mathfrak{p}) \arrow[d] \arrow[dr, "\int"] & \\
H^1_f(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}) \arrow[r, "\mathrm{loc}_n"'] & H^1_f(K_\mathfrak{p}, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}) \arrow[r, "\log_{\mathrm{BK}}"'] & \pi_1^{\text{dR}}(X_{K_\mathfrak{p}})_n / F^0 \pi_1^{\text{dR}}(X_{K_\mathfrak{p}})_n
\end{tikzcd}$$

Such a diagram diagram is known as *Kim's cutter*[13]. We have drawn this diagram by analogy, but we have still not precisely defined all of the terms and maps in it. We will spend the rest of Section 4.3 doing so.

4.3.1. *Non-Abelian Cohomology Varieties.* We first mention what we mean by $H^1(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n})$.

For a group G acting on a group U, the set $H^1(G, U)$ is defined to be the set of isomorphism classes of G-equivariant torsors under U.

Therefore, for us, an element of $H^1(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n})$ is a scheme over $\mathbb{Q}_p$ with a continuous algebraic action of G_K and a G_K-equivariant algebraic action of $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}$ making it into a $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}$-torsor.

Kim defines this in [Kim05, §1] and shows that the short exact sequence

$$0 \to \pi_1^{\text{ét}}(X_{\overline{K}})^{[n]}_{\mathbb{Q}_p} / \pi_1^{\text{ét}}(X_{\overline{K}})^{[n+1]}_{\mathbb{Q}_p} \to \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n} \to \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n-1} \to 0$$

[13] I am told that it is called Kim's cutter not only because it 'cuts out' a subset of $X(Z_\mathfrak{p})$, but because it resembles a box cutter, with the triangular part of the diagram being the blade and the rectangular part the handle.

gives rise to a long exact sequence

(3)

$$\cdots \to H^1(K, \pi_1^{\text{ét}}(X_{\overline{K}})^{[n]}_{\mathbb{Q}_p}/\pi_1^{\text{ét}}(X_{\overline{K}})^{[n+1]}_{\mathbb{Q}_p}) \to H^1(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}) \to H^1(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n-1}) \to \cdots$$

Note that, since $\pi_1^{\text{ét}}(X_{\overline{K}})^{[n]}_{\mathbb{Q}_p}/\pi_1^{\text{ét}}(X_{\overline{K}})^{[n+1]}_{\mathbb{Q}_p}$ is an ordinary p-adic Galois representation, the cohomology group $H^1(K, \pi_1^{\text{ét}}(X_{\overline{K}})^{[n]}_{\mathbb{Q}_p}/\pi_1^{\text{ét}}(X_{\overline{K}})^{[n+1]}_{\mathbb{Q}_p})$ has the structure of a $\mathbb{Q}_p$-vector space. Because we are considering non-abelian cohomology, there is no natural group structure on $H^1(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n})$. But using induction on the long exact sequences (3), Kim ([Kim05, §1]) identifies it with the set of $\mathbb{Q}_p$-points of an affine variety over $\mathbb{Q}_p$ (in fact isomorphic to an affine space).

4.3.2. *Bloch-Kato Selmer Conditions.* We have to understand what it means for an element

$$\alpha \in H^1(K_v, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n})$$

to be crystalline, de Rham, or unramified.

In fact, this is simple. Such an element corresponds to a torsor T_α under $\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}$ whose coordinate ring is a p-adic representation of G_{K_v}. We say that the element is α is crystalline, de Rham, or unramified, if the corresponding is true of

$$\mathcal{O}(T_\alpha)$$

as a p-adic representation of G_{K_v}, keeping in mind Remark 4.6.

Kim shows that the subset of

$$H^1(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n})$$

cut out by the corresponding local conditions, denoted

$$H^1_f(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}),$$

is actually a subvariety, known as the *Selmer variety*. It is discussed in more detail in [Kim09], where it is denoted $\mathrm{Sel}(X/Z)_n$.

We similarly refer to $H^1_f(K_\mathfrak{p}, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n})$ as the *local Selmer variety* and denote it by $\mathrm{Sel}(X/Z_\mathfrak{p})_n$.

4.3.3. *Non-Abelian Bloch-Kato Exponential.* There is a Bloch-Kato exponential and logarithm in the non-abelian setting, giving an isomorphism

$$H^1_f(K_v, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}) \xrightarrow[\log_{\mathrm{BK}}]{\sim} D_{\mathrm{dR}}\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}/D^+_{\mathrm{dR}}\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n} = \pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n$$

The busy reader may wish to take this on faith and proceed to the next section. But to explain how to define this map, we need to understand how to write the Bloch-Kato logarithm in terms of the torsor description of cohomology classes.

As discussed in Section 4.3.1, the cohomology group

$$H^1(K_v, V_p)$$

is isomorphic to the set of G_{K_v}-equivariant torsors under V_p. To see how this relates to the definition of cohomology in terms of extensions, note that to the extension

$$0 \to V_p \to E_\alpha \to \mathbb{Q}_p \to 0.$$

is associated the preimage T_α of $1 \in \mathbb{Q}_p$. This preimage has a Galois action, in the sense of a Galois action on its coordinate ring as an affine space. But it does not have the structure of a linear representation - for it is merely a torsor under V_p - and therefore an affine space rather than a vector space.

By considering coordinate rings, one may give $D_{\mathrm{dR}}(T_\alpha)$ the structure of a torsor under $D_{\mathrm{dR}}(V_p)$. Furthermore, there is still a subspace $D^+_{\mathrm{dR}}(T_\alpha) \subseteq D_{\mathrm{dR}}(T_\alpha)$; but this is an *affine* subspace, not a vector subspace in any natural way.

By analyzing the long exact sequence in Section 3.2.3, it turns out that $\log_{\mathrm{BK}}$ may be defined as follows. Given $\alpha \in H^1_f(K_v, V_p)$, there is a Frobenius action on the affine space $D_{\mathrm{dR}}(T_\alpha) = D_{\mathrm{crys}}(T_\alpha)$, and it has a unique Frobenius-invariant point. The difference of this element with $D^+_{\mathrm{dR}}(T_\alpha)$ is a well-defined element of $D_{\mathrm{dR}}(V_p)/D^+_{\mathrm{dR}}(V_p)$ that coincides with $\log_{\mathrm{BK}} \alpha$.

In the non-abelian setting, one may define a Bloch-Kato exponential map

$$H^1_f(K_v, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}) \to D_{\mathrm{dR}}\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}/D^+_{\mathrm{dR}}\pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n} = \pi_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})_n$$

analogously, as follows. We find the unique Frobenius-invariant point on $D_{\mathrm{crys}}T_\alpha$ and then take the difference between this and $D^+_{\mathrm{dR}}T_\alpha$. It is a simple exercise to check that this non-abelian Bloch-Kato logarithm is compatible with exact sequences. It then follows by induction on the exact sequences (3) that the non-abelian Bloch-Kato logarithm is compatible with the ordinary Bloch-Kato logarithm for the representations $\pi_1^{\text{ét}}(X_{\overline{K}})^{[n]}_{\mathbb{Q}_p}/\pi_1^{\text{ét}}(X_{\overline{K}})^{[n+1]}_{\mathbb{Q}_p}$.

4.4. **Kim's Cutter.** We have defined Kim's cutter

(Kim's Cutter)

$$\begin{tikzcd} X(Z) \arrow[r] \arrow[d, "\kappa"] & X(Z_{\mathfrak{p}}) \arrow[d, "\kappa_{\mathfrak{p}}"'] \arrow[dr, "\int"] & \\ H^1_f(K, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}) \arrow[r, "\mathrm{loc}_n"'] & H^1_f(K_{\mathfrak{p}}, \pi_1^{\text{ét}}(X_{\overline{K}})_{\mathbb{Q}_p,n}) \arrow[r, "\sim", "\log_{\mathrm{BK}}"'] & \pi_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})_n \end{tikzcd}$$

We have defined all of the terms in the diagram and every map except $\int$. We will explain what it has to do with integration in Section 5. For now, we will simply define it to be the unique map that makes the diagram commute.

Kim defines the following subsets "cut-out" by the diagram:

Definition 4.7. We set

$$X(Z_{\mathfrak{p}})_n := \kappa_{\mathfrak{p}}^{-1}(\mathrm{Im}(\mathrm{loc}_n)) = \int^{-1}(\mathrm{Im}(\log_{\mathrm{BK}} \circ \mathrm{loc}_n)).$$

These sets are decreasing as n increases, and their usefulness is expressed by the fact that

$$X(Z) \subseteq X(Z_{\mathfrak{p}})_n \subseteq X(Z_{\mathfrak{p}}).$$

Kim proves two important theorems about these sets in [Kim09]. The first is [Kim09, Theorem 1]

Theorem 4.8 (Kim)**.** *Let X be a hyperbolic curve over $\mathbb{Q}$. The map $\kappa_{\mathfrak{p}}$ has dense image.*

An important corollary is:

Corollary 4.9. *If* loc_n *is non-dominant for some* n*, then* $X(Z_{\mathfrak{p}})_n$ *is in the zero locus of a nonzero Coleman function. Thus if* $Z_{\mathfrak{p}} \cong \mathbb{Z}_p$*, then* $X(Z_{\mathfrak{p}})_n$ *is finite.*

If $Z_{\mathfrak{p}} \ncong \mathbb{Z}_p$, then $X(Z_{\mathfrak{p}})$ is a p-adic manifold of dimension > 1, and the zero-set of a single nonzero Coleman function is not necessarily finite. Dogra ([Dog19]) has gotten around this by considering the product $\prod_{\mathfrak{p}|p} X(Z_{\mathfrak{p}})$ and proving an 'unlikely intersection' result.

The second result is [Kim09, Theorem 2]:

Theorem 4.10 (Kim)**.** *Let* X *is a hyperbolic curve over* $\mathbb{Q}$*. Then a portion of the Bloch-Kato conjectures (*[BK90, Conjecture 5.3]*)*[14] *implies that* $X(Z_{\mathfrak{p}})_n$ *is finite for sufficiently large* n*.*

Note that this result has been extended to all number fields K in [Dog19, Theorem 1.1(2)].

In some cases, one is able to prove this unconditionally. The case when X has CM Jacobian was proven by Coates and Kim ([CK10]), and then Ellenberg and Hast ([EH17]) extended this to all solvable covers of $\mathbb{P}^1$ (in particular, they reproved Faltings' Theorem for all hyperelliptic and superelliptic curves).

5. Non-Abelian Integration

In order to prove Theorem 4.10 or to perform any explicit computations, it is necessary to better understand the map $\int$. That is the purpose of Section 5.

We first recall what happens in the abelian case, when $n = 1$. As described in Section 3.2.1, the lower-right corner of Kim's cutter is

$$H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})/F^0 H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}}) = T := H^0(X_{J_{\mathfrak{p}}}, \Omega^1)^\vee = H^0(X_{K_{\mathfrak{p}}}, \Omega^1)^\vee.$$

As mentioned in Section 3.2.3, the Bloch-Kato logarithm agrees in this case with the map log of Section 1.1. The map log is defined using integration, as follows. If $P \in J(K)$, then $\log P \in T := H^0(X_{J_{\mathfrak{p}}}, \Omega^1)^\vee$ is defined by the formula

$$\log P(\omega) = \int_O^P \omega,$$

where integration means p-adic Coleman integration, a topic the reader may read about in [Bes12]. Similarly, if we want to write things intrinsically in terms of X, then for $P \in X(K)$, the element $\int(P) \in T = H^0(X_{K_{\mathfrak{p}}}, \Omega^1)\vee$ is defined by

$$\int(P)(\omega) = \int_O^P \omega.$$

Note that we are taking

$$\omega \in H^0(X_{K_{\mathfrak{p}}}, \Omega^1) = T^\vee = (H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})/F^0 H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}}))^\vee,$$

the space of linear functionals on $H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})/F^0 H_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}})$. We want to replace T by a variety in the non-abelian setting, but we can't talk about functionals on a variety; only regular functions on a variety.

[14] More specifically, we need

Conjecture 4.11. *For integers* r *and* n *and a smooth proper variety* Y *over* K*, we have*

$$K_{2r-n-1}^{(r)}(Y) \otimes \mathbb{Q}_p \cong H_g^1(G_K, H^n(Y_{\overline{K}}, \mathbb{Q}_p))$$

and only in the case $Y = X^n$.

We can thus rephrase the abelian case as follows: an element of T is the same a $\mathbb{Q}_p$-algebra homomorphism $\mathcal{O}(T) \to \mathbb{Q}_p$. The fact that this is the same as a functional on $T^\vee$ is because a basis for $T^\vee$ is the same as a set of polynomial generators of $\mathcal{O}(T) = \operatorname{Sym} T^\vee$. So instead of asking to specify $\int(P)(\omega)$ only for $\omega \in T^\vee$, we could just ask to specify it for all $\omega \in \operatorname{Sym} T^\vee = \mathcal{O}(T)$.

In other words, we might hope that for $\omega \in \mathcal{O}(\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n)$, we can write

$$\int(P)(\omega)$$

as some sort of integral from O to P with integrand defined by ω. This leaves two questions: (1) What do we mean by an integral in general and (2) How can we relate integrands of such integrals to elements of $\mathcal{O}((\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n)$. In fact, $\mathcal{O}((\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n)$ is a subring of $\mathcal{O}((\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n)$, so it suffices to ask about all $\omega \in \mathcal{O}((\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n)$.

We may answer both questions using the theory of iterated integration, which we now discuss.

Remark 5.1. If $\omega \in T^\vee$, then ω defines a linear functional $H_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})/F^0H_1^{\mathrm{dR}}(X_{K_\mathfrak{p}}) \to \mathbb{Q}_p$. Using the projection

$$\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n \to \pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_1/F^0\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_1 = H_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})/F^0H_1^{\mathrm{dR}}(X_{K_\mathfrak{p}}),$$

ω defines an element of $\mathcal{O}(\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n)$. The problem is that most elements of $\mathcal{O}(\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n/F^0\pi_1^{\mathrm{dR}}(X_{K_\mathfrak{p}})_n)$ do not come from $\omega \in T^\vee$ for $n > 1$.

5.1. **Iterated Integrals.** The type of iterated integration used in non-abelian Chabauty's method is p-adic. However, we find it more pedagogical to explain the idea of iterated integration by first explaining complex iterated integration, which should be less of a conceptual leap for the reader. We will then turn to the related notion of a vector bundle with unipotent connection in Section 5.2.

We recommend [Hai05, §1] as an introduction to the theory of iterated integrals and Chen's π_1 de Rham theorem. We have followed it to some extent in our exposition. The reader may also wish to consult [Hai02] and [Bro13].

For a smooth manifold M, let PM be the space of piecewise smooth paths in M, i.e., piecewise smooth maps $\gamma\colon [0,1] \to M$. Then a complex-valued differential 1-form ω on M can be integrated along any piecewise smooth path and therefore defines a function $\int \omega\colon PM \to \mathbb{C}$.

Many people are familiar with the fact that if ω is a 1-form on a manifold, M, then it defines a linear functional $H_1(M,\mathbb{Z}) \to \mathbb{C}$. This follows from the facts

(1) If ω is closed, then $\int_\gamma \omega$ depends only on the homotopy class of γ relative to its endpoints.
(2) For paths α and β for which the endpoint of α is the initial point of β, we can form the composition $\alpha\beta$, and we have

$$\int_{\alpha\beta} \omega = \int_\alpha \omega + \int_\beta \omega.$$

Specifically, if $m \in M$ and ω is closed, the first part implies that $\int \omega$ defines a function $\pi_1(M,m) \to \mathbb{C}$. The second part implies that this function is a group homomorphism to $(\mathbb{C},+)$. Since $(\mathbb{C},+)$ is abelian, this homomorphism must factor through $H_1(M,\mathbb{Z}) = \pi_1(M,m)^{ab}$.

Less well-known is the following definition:

Definition 5.2. If $\omega_1, \omega_2, \cdots, \omega_r$ are differential 1-forms on M, and $\omega \in PM$, then we define the iterated integral

$$\int_\gamma \omega_1\omega_2\cdots\omega_r$$

as follows. Define $f_j(t)$ to be the piecewise smooth complex valued function on $[0,1]$ such that $\gamma^*\omega_j = f_j(t)\,dt$. Then we define

$$\int_\gamma \omega_1\omega_2\cdots\omega_r := \int_{0\le t_1\le t_2\le\cdots\le t_r\le 1} f_1(t_1)f_2(t_2)\cdots f_r(t_r)\,dt_1dt_2\cdots dt_r.$$

Remark 5.3. The reason for the name *iterated integral* is as follows. Suppose $x, y \in M$, and we restrict to paths γ from x to y. If we view the output as a function of y, then this function may be defined by iteratively taking antiderivatives. We take the antiderivative of ω_1 along γ to get a function on the path γ. We then multiply this function by ω_2 to get another differential form along γ, and take the antiderivative of that differential form. We take the resulting function, multiply by ω_3, antidifferentiate, and so and so forth, until we antidifferentiate a function times ω_r to produce our function of y. The constant of integration is chosen at each stage such that the function vanishes at x.

This defines a function $\int \omega_1\omega_2\cdots\omega_r \colon PM \to \mathbb{C}$. Under certain conditions, it factors through homotopy relative to endpoints and therefore defines a function on fundamental groups:

Fact 5.4. *The iterated integral $\int_\gamma \omega_1\omega_2\cdots\omega_r$ depends only on the homotopy class of γ relative to the endpoints iff each ω_j is closed, and $\omega_j \wedge \omega_{j+1} = 0$ for $j = 1, \cdots, r-1$. In that case, for each $m \in M$, it defines a function*

$$\int \omega_1\cdots\omega_r \colon \pi_1(M,m) \to \mathbb{C}.$$

We may extend linearly to a functional

$$\int \omega_1\cdots\omega_r \colon \mathbb{Q}[\pi_1(M,m)] \to \mathbb{C} \tag{4}$$

on the group ring $\mathbb{Q}[\pi_1(M,m)]$ of $\pi_1(M,m)$.

Remark 5.5. If M is a one-dimensional complex manifold, and ω_j are all holomorphic 1-forms, then the condition of Fact 5.4 is automatically satisfied.

Remark 5.6. There is a more general condition, due to Chen, which ensures that the iterated integral will be homotopy invariant. This will be described in Section 5.2 as an integrability condition on a certain vector bundle with connection.

The following fact shows that iterated integrals can detect elements of $\pi_1(M,m)$ not visible in $H_1(X,\mathbb{Z})$:

Example 5.7. If $\alpha, \beta \in \pi_1(M,m)$, then

$$\int_{\alpha\beta\alpha^{-1}\beta^{-1}} \omega_1\omega_2 = \begin{vmatrix} \int_\alpha \omega_1 & \int_\alpha \omega_2 \\ \int_\beta \omega_1 & \int_\alpha \omega_2 \end{vmatrix}$$

Thus the function $\int \omega_1\omega_2 \colon \pi_1(M,m) \to \mathbb{C}$ does not factor through $\pi_1(M,m)^{ab}$. On the other hand, the property (2) of $\int \omega$ can be restated by saying that $\int \omega_1 \cdots \omega_r$ kills $(\alpha-1)(\beta-1)$ for every $\alpha, \beta \in \pi_1(M,m)$. More generally, one may prove the following:

Fact 5.8. *Let J be the augmentation ideal of $\mathbb{Q}[\pi_1(M,m)]$. The functional*

$$\int \omega_1 \cdots \omega_r \colon \mathbb{Q}[\pi_1(M,m)] \to \mathbb{C}$$

vanishes on elements of J^{r+1}.

We will not prove this fact in this section. Along with Fact 5.4 above and Fact 5.15 below, we will prove it in Section 5.3 as an easy corollary of the theory of vector bundles with unipotent connection.

Then for any r and sequence $\omega_1 \cdots \omega_r$ of differential forms satisfying the condition of homotopy invariance, we get a functional

$$\int \omega_1 \cdots \omega_r \in \mathrm{H}om_{\mathbb{Q}}(\mathbb{Q}[\Gamma]/J^{r+1}, \mathbb{C}),$$

thus for any r, we have

$$\int \omega_1 \cdots \omega_r \in \varinjlim \mathrm{H}om_{\mathbb{Q}}(\mathbb{Q}[\Gamma]/J^{m}, \mathbb{C}) = \mathcal{O}(\pi_1(M,m)_{\mathbb{C}}),$$

where $\pi_1(M,m)_{\mathbb{C}}$ is the unipotent completion of $\pi_1(M,m)$ over $\mathbb{C}$ via Construction 4.2.

Part of Chen's π_1 de Rham theorem (c.f. [Hai05, Theorem 9]) states:

Theorem 5.9. *$\mathcal{O}(\pi_1(M,m)_{\mathbb{C}})$ is spanned as a vector space over $\mathbb{C}$ by functionals of the form $\int \omega_1 \cdots \omega_r$ as $\omega_1, \cdots, \omega_r$ vary over differential 1-forms on M for which the corresponding iterated integral is homotopy-invariant.*

Remark 5.10. In fact, one need only choose the ω_i form a fixed set of differential 1-forms whose cohomology classes span the first cohomology group.

Remark 5.11. The unit element of the ring $\mathcal{O}(\pi_1(M,m)_{\mathbb{C}})$ corresponds by convention to the empty sequence of differentials forms, i.e., to $r = 0$.

Notice that we have not discussed the presence (or absence) of relations between the symbols $\int \omega_1 \cdots \omega_r$. Chen's full theorem describes $\mathcal{O}(\pi_1(M,m)_{\mathbb{C}})$ as the space spanned by homotopy-invariant iterated integrals $\int \omega_1 \cdots \omega_r$ modulo certain relations. More precisely, these relations are given by a differential in the bar construction applied to the differential graded algebra of differential forms on M. Furthermore, the condition of homotopy-invariance may

While we do not go into the details of the bar construction, we note the following important consequence:

Fact 5.12. *Suppose the fundamental group of M is a free group (e.g., if $M = X^{\mathrm{an}}$ for X a smooth affine algebraic curve over $\mathbb{C}$). Choose a sequence of differential 1-forms $\eta_1, \cdots, \eta_k$ whose cohomology classes span $H^1(M, \mathbb{C})$. Then the set of iterated integrals*

$$\int \omega_1 \cdots \omega_r$$

ranging over nonnegative integers r *and*

$$\omega_i \in \{\eta_1, \cdots, \eta_k\}$$

forms a basis of the vector space $\mathcal{O}(\pi_1(M,m)_{\mathbb{C}})$.

5.1.1. *Iterated Integrals of Algebraic Differential Forms.* Suppose $M = X_{\mathbb{C}}^{\mathrm{an}}$ for X a variety over a subfield K of $\mathbb{C}$, and fix $m \in X(K)$. If X is affine, then the de Rham cohomology of M is generated over $\mathbb{C}$ by the classes of algebraic differential forms on X. In that case, we make the following definition:

Definition 5.13. We define $\mathcal{O}(\pi_1^{\mathrm{dR}}(X,m))$ to be the additive subgroup of $\mathcal{O}(\pi_1(M,m)_{\mathbb{C}})$ spanned by iterated integrals of the form

$$\int \omega_1 \cdots \omega_r$$

for $\omega_1, \cdots, \omega_r$ *algebraic* differential forms on X.

It is clear that this is a K-vector space. It is not clear that it is either a ring or a Hopf algebra. However, the following two facts imply that it is indeed a sub-Hopf algebra over K:

Fact 5.14 (Product Formula). *For* $\gamma \in PM$ *and* $\omega_1, \cdots, \omega_r, \omega_{r+1}, \cdots, \omega_{r+s}$ *differential* 1*-forms on* M*, we have*

$$\int_\gamma \omega_1 \cdots \omega_r \int_\gamma \omega_{r+1} \cdots \omega_{r+s} = \sum_{\sigma \in \text{Ш}(r,s)} \int_\gamma \omega_{\sigma(1)} \cdots \omega_{\sigma(r+s)},$$

where $\text{Ш}(r,s)$ *is the subgroup of the symmetric group* S_{r+s} *consisting of* (r,s)-shuffle permutations*, i.e., permutations that are monotone when restricted to the subsets* $\{1, \cdots, r\}$ *and* $\{r+1, \cdots, r+s\}$ *of* $\{1, \cdots, r+s\}$.

Fact 5.15 (Coproduct Formula). *For* $\alpha, \beta \in PM$ *for which* $\alpha(1) = \beta(0)$ *and* $\omega_1, \cdots, \omega_r$ *differential* 1*-forms on* M*, we have*

$$\int_{\alpha\beta} \omega_1 \cdots \omega_r = \sum_{i=0}^{r} \int_\alpha \omega_1 \cdots \omega_i \int_\beta \omega_{i+1} \cdots \omega_r,$$

where $\omega_1 \cdots \omega_i$ *denotes the empty sequence when* $i = 0$*, and so does* $\omega_{i+1} \cdots \omega_r$ *when* $i = r$.

In particular, the coproduct of $\int \omega_1 \cdots \omega_r$ *in the Hopf algebra* $\mathcal{O}(\pi_1(M,m)_{\mathbb{C}})$ *is*

$$\sum_{i=0}^{r} \int \omega_1 \cdots \omega_i \otimes \int \omega_{i+1} \cdots \omega_r.$$

It follows that $\mathcal{O}(\pi_1^{\mathrm{dR}}(X,m))$ is a Hopf algebra over K.

Definition 5.16. We define the *unipotent algebraic de Rham fundamental group*

$$\pi_1^{\mathrm{dR}}(X,m)$$

of the scheme X at $m \in X(K)$ as the group scheme

$$\operatorname{Spec} \mathcal{O}(\pi_1^{\mathrm{dR}}(X,m))$$

over K.

When K is a finite extension of $\mathbb{Q}_p$, it is naturally isomorphic to the group defined using D_{dR} in Section 4.2.2.

When X is affine, and X^{an} has free fundamental group (e.g., if X is a smooth affine curve), then Fact 5.12 holds for $\mathcal{O}(\pi_1^{\mathrm{dR}}(X,m))$ in place of $\mathcal{O}(\pi_1(X^{\mathrm{an}},m)_{\mathbb{C}})$ with $\eta_1,\cdots,\eta_k$ all algebraic differential 1-forms.

Remark 5.17. We will explain how to define the unipotent algebraic de Rham fundamental group for arbitrary smooth varieties using the Tannakian formalism in Section 5.2. However, there is another, fairly direct way to extend Definition 5.16 to the case of non-affine varieties.

Recall Van Kampen's Theorem, which states that if M is a connected topological manifold with open subsets U and V covering M, and $m \in U \cap V$, then $\pi_1(M,m)$ is isomorphic to the pushout (colimit) of the natural diagram

$$\begin{tikzcd} \pi_1(U\cap V,m) \arrow[r] \arrow[d] & \pi_1(U,m) \\ \pi_1(V,m) & \end{tikzcd}$$

The unipotent completion functor is a left adjoint by Construction 4.5, hence it commutes with colimits, and thus Van Kampen's Theorem holds for unipotent fundamental groups. If X is a general smooth variety, we may cover it by affine opens such that the pairwise intersections are affine. Then we define the algebraic de Rham fundamental group of X to be the colimit of the corresponding diagram of unipotent algebraic de Rham fundamental groups of affine open subvarieties.

5.2. **De Rham Fundamental Groups via Vector Bundles with Unipotent Connection.** There is a more elegant yet more abstract definition of $\pi_1^{\mathrm{dR}}(X)$ as the Tannakian fundamental group of the category of algebraic vector bundles with unipotent algebraic connection. To explain the definition, we first review the classical relationship between fundamental groups and vector bundles with connection, known as the Riemann-Hilbert correspondence.

For this we recall the definition of a connection, analogously in three contexts. Let $(M,\mathcal{O}_M)$ be a ringed space that is either

(1) A smooth manifold M equipped with its sheaf $\mathcal{O}_M$ of C^∞ functions.
(2) A complex manifold M equipped with its sheaf $\mathcal{O}_M$ of holomorphic functions.
(3) A smooth variety M over a field equipped with its sheaf $\mathcal{O}_M$ of algebraic functions.

In each case, we let Ω_M^i refer to the sheaf of C^∞ (resp. holomorphic, algebraic) differential i-forms, and we let $d\colon \mathcal{O}_M \to \Omega_M^1$ be the canonical derivation.

Definition 5.18. If E is a sheaf of modules over $\mathcal{O}_M$, then a connection ∇ on E is a map

$$\nabla\colon E \to E\otimes\Omega_M^1$$

of sheaves of abelian groups satisfying the Leibniz rule

$$\nabla(fs) = f\nabla(s) + \nabla(s)\otimes df$$

for all $f \in \mathcal{O}_M(U)$ and $s \in E(U)$ and open sets $U \subseteq M$.

We will focus mainly on the case when E is locally free, i.e., a vector bundle. We let r denote the rank of E as a vector bundle.

5.2.1. *Differential Equations as Connections on Vector Bundles.* Locally, such a ∇ is given by a differential operator, and the condition $\nabla(s) = 0$ is a system of linear ordinary differential equations (ODEs. More specifically, let U be an open subset, and choose an isomorphism (trivialization)

$$E\big|_U \cong \mathcal{O}_M^r\big|_U,$$

so that any $s \in E(U)$ may be written as

$$(f_1, \cdots, f_r) = \sum_{i=1}^r f_i s_i$$

for $f_i \in \mathcal{O}_M(U)$, where $s_i \in E(U)$ denote the section for which $f_i = 1$ and $f_j = 0$ for $j \neq i$.

For $1 \leq i, j \leq r$, we define ω_{ij} by

$$\nabla(s_j) = \sum_{i=1}^r s_i \otimes \omega_{ij}.$$

The Leibniz rule implies that for a general $s = (f_1, \cdots, f_r)$, we have

$$\nabla(s) = \sum_{i=1}^r s_i \otimes (df_i + \sum_{j=1}^r f_j \omega_{ij}).$$

Letting Ω[15] denote the matrix of differential 1-forms $\{\omega_{ij}\}$, we may write the previous equation in the simple form

$$\nabla = d + \Omega.$$

In particular, relative to a trivialization, a connection on a rank r vector bundle is the same thing as an $r \times r$ matrix of differential 1-forms. We define

Definition 5.19. A section $s \in E(U)$ is *horizontal* if $\nabla(s) = 0$.

The condition that s is horizontal is none other than the condition that the components $f_1, \cdots, f_r$ of s satisfy the system of linear ODEs:

$$df_i = -\sum_{j=1}^r f_j \omega_{ij}, \qquad i = 1, \cdots, r,$$

also written in matrix form

$$d\underline{f} = -\Omega \underline{f},$$

where $\underline{f}$ denotes the column vector associated to $(f_1, \cdots, f_r)$.

We will explain the differential equation and thus vector bundle with connection associated with an iterated integral in Section 5.3. We will now discuss some abstract properties of connections and their relationship to fundamental groups. The reader who is not already familiar with connections may prefer to skip to Section 5.3 to gain intuition from some concrete examples of connections.

[15]Many texts denote the matrix by Γ and refer to its entries as *Christoffel symbols*.

5.2.2. *Category of Vector Bundles with Flat Connection.*

Definition 5.20. Let (E, ∇) be a vector bundle with connection. Then we define the *curvature* of ∇

$$\nabla^2 \in \mathrm{End}(E) \otimes \Omega^2_M$$

as follows. We choose an open set U and a trivialization of E on U. Then in the notation of Section 5.2.1, we set

$$\nabla^2\big|_U := d\Omega + \Omega \wedge \Omega,$$

where $d\Omega$ denotes componentwise exterior differentiation, and $\Omega \wedge \Omega$ is defined as a matrix multiplication using the wedge product.

Then ∇^2 well-defined (i.e., independent of trivialization), a fact whose proof we will not discuss.

Our only reason for introducing the notion of curvature is the following definition:

Definition 5.21. A connection (E, ∇) is *flat* (also called *integrable*) if $\nabla^2 = 0$.

The collection of all vector bundles with flat connection forms an abelian tensor category:

Definition 5.22. The category

$$\mathrm{Conn}(M)$$

of vector bundles with flat connection on M has objects vector bundles equipped with a flat connection and morphisms maps of vector bundles that intertwine the two connections.

If (E_1, ∇_1) and (E_2, ∇_2) are vector bundles with flat connection, we define the tensor product connection on $E_1 \otimes E_2$ to be the connection ∇ defined by

$$\nabla(s_1 \otimes s_2) = \nabla_1(s_1) \otimes s_2 + s_1 \otimes \nabla_2(s_2)$$

for $U \subseteq M$ open, $s_1 \in E_1(U)$, and $s_2 \in E_2(U)$.

The unit object for this tensor product is given by the trivial rank 1 vector bundle $\mathcal{O}_M$ equipped with the trivial connection $\nabla = d \colon \mathcal{O}_M \to \Omega^1_M$.

5.2.3. *Connections and Fundamental Groups.* Let M be a connected smooth or complex manifold and $m \in M$. Then the classical Riemann-Hilbert correspondence gives a one-to-one correspondence between vector bundles with flat connection on M and representations of the fundamental group. To do this, we need to define an action of $\pi_1(M, m)$ on the fibers of a vector bundle with flat connection:

Construction 5.23. Let (E, ∇) be a vector bundle with flat connection on a pointed smooth (resp. complex) manifold (M, m). Let $\gamma \colon [0, 1] \to M$ be a loop based at m. We define the *parallel transport* endomorphism of E_m defined by γ as follows.

Let $v \in E_m$. Then we choose a section s of E along γ such that $s(0) = v$, and $\nabla(s) = 0$. A section along γ refers to a map $s \colon [0, 1] \to E$ whose composition with the projection $E \to M$ is γ, and the condition $\nabla(s) = 0$ means that locally on $[0, 1]$, we can write s as the restriction of a horizontal section on some open of M. The existence and uniqueness of such an s follows from the existence and uniqueness theorems for solutions to systems of linear ODEs (resp. holomorphic systems of linear ODEs).

Then we define $\gamma(v)$ to be $s(v)$. The uniqueness ensures that this is well-defined relative to γ.

Fact 5.24. *The parallel transport of Construction 5.23 depends only on the homotopy class of γ relative to its endpoints iff the connection ∇ is flat. In thise case, we call parallel transport the* monodromy action*, and it defines a group action of $\pi_1(M, m)$ on E_m.*

The Riemann-Hilbert correspondence then states:

Theorem 5.25. *Let (M, m) be a connected pointed smooth or complex manifold. There is an equivalence of categories between*

$$\mathrm{Conn}(M)$$

and the category

$$\mathbf{Rep}_{\mathbb{C}}(\pi_1(M, m))$$

of $\mathbb{C}$-linear representations of $\pi_1(M, m)$, sending (E, ∇) to the fiber E_m with action given by Fact 5.24.

Remark 5.26. There is an intermediate notion of *local system*, which allows us to define a functor in the other direction and to prove this correspondence. If R is a field, then an R-linear local system is a sheaf of finite-dimensional R-vector spaces locally isomorphic to a constant sheaf of the form $\underline{R}^r$. Then the theory of covering spaces for fundamental groups allows one to show that on a connected pointed manifold (M, m), the correspondence sending a local system $\mathcal{F}$ to $\mathcal{F}_m$ is an equivalence of categories between R-linear local systems and R-linear representations of $\pi_1(M, m)$.

If $\mathcal{F}$ is a $\mathbb{C}$-linear local system, then $\mathcal{F} \otimes_{\underline{\mathbb{C}}} \mathcal{O}_M$ has the structure of a locally free sheaf of modules (hence vector bundle), and there is a natural connection on it defined by declaring all sections of $\mathcal{F}$ to be horizontal. In the other direction, if (E, ∇) is a flat connection on a vector bundle, then $\ker \nabla$[16] is a $\mathbb{C}$-linear local system.

Remark 5.27. If M is a smooth (real) manifold, there is an $\mathbb{R}$-linear version of connections and Riemann-Hilbert. However, we are interested eventually in algebraic varieties, so we focus on the complex version.

Remark 5.28. In case M is not connected, or one does not wish to choose a basepoint, there is a version using the fundamental groupoid of M in place of $\pi_1(M, m)$.

Because we deal with unipotent fundamental groups, we restrict to the category

$$\mathrm{Un}(M)$$

of unipotent objects (c.f. Definition 4.4) of $\mathrm{Conn}(M)$. Then for a smooth or complex manifold M, Riemann-Hilbert induces an equivalence of categories

$$\mathrm{Un}(M) \cong \mathbf{Rep}_{\mathbb{C}}^{\mathrm{alg}}(\pi_1(M, m)_{\mathbb{C}}).$$

5.2.4. *Algebraic Vector Bundles and the de Rham Fundamental Group.* Suppose first that X is a proper smooth algebraic variety over a field $K \subseteq \mathbb{C}$. Then every algebraic vector bundle with algebraic connection (E, ∇) gives rise to a corresponding holomorphic vector bundle with holomorphic connection on the complex manifold $X_{\mathbb{C}}^{\mathrm{an}}$ associated to the algebraic variety $X_{\mathbb{C}}$. The GAGA principle of Serre implies that this is an equivalence:

[16] We take the kernel in the category of sheaves of abelian groups.

Fact 5.29. *For a smooth proper algebraic variety X, the functor from* $\mathrm{Conn}(X_{\mathbb{C}})$ *to* $\mathrm{Conn}(X^{\mathrm{an}})$ *sending an algebraic vector bundle with flat connection on $X_{\mathbb{C}}$ to the corresponding holomorphic object on X^{an} is an equivalence of categories.*

Remark 5.30. This equivalence clearly respects the tensor category structures and thus extends to an equivalence between $\mathrm{Un}(X_{\mathbb{C}})$ and $\mathrm{Un}(X^{\mathrm{an}})$

Suppose X is a smooth but not necessarily proper algebraic variety. Then one cannot directly apply GAGA, and the functor of Fact 5.29 is no longer an equivalence in general. Nonetheless, via the notion of regular singularities ([Del70, Définition 4.5]), Deligne shows that it is an equivalence for the subcategory $\mathrm{Un}(X)$:[17]

Fact 5.31. *For a smooth algebraic variety X, the functor from* $\mathrm{Un}(X_{\mathbb{C}})$ *to* $\mathrm{Un}(X^{\mathrm{an}})$ *is an equivalence of categories.*

If we remember that X is defined over K, we may consider algebraic vector bundles with flat connection on X instead of on $X_{\mathbb{C}}$. We denote the category of such objects by $\mathrm{Conn}(X)$, and the subcategory of unipotent objects by $\mathrm{Un}(X)$.

Let us assume that $X(K)$ is nonempty and fix $x \in X(K)$. Then $\mathrm{Un}(X)$ is a neutral Tannakian category, with fiber functor given by the stalk at x.

Definition 5.32. We define $\pi_1^{\mathrm{dR}}(X, x)$ as the Tannakian fundamental group of the category $\mathrm{Un}(X)$ with fiber functor at x; i.e., it is the unique pro-unipotent group for which there is an equivalence of categories respecting the tensor product

$$\mathrm{Un}(X) \cong \mathbf{Rep}_K^{\mathrm{alg}}(\pi_1^{\mathrm{dR}}(X, x))$$

and intertwining the fiber functor $(E, \nabla) \mapsto E_x$ with the forgetful functor $\mathbf{Rep}_K^{\mathrm{alg}}(\pi_1^{\mathrm{dR}}(X, x)) \to \mathrm{Vect}_K$.

The Riemann-Hilbert correspondence gives a comparison isomorphism

$$\pi_1^{\mathrm{dR}}(X, x) \otimes_K \mathbb{C} = \pi_1^{\mathrm{dR}}(X_{\mathbb{C}}, x) \cong \pi_1(X^{\mathrm{an}}, x)_{\mathbb{C}}. \tag{5}$$

There is a natural isomorphism between the algebraic de Rham fundamental group of Section 5.2 and that of Section 5.1 compatible with (5),

5.2.5. *Deligne's Canonical Extension.* While we have explained everything about connections necessary for defining the algebraic de Rham fundamental group, there is another topic worth mentioning. It is the notion of Deligne's *canonical extension* of a vector bundle with connection from a noncompact smooth algebraic variety to a compactification.

We let X denote an algebraic curve over a field K of characteristic 0, $\overline{X}$ the unique smooth compactification of X, and $Y = \overline{X} \setminus X$. The following is [Del70, Proposition 5.2]:

Fact 5.33. *Given $(E, \nabla) \in \mathrm{Un}(X)$, there is a unique extension of (E, ∇) to a vector bundle $\overline{E}$ and a meromorphic connection $\overline{\nabla}$ on $\overline{E}$ such that for each point $y \in Y$*

(1) There is a trivialization of $\overline{E}$ in a neighborhood of y on which the matrix Ω consists of differential forms with at most simple poles at y

(2) If we take the residues of Ω componentwise, then the resulting matrix is nilpotent

[17]More precisely, he shows it is an equivalence on the subcategory of $\mathrm{Conn}(X)$ of those connections with regular singularities ([Del70, Théorème 5.9]) and then shows that $\mathrm{Un}(X)$ is contained within this subcategory ([Del89, 10.25]).

Then $(\overline{E}, \overline{\nabla})$ *is known as the* canonical extension[18] *of* (E, ∇).

Remark 5.34. The two conditions in Fact 5.33 amount to the statement that $(\overline{E}, \overline{\nabla})$ is a unipotent object of the category of vector bundles with meromorphic connection on $\overline{X}$.

There's a very important point about Fact 5.33 that bears repeating:

The vector bundle $\overline{E}$ depends not only on E but also on ∇.

That is, we could have two different connections ∇_1 and ∇_2 on the same vector bundle E, for which the corresponding extensions are not isomorphic even as vector bundles.

One reason we care about the canonical extension is that it interacts nicely with the Hodge filtration. To explain the relationship, let $\mathrm{Un}^{\mathrm{vect}}(\overline{X})$ denote the category of unipotent algebraic vector bundles on $\overline{X}$. By a unipotent algebraic vector bundle, we mean a unipotent object in the abelian tensor category of coherent sheaves on $\overline{X}$.

While the category of all vector bundles on a positive-dimensional scheme is not an abelian category,[19] the category $\mathrm{Un}^{\mathrm{vect}}$ of a proper scheme is an abelian and in fact Tannakian category. This is due to the fact that every morphism between trivial vector bundles on a proper scheme is constant.

Deligne's canonical extension thus provides a canonical extension functor:

$$\mathrm{Un}(X) \to \mathrm{Un}^{\mathrm{vect}}(\overline{X}).$$

We have the following fact:

Fact 5.35. *There is an equivalence*

$$\mathrm{Un}^{\mathrm{vect}}(\overline{X}) \cong \mathbf{Rep}_K^{\mathrm{alg}}(F^0\pi_1^{\mathrm{dR}}(X,x)) \tag{6}$$

for which the canonical extension functor is induced by restriction along the inclusion

$$F^0\pi_1^{\mathrm{dR}}(X,x) \hookrightarrow \pi_1^{\mathrm{dR}}(X,x).$$

Remark 5.36. The LHS of the equivalence (6) depends only on $\overline{X}$ and not on X. This shows that $F^0\pi_1^{\mathrm{dR}}(X) = F^0\pi_1^{\mathrm{dR}}(\overline{X})$.

Remark 5.37. We will give a nice description of this functor at the end of Section 5.3.1 when (E, ∇) is the rank 2 connection associated to a closed differential 1-form.

5.3. **Iterated Integrals and Vector Bundles with Connection.** We now explain how to combine the approaches of Sections 5.1 and 5.2.

5.3.1. *Unipotent Connections for Ordinary Line Integrals.* We first explain how to think of an ordinary (abelian) line integral in terms of a vector bundle with connection. Let ω be a 1-form on M, and let γ be a path on M from x to y. Then evaluating $\int_\gamma \omega$ is the same solving the differential equation

$$df = \omega$$

along the path γ subject to the initial condition $f(x) = 0$.

[18] *prolongement canonique* in French

[19] And the category of coherent sheaves, while an abelian tensor category, is not *rigid*, so it is not a Tannakian category.

One problem with this differential equation is that it is not homogeneous linear. In other words, the set of solutions do not form a vector space. The solution to this problem is to consider the system of equations

$$\begin{aligned} df - \omega g &= 0 \\ dg &= 0. \end{aligned}$$

The condition $dg = 0$ ensures that g is constant. If we include the initial condition $(f(x), g(x)) = (0, 1)$, then $f(y)$ indeed equals $\int_\gamma \omega$.

The differential equation above may be rephrased in the matrix form

$$dv = \begin{pmatrix} 0 & \omega \\ 0 & 0 \end{pmatrix} v,$$

where v is the column vector $\begin{pmatrix} f \\ g \end{pmatrix}$. In other words, the solutions to this differential equation are horizontal sections of the connection ∇_ω on $E_\omega := \mathcal{O}_M^2$ given by

$$\Omega_\omega := -\begin{pmatrix} 0 & \omega \\ 0 & 0 \end{pmatrix}.$$

The parallel transport is given by the matrix

$$A_\omega(\gamma) := \begin{pmatrix} 1 & \int_\gamma \omega \\ 0 & 1 \end{pmatrix}.$$

This matrix is a unipotent matrix, corresponding to the fact that ∇_ω is a unipotent connection, corresponding to a unipotent representation of the fundamental group. The matrix Ω_ω is not unipotent but rather nilpotent; the reason is that the Lie algebra of the group of unipotent matrices is the set of nilpotent matrices.

The curvature of this connection (relative to the given trivialization) is simply the matrix

$$\begin{pmatrix} 0 & d\omega \\ 0 & 0 \end{pmatrix}.$$

In other words, ∇_ω is flat iff ω is closed.

Since it is well-known that $\int_\gamma \omega$ depends only on the homotopy class of γ relative to its endpoints iff ω is closed, this provides a simple proof in this case of the claim in Fact 5.24 that the parallel transport depends only on the homotopy class of γ[20] iff the connection is flat.

Let us see what happens in the context and notation of Section 5.2.5. In this case, algebraic de Rham cohomology $H^1_{\mathrm{dR}}(X)$ is computed as the hypercohomology

$$\mathbb{H}^1(X, \Omega^\bullet_{\overline{X}}(\log Y))$$

of the de Rham complex with logarithmic singularities on T. The first term of this complex is simply $\mathcal{O}_{\overline{X}}$. One consequence of this is that there is a map $H^1_{\mathrm{dR}}(X) \to H^1(\overline{X}, \mathcal{O}_{\overline{X}})$ coming from the Hodge-to-de Rham spectral sequence. The map is related to the canonical extension functor of Section 5.2.5 as follows. Let $\overline{E}_\omega \in \mathrm{Un}^{\mathrm{vect}}(\overline{X})$ denote the canonical extension of $(E_\omega, \nabla_\omega)$. Then $\overline{E}_\omega$ is an extension

$$0 \to \mathcal{O}_{\overline{X}} \to \overline{E}_\omega \to \mathcal{O}_{\overline{X}} \to 0.$$

[20]From now on we omit the phrase 'relative to its endpoints' as that is understood.

This extension represents a class in

$$\mathrm{Ext}^1_{\mathrm{Coh}(\overline{X})}(\mathcal{O}_{\overline{X}}, \mathcal{O}_{\overline{X}}) = H^1(\overline{X}, \mathcal{O}_{\overline{X}}).$$

Then this class is precisely the image in $H^1(\overline{X}, \mathcal{O}_{\overline{X}})$ of the cohomology class represented by ω.

5.3.2. *Unipotent Connections for Iterated Integrals.* Let $\underline{\omega} = \omega_1, \omega_2, \cdots, \omega_r$ be a sequence of differential forms on M and γ a path from x to y. The procedure for iterated integration described in Remark 5.3 amounts to solving the following system of differential equations

$$\begin{aligned} df_0 &= 0 \\ df_i - \omega_i &= 0 \qquad i = 1, \cdots, r \end{aligned}$$

along with the initial conditions $f_0(x) = 1$ and $f_i(x) = 0$ for $i \geq 1$, so that

$$f_r(y) = \int_\gamma \omega_1 \cdots \omega_r.$$

Letting $\underline{f}$ denote the column vector associated to $(f_0, \cdots, f_r)$, we may write this equation as

$$d\underline{f} = -\Omega_{\underline{\omega}} \underline{f}$$

where

$$\Omega_{\underline{\omega}} = -\begin{pmatrix} 0 & 0 & 0 & \dots & 0 \\ \omega_1 & 0 & 0 & \dots & 0 \\ 0 & \omega_2 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \omega_r & 0 \end{pmatrix}$$

We refer to $\mathcal{O}_M^{r+1}$ with the connection given by $\Omega_{\underline{\omega}}$ as $(E_{\underline{\omega}}, \nabla_{\underline{\omega}})$. The associated parallel transport matrix along γ is

$$A_{\underline{\omega}}(\gamma) := \begin{pmatrix} 1 & 0 & 0 & 0 & \dots & 0 \\ \int_\gamma \omega_1 & 1 & 0 & 0 & \dots & 0 \\ \int_\gamma \omega_1\omega_2 & \int_\gamma \omega_2 & 1 & 0 & \dots & 0 \\ \int_\gamma \omega_1\omega_2\omega_3 & \int_\gamma \omega_2\omega_3 & \int_\gamma \omega_3 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & 0 \\ \int_\gamma \omega_1 \cdots \omega_r & \int_\gamma \omega_2 \cdots \omega_r & \dots & \int_\gamma \omega_{r-1}\omega_r & \int_\gamma \omega_r & 1 \end{pmatrix}$$

This expression provides a quick proof of Fact 5.15. Indeed, by the group action property of Fact 5.24, $A_{\underline{\omega}}(\alpha\beta) = A_{\underline{\omega}}(\beta) A_{\underline{\omega}}(\alpha)$. The lower-left entry of this product is then the RHS of Fact 5.15.

The curvature may be expressed in local coordinates as

$$
\begin{aligned}
\nabla^2_{\underline{\omega}} &= d\Omega_{\underline{\omega}} + \Omega_{\underline{\omega}} \wedge \Omega_{\underline{\omega}} \\
&= -\begin{pmatrix}
0 & 0 & 0 & 0 & \dots & 0 \\
d\omega_1 & 0 & 0 & 0 & \dots & 0 \\
0 & d\omega_2 & 0 & 0 & \dots & 0 \\
0 & 0 & d\omega_3 & 0 & \dots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & 0 \\
0 & 0 & \dots & 0 & d\omega_r & 0
\end{pmatrix}
+
\begin{pmatrix}
0 & 0 & 0 & 0 & \dots & 0 \\
0 & 0 & 0 & 0 & \dots & 0 \\
\omega_2 \wedge \omega_1 & 0 & 0 & 0 & \dots & 0 \\
0 & \omega_3 \wedge \omega_2 & 0 & 0 & \dots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & 0 \\
0 & 0 & \dots & \omega_r \wedge \omega_{r-1} & 0 & 0
\end{pmatrix} \\
&= -\begin{pmatrix}
0 & 0 & 0 & 0 & \dots & 0 \\
d\omega_1 & 0 & 0 & 0 & \dots & 0 \\
\omega_1 \wedge \omega_2 & d\omega_2 & 0 & 0 & \dots & 0 \\
0 & \omega_2 \wedge \omega_3 & d\omega_3 & 0 & \dots & 0 \\
\vdots & \vdots & \ddots & \ddots & \ddots & 0 \\
0 & 0 & \dots & \omega_{r-1} \wedge \omega_r & d\omega_r & 0
\end{pmatrix}.
\end{aligned}
$$

In particular, the connection is flat iff $d\omega_i = 0$ for $i = 1, \cdots, r$ and $\omega_i \wedge \omega_{i+1} = 0$ for $i = 1, \cdots, r-1$. By Fact 5.24, this is equivalent to the iterated integral being homotopy invariant, thus proving Fact 5.4.

5.3.3. *Iterated Integrals as Tannakian Matrix Coefficients.* We conclude Section 5.2 with an explanation of the relationship between Definition 5.16 and Definition 5.32

More specifically, given an iterated integral $\int \omega_1 \cdots \omega_r = \int \underline{\omega}$ on a pointed algebraic variety (X, x) over a subfield $K \subseteq \mathbb{C}$, we explain how to associate a regular function on $\pi_1^{\mathrm{dR}}(X, x)$ using Definition 5.32.

Let $(E_{\underline{\omega}}, \nabla_{\underline{\omega}})$ denote the vector bundle with connection defined in Section 5.3.2. Via Definition 5.32, we may view

$$(E_{\underline{\omega}}, \nabla_{\underline{\omega}})$$

as an object of the category

$$\mathbf{Rep}_K^{\mathrm{alg}}(\pi_1^{\mathrm{dR}}(X, x))$$

with underlying vector space

$$(E_{\underline{\omega}})_x.$$

That this representation is algebraic means (by the functor of points formalism) that for any K-algebra R, we have an action of the abstract group

$$\pi_1^{\mathrm{dR}}(X, x)(R)$$

on

$$(E_{\underline{\omega}})_x \otimes_K R \cong R^{r+1},$$

in a manner functorial in the K-algebra R.

Let

$$v = (1, 0, \dots, 0) \in (E_{\underline{\omega}})_x \otimes_K R \cong (\mathcal{O}_M^{r+1})_x \otimes_K R = R^{r+1}. \tag{7}$$

Notice that this v corresponds to the initial condition mentioned at the beginning of Section 5.3.2. Let $\mathrm{pr}_{r+1} \colon (E_{\underline{\omega}})_x \otimes_K R \to R$ denote projection onto the $r+1$st coordinate via the isomorphism (7).

For $\gamma \in \pi_1^{\mathrm{dR}}(X,x)(R)$, we set

$$\int \underline{\omega}(\gamma) = \mathrm{pr}_{r+1}(\gamma(v)) \in R = \mathbb{A}^1(R)$$

This association is functorial in the K-algebra R and thus defines a morphism

$$\int \underline{\omega} \colon \pi_1^{\mathrm{dR}}(X,x) \to \mathbb{A}^1,$$

i.e., an element of $\mathcal{O}(\pi_1^{\mathrm{dR}}(X,x))$.

Remark 5.38. The association of a regular function f on a Tannakian fundamental group G to an object V of the Tannakian category $\mathcal{C}$, and a vector v and covector c in the fiber of V, is known as a *Tannakian matrix coefficient*. In our case $f = \int \underline{\omega}$, $G = \pi_1^{\mathrm{dR}}(X,x)$, $V = (E_{\underline{\omega}}, \nabla_{\underline{\omega}})$, $\mathcal{C} = \mathrm{Un}(X)$, $v = v$, and $c = \mathrm{pr}_{r+1}$. It is thus called because it sends an element γ of the group G to a certain coefficient of the matrix associated to the action of γ on V in a basis adapted to v and c. One may read more about Tannakian matrix coefficients in [**?**, §2.2].

5.4. **p-adic Iterated Integrals.** We are finally ready to talk about the integration map $\int$ in Kim's cutter. Let

$$\underline{\omega} \in \mathcal{O}(\pi_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}}, O)/F^0\pi_1^{\mathrm{dR}}(X_{K_{\mathfrak{p}}}, O)).$$

Defining the map $\int$ amounts to associating a $\mathbb{Q}_p$-valued function on $X(K_{\mathfrak{p}})$ for each such $\underline{\omega}$. This function will be the iterated Coleman integral

$$\int_O^P \underline{\omega}.$$

We explain how to define iterated Coleman integrals via the formalism of Besser ([Bes02]). The original theory of p-adic iterated integration is due to Coleman ([Col82]). A useful reference is [Bes12, §1.5].

See `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.174.4732&rep=rep1&type=pdf`
and

References

[BDM+19] Jennifer Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman, and Jan Vonk. Explicit Chabauty-Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019.

[Bel09] Joel Bellaiche. An introduction to Bloch and Kato's conjecture. Notes from Lectures at a Clay Summer Institute, 2009.

[Bes02] Amnon Besser. Coleman integration using the Tannakian formalism. *Math. Ann.*, 322(1):19–48, 2002.

[Bes12] Amnon Besser. Heidelberg lectures on Coleman integration. In *The arithmetic of fundamental groups—PIA 2010*, volume 2 of *Contrib. Math. Comput. Sci.*, pages 3–52. Springer, Heidelberg, 2012.

[BK90] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[Bou98] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 1–3.* Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[Bre94] Lawrence Breen. Tannakian categories. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 337–376. Amer. Math. Soc., Providence, RI, 1994.

[Bro13] Francis Brown. Iterated integrals in quantum field theory. In *Geometric and topological methods for quantum field theory*, pages 188–240. Cambridge Univ. Press, Cambridge, 2013.

[Cha41] Claude Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[CK10] John Coates and Minhyong Kim. Selmer varieties for curves with CM Jacobians. *Kyoto J. Math.*, 50(4):827–852, 2010.

[Col82] Robert F. Coleman. Dilogarithms, regulators and p-adic L-functions. *Invent. Math.*, 69(2):171–208, 1982.

[Col85] Robert F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[Del70] Pierre Deligne. *Équations différentielles à points singuliers réguliers*. Lecture Notes in Mathematics, Vol. 163. Springer-Verlag, Berlin-New York, 1970.

[Del89] Pierre Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over* $\mathbf{Q}$ *(Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 79–297. Springer, New York, 1989.

[Dog19] Netan Dogra. Unlikely intersections and the chabauty-kim method over number fields, 2019.

[EH17] Jordan S. Ellenberg and Daniel Rayor Hast. Rational points on solvable curves over $\mathbb{Q}$ via non-abelian chabauty, 2017.

[Fen16] Tony Feng. The BlochâĂŞKato Selmer Group. Lectures for a talk in the Number Theory Learning Seminar at Stanford, 2016.

[Hai02] Richard Hain. Iterated integrals and algebraic cycles: examples and prospects. In *Contemporary trends in algebraic geometry and algebraic topology (Tianjin, 2000)*, volume 5 of *Nankai Tracts Math.*, pages 55–118. World Sci. Publ., River Edge, NJ, 2002.

[Hai05] Richard Hain. Lectures on the hodge-de rham theory of the fundamental group of $\mathbb{P}^1 \setminus \{0, 1\infty\}$, 2005. Arizona Winter School 2005.

[Kim05] Minhyong Kim. The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.*, 161(3):629–656, 2005.

[Kim09] Minhyong Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009.

[MP12] William McCallum and Bjorn Poonen. The method of Chabauty and Coleman. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 99–117. Soc. Math. France, Paris, 2012.

[Qui69] Daniel Quillen. Rational homotopy theory. *Ann. of Math. (2)*, 90:205–295, 1969.

[Ser06] Jean-Pierre Serre. *Lie algebras and Lie groups*, volume 1500 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2006. 1964 lectures given at Harvard University, Corrected fifth printing of the second (1992) edition.

[Sto07] Michael Stoll. Finite descent obstructions and rational points on curves. *Algebra Number Theory*, 1(4):349–391, 2007.

[Sui07] Esther Suisse. Groupes nilpotents sans torsions et complétés de malcev, 2007.

[Vez] Alberto Vezzani. The pro-unipotent completion.

D.C. Department of Mathematics, MIT, 77 Massachusetts Avenue, Cambridge, MA 02139, USA. Email address: `corwind@alum.mit.edu`