

MASSEY PRODUCTS FOR ELLIPTIC CURVES OF RANK 1

MINHYONG KIM

The author must begin with an apology for writing on a topic so specific, so elementary, and so well-understood as the study of elliptic curves of rank 1. Nevertheless, it is hoped that a contribution not entirely without value or novelty is to be found within the theory of *Selmer varieties* for hyperbolic curves, applied to the complement $X = E \setminus \{e\}$ of the origin inside an elliptic curve E over \mathbb{Q} with Mordell-Weil rank 1. Assume throughout this paper that p is an odd prime of good reduction such that $\text{III}(E)[p^\infty]$ is finite and that E has integral j -invariant. All of these assumptions will hold, for example, if E has complex multiplication and $\text{ord}_{s=1} L(E, s) = 1$.

Let \mathcal{E} be a regular \mathbb{Z} -model for E and \mathcal{X} the complement in \mathcal{E} of the closure of e . The main goal of the present inquiry is

to find explicit analytic equations defining $\mathcal{X}(\mathbb{Z})$ inside $\mathcal{X}(\mathbb{Z}_p)$.

The approach of this paper makes use of a *rigidified Massey product* in Galois cohomology.¹ That is, the étale local unipotent Albanese map

$$\mathcal{X}(\mathbb{Z}_p) \xrightarrow{j_{2,1,loc}^{ét}} H_f^1(G_p, U_2)$$

to the level-two local Selmer variety (recalled below) associates to point z a non-abelian cocycle $a(z)$, which can be broken canonically into two components $a(z) = a_1(z) + a_2(z)$, with $a_1(z)$ taking values in

$$U_1 \simeq H_1(\bar{X}, \mathbb{Q}_p) \simeq H_1(\bar{E}, \mathbb{Q}_p) \simeq T_p(E) \otimes \mathbb{Q}_p$$

and $a_2(z)$ in $U^3 \setminus U^2 \simeq \mathbb{Q}_p(1)$. Denoting by $c^p : G_p \rightarrow \mathbb{Q}_p$ the logarithm of the p -adic cyclotomic character, we use a Massey triple product

$$z \mapsto (c^p, a_1(z), a_1(z)) \in H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p$$

to construct a function on the local points of \mathcal{X} . Recall that Massey products are secondary cohomology products arising in connection with associative differential graded algebras (A, d) : If we are given classes $[\alpha], [\beta], [\gamma] \in H^1(A)$ such that

$$[\alpha][\beta] = 0 = [\beta][\gamma],$$

we can solve the equations

$$dx = \alpha\beta, \quad dy = \beta\gamma$$

for $x, y \in A^1$. The element

$$x\gamma + \alpha y \in A^2$$

Received by the editors February 24, 2009 and, in revised form, January 3, 2010.

2010 *Mathematics Subject Classification*. Primary 11G05.

Key words and phrases. Elliptic curve, Selmer variety, Massey product.

¹The reader is invited to consult [7] for the corresponding construction in Deligne cohomology and [27] for a \mathbb{G}_m -analogue.

satisfies

$$d(x\gamma + \alpha y) = dx\gamma - \alpha dy = 0,$$

so that we obtain a class

$$[x\gamma + \alpha y] \in H^2(A).$$

Of course it depends on the choice of x and y , so that the product as a function of the initial triple takes values in

$$H^2(A)/[H^1(A)[\gamma] + [\alpha]H^1(A)].$$

The elements x and y constitute a *defining system* for the Massey product. It is possible, however, to obtain a precise realization taking values in $H^2(G_p, \mathbb{Q}_p(1))$ in the present situation, starting from a non-abelian cocycle $a = a_1 + a_2$ with values in U_2 . For this, we make use, on the one hand, of the component a_2 , which is not a cocycle but satisfies the equation

$$da_2 = -(1/2)(a_1 \cup a_1).$$

That is to say, the cochain $-2a_2$ is one piece of a defining system, already included in the cocycle a . On the other hand, the equation for the other component b of a defining system looks like

$$db = c^p \cup a_1.$$

At this point, the assumption on the elliptic curve comes into play, implying that a_1 is the localization at p of a global cocycle

$$a_1^{glob}$$

with the property that the localizations $a_1^{glob, l}$ at all primes $l \neq p$ are trivial. Since c^p is also the localization of the global p -adic log cyclotomic character c , we get an equation

$$db = c \cup a_1^{glob}$$

to which we may now seek a global solution, i.e., a cochain b on a suitable global Galois group. The main point then is that our assumptions on E can be further used to deduce its existence. Having solved the equation globally, we again localize to a cochain $b^{glob, p}$ on the local Galois group at p . It is then a simple exercise to see that the Massey product

$$b^{glob, p} \cup a_1 + c^p \cup (-2a_2)$$

obtained thereby is independent of the choice of b^{glob} , giving us a well-defined function

$$\psi^p : H_f^1(G_p, U_2) \rightarrow H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p.$$

This function is in fact non-zero and algebraic with respect to the structure of $H_f^1(G_p, U_2)$ as a \mathbb{Q}_p -variety. The main theorem then says:

Theorem 0.1.

$$\psi^p \circ j_{2, loc}^{et}$$

vanishes on the global points $\mathcal{X}(\mathbb{Z}) \subset \mathcal{X}(\mathbb{Z}_p)$.

This result suffices to show the finiteness of integral points. However, the matter of real interest is an explicit computation of the composition $\psi^p \circ j_{2, loc}^{et}$. At this point, the log map to the De Rham realization will intervene, and the third section provides a flavor of the formulas one is to expect. To get explicit expressions we choose a global regular differential form α on E and a differential β of the

second kind with a pole of order two only at $e \in E$ and with the property that $[-1]^*(\beta) = -\beta$. There are then analytic functions

$$\log_\alpha(z) = \int_b^z \alpha, \quad \log_\beta(z) = \int_b^z \beta, \quad D_2(z) = \int_b^z \alpha\beta,$$

on $\mathcal{X}(\mathbb{Z}_p)$ arising via (iterated) Coleman integration.

Corollary 0.2. *Suppose there is a point y of infinite order in $\mathcal{E}(\mathbb{Z})$. Then*

$$\mathcal{X}(\mathbb{Z}) \subset \mathcal{E}(\mathbb{Z}_p)$$

is in the zero set of

$$(\log_\alpha(y))^2(D_2(z) - (1/2)\log_\alpha(z)\log_\beta(z)) - (\log_\alpha(z))^2(D_2(y) - (1/2)\log_\alpha(y)\log_\beta(y)).$$

We obtain thereby a rather harmonious constraint on the locus of global integral points, albeit in an absurdly special situation. In fact, the theorem itself implies that the function of z ,

$$(D_2(z) - (1/2)\log_\alpha(z)\log_\beta(z)) - \frac{(D_2(y) - (1/2)\log_\alpha(y)\log_\beta(y))}{\log_\alpha(y)^2}(\log_\alpha(z))^2,$$

is independent of the choice of y . However, in its present formulation, it requires us to have in hand one integral point before commencing the search for others.

Perhaps naively, the author has believed for some time that a satisfactory description of the set of global points is possible even for general hyperbolic curves, compact or affine, by way of a non-abelian Poitou-Tate duality of sorts, coupled to a non-abelian explicit reciprocity law (cf. [15]). As yet, a plausible formulation of such a duality is unclear, and more so the prospect of applications to Diophantine problems. What is described in the following sections is a faint projection of the phenomenon whose general nature remains elusive, a projection made possible through the most stringent assumptions that are compatible still with statements that are not entirely trivial. For the tentative nature of this exposition then, even more apologies are in order.

1. PRELIMINARY REMARKS

Within the strictures of the present framework, it will be sufficient to work with the Selmer variety associated to $U_2 = U^3 \setminus U$, the first non-abelian level of the \mathbb{Q}_p -pro-unipotent fundamental group

$$U := \pi_1^{u, \mathbb{Q}_p}(\bar{X}, b)$$

of

$$\bar{X} = X \times_{\text{Spec}(\mathbb{Q})} \text{Spec}(\bar{\mathbb{Q}})$$

with a rational tangential base-point b pointing out of the origin of E [5]. Here, the superscript refers to the descending central series (in the sense of pro-algebraic groups)

$$U^1 = U, \quad U^{n+1} = [U, U^n]$$

of U while the subscript denotes the corresponding quotients

$$U_n = U^{n+1} \setminus U.$$

In particular, there is a canonical isomorphism

$$U_1 \simeq H_1(\bar{X}, \mathbb{Q}_p).$$

But since \bar{X} is missing just one point, the map

$$H_1(\bar{X}, \mathbb{Q}_p) \rightarrow H_1(\bar{E}, \mathbb{Q}_p)$$

is an isomorphism when base-changed to \mathbb{C} , and hence, is an isomorphism. That is, we have

$$U_1 \simeq H_1(\bar{X}, \mathbb{Q}_p) \simeq H_1(\bar{E}, \mathbb{Q}_p) \simeq T_p E \otimes \mathbb{Q}_p.$$

There is also an exact sequence

$$0 \rightarrow U^3 \setminus U^2 \rightarrow U_2 \rightarrow U_1 \rightarrow 0.$$

The commutator map induces an anti-symmetric pairing

$$U_1 \otimes U_1 \rightarrow U^3 \setminus U^2,$$

which therefore leads to an isomorphism

$$U^3 \setminus U^2 \simeq \wedge^2 H_1(\bar{E}, \mathbb{Q}_p) \simeq \mathbb{Q}_p(1)$$

as representations for $G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. The logarithm map

$$\log : U \rightarrow L := \text{Lie } U$$

is an isomorphism of schemes allowing us to identify U_2 with $L_2 = L^2 \setminus L$, which, in turn, fits into an exact sequence

$$0 \rightarrow L^3 \setminus L^2 \rightarrow L_2 \rightarrow L_1 \rightarrow 0.$$

If we choose any elements A and B of L_2 lifting a basis of L_1 , then $C := [A, B]$ is a basis for $L^3 \setminus L^2$. Using the Campbell-Hausdorff formula, we can express the multiplication in U_2 , transferred over to L via the logarithm, as

$$(aA + bB + cC) * (a'A + b'B + c'C) = (a + a')A + (b + b')B + (c + c' + (1/2)(ab' - ba'))C.$$

Given such a choice of A and B , we will also denote an element of L_2 as $l = l_1 + l_2$ where l_1 is a linear combination of A and B while l_2 is a multiple of C . In this notation, the group law becomes

$$(l_1 + l_2) * (l'_1 + l'_2) = l''_1 + l''_2,$$

where $l''_1 = l_1 + l'_1$ and $l''_2 = l_2 + l'_2 + (1/2)[l_1, l'_1]$. We simplify notation a bit and put $Z := L^3 \setminus L^2$. The Lie bracket

$$[\cdot, \cdot] : L_2 \otimes L_2 \rightarrow Z$$

factors to a bilinear map

$$L_1 \otimes L_1 \rightarrow Z,$$

which we denote also by a bracket.

Lemma 1.1. *Let p be an odd prime. There is a G -equivariant vector space splitting*

$$s : L_1 \hookrightarrow L_2$$

of the exact sequence

$$0 \rightarrow Z \rightarrow L_2 \xrightarrow{f} L_1 \rightarrow 0.$$

Proof. Denote by i the involution on E that send x to $-x$ for the group law. The origin is fixed and i induces the antipode map on the tangent space $T := T_e(E)$. In particular, we get an isomorphism

$$i_* : \pi_1^{u, \mathbb{Q}_p}(\bar{X}, b) \simeq \pi_1^{u, \mathbb{Q}_p}(\bar{X}, -b).$$

Consider the $\hat{\pi}_1(\bar{X}, b)$ -torsor of paths (for the pro-finite fundamental group) $\hat{\pi}_1(\bar{X}; b, -b)$ from b to $-b$. By definition, we have

$$\hat{\pi}_1(\bar{X}; b, -b) := \text{Isom}(F_b, F_{-b}).$$

Recall briefly the definition of F_v for $v \in T^0 = T \setminus \{0\}$ ([5], section 15). F_v associates to any cover $Y \rightarrow \bar{X}$ the fiber over v of the corresponding cover ('the principal part')

$$Pr(Y) \rightarrow \bar{T}^0 = T^0 \otimes \bar{\mathbb{Q}}$$

of \bar{T}^0 . Now, choose an isomorphism $z : T \simeq \mathbb{A}^1$ that takes b to 1. Then we get an isomorphism $(T^0, b) \simeq (\mathbb{G}_m, 1)$, and the pro- p universal covering of \bar{T}^0 is the pull-back of the tower

$$(\cdot)^{p^n} : \bar{\mathbb{G}}_m \rightarrow \bar{\mathbb{G}}_m.$$

But then, the inverse image of -1 , that is $z^{-1}(-1)$, in each level of the tower gives a compatible G -invariant sequence of elements and trivializes the torsor $\hat{\pi}_1(\bar{T}^0; b, -b)$. Hence, its image in $\hat{\pi}_1(\bar{X}; b, -b)$ will also be a trivialization. We then take the unipotent image of this trivialization to get an isomorphism $t : \pi_1^{u, \mathbb{Q}_p}(\bar{X}, -b) \simeq \pi_1^{u, \mathbb{Q}_p}(\bar{X}, b)$. Note that in the abelianization, we have the canonical isomorphisms

$$\pi_1^{u, \mathbb{Q}_p}(\bar{X}, -b)^{ab} \simeq H_1(\bar{E}, \mathbb{Q}_p) \simeq \pi_1^{u, \mathbb{Q}_p}(\bar{X}, b)^{ab}.$$

Furthermore, for an étale cover $Y \rightarrow \bar{E}$, the principal part $Pr(Y) \rightarrow \bar{T}^0$ extends to an étale cover of \bar{T} , and hence, is trivial. So the image of t acting on $H_1(\bar{E}, \mathbb{Q}_p)$ is the identity. Therefore, we have constructed an isomorphism $I := t \circ i_* : U_2 \simeq U_2$ that lifts the map $x \mapsto -x$ on U_1 . This gives a corresponding Lie algebra isomorphism

$$L_2 \simeq L_2,$$

which we will denote by the same letter I . Since $Z \subset L_2$ is generated by the bracket of two basis elements from L_1 , we see that I restricts to the identity on Z .

Now we define the splitting by putting

$$s(x) := (1/2)(x' - I(x'))$$

for any lift x' of x to L_2 . Since another lift will differ from x' by an element of Z on which I acts as the identity, the formula is independent of the lift. We can then use this independence to check that the map is linear. If x' and y' are lifts of x and y , then $\lambda x' + \mu y'$ is a lift of $\lambda x + \mu y$. So

$$s(\lambda x + \mu y) = (1/2)(\lambda x' + \mu y' - I(\lambda x' + \mu y')) = \lambda(1/2)(x' - I(x')) + \mu(1/2)(y' - I(y')).$$

Similarly, if $g \in G$, then $g(x')$ will be a lift of $g(x)$, so that

$$s(g(x)) = (1/2)(g(x') - I(g(x'))) = (1/2)(g(x') - g(I(x'))) = g(s(x)). \quad \square$$

We will use this splitting to write

$$L_2 = L_1 \oplus Z$$

as a G -representation, so that an arbitrary $l \in L_2$ can be decomposed into $l = l_1 + l_2$ as described above, except independently of a specific basis of L_1 . Using the

identification via the log map, we will abuse notation a bit and write $u = u_1 + u_2$ also for an element of U_2 .

For any $\lambda \in \mathbb{Q}_p$, we then get a Lie algebra homomorphism

$$m(\lambda) : L_2 \rightarrow L_2$$

by defining

$$m(\lambda)l = \lambda l_1 + \lambda^2 l_2,$$

which is furthermore compatible with the G -action. Thus, $m(\lambda)$ can also be viewed as a G -homomorphism of U_2 . We note that the extra notation is used for the moment to distinguish this action of the multiplicative monoid \mathbb{Q}_p from the original scalar multiplication.

We recall the continuous group cohomology [16]

$$H^1(G, U_2) := U_2 \backslash Z^1(G, U_2).$$

The set $Z^1(G, U_2)$ of continuous 1-cocycles of G with values in U_2 consists of continuous maps

$$a : G \rightarrow U_2$$

such that

$$a(gh) = a(g)ga(h).$$

Using the identification of U_2 with $L_2 = L_1 \oplus Z$ just discussed, we will write such a map also as

$$a = a_1 + a_2$$

with a_1 taking values in L_1 and a_2 taking values in Z . The cocycle condition is then given by

$$\begin{aligned} a_1(gh) + a_2(gh) &= (a_1(g) + a_2(g)) * (ga_1(h) + ga_2(h)) \\ &= a_1(g) + ga_1(h) + a_2(g) + ga_2(h) + (1/2)[a_1(g), ga_1(h)]. \end{aligned}$$

In fact, given two cochains c, c' with values in L_1 , we define

$$(c \cup c')(g, h) = [c(g), c'(h)],$$

a cochain with values in Z . The cocycle condition spelled out above then says that

- (1) a_1 is a cocycle with values in L_1 ;
- (2) a_2 is not a cocycle in general, but satisfies

$$ga_2(h) - a_2(gh) + a_2(h) = -(1/2)[a_1(g), ga_1(h)],$$

or, recognizing on the left-hand side the differential of the cochain a_2 ,

$$da_2 = -(1/2)(a_1 \cup a_1).$$

This can be viewed as a Galois-theoretic *Maurer-Cartan equation* (called the *deformation equation* in the introduction to [9], where a differential geometric moduli space of principal bundles is constructed). So even when we have split the Galois action and considered values in a Lie algebra, the non-abelian group structure imposes a condition on the cochains that come together to form non-abelian cocycles. The cohomology set is then defined by taking a quotient under the action of U_2 :

$$(u \cdot a)(g) = ua(g)g(u^{-1}).$$

This discussion carries over verbatim to various local Galois groups $G_l = \text{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$ as l runs over the primes of \mathbb{Q} , which all act on U via the inclusion $G_l \rightarrow G$ induced by an inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_l$, and leading to the cohomology sets $H^1(G_l, U_2)$.

Now we choose p to be an odd place of good reduction for E and denote by T the set $S \cup \{p\}$, where S is a finite set of places that contains the infinite place and the places of bad reduction for E . We let $G_T = \text{Gal}(\mathbb{Q}_T/\mathbb{Q})$ be the Galois group of the maximal extension of \mathbb{Q} unramified outside T . In previous work [4, 16, 17, 18, 19, 20], we have made use of the Selmer variety

$$H_f^1(G, U_2) \subset H^1(G_T, U_2) \subset H^1(G, U_2).$$

By definition, $H_f^1(G, U_2)$ consists of cohomology classes that are unramified outside T and crystalline at p . Associating to a point $x \in X(\mathbb{Q})$ the torsor of paths

$$\pi_1^{u, \mathbb{Q}_p}(\bar{X}; b, x)$$

defines a map

$$X(\mathbb{Q}) \rightarrow H^1(G, U_2)$$

that takes $\mathcal{X}(\mathbb{Z}_S) \subset X(\mathbb{Q})$ to $H_f^1(G, U)$.

Lemma 1.2. *Let $l \neq p$, and $G_l := \text{Gal}(\bar{\mathbb{Q}}_l/\mathbb{Q}_l)$. Then on the globally integral points, the map*

$$\mathcal{X}(\mathbb{Z}) \rightarrow H_f^1(G, U_2) \rightarrow H^1(G_l, U_2)$$

is trivial.

Proof. In fact, we can show that the image of

$$\mathcal{X}(\mathbb{Z}_l) \rightarrow H^1(G_l, U_n)$$

is trivial for all n .

By the assumption on integrality of the j -invariant, E has potentially good reduction everywhere. We fix a normal subgroup $N \subset G_l$ of finite index such that E has good reduction over the fixed field of N . Then by [20], pp. 230-231, the image of

$$\mathcal{X}(\mathbb{Z}_l) \rightarrow H^1(N, U_n)$$

is trivial. That is, if $a(x)$ is a cocycle on G_l corresponding to a point $x \in \mathcal{X}(\mathbb{Z}_l)$, then there is a $u \in U_n$ such that

$$a(x)(h) = u^{-1}h(u)$$

for all $h \in N$. That is,

$$b(x)(g) = ua(x)(g)g(u^{-1})$$

is a cocycle that represents x and $b(x)(h) = e$ for all $h \in N$. Note also that

$$b(x)(gh) = b(x)(g)gb(x)(h) = b(x)(g)ge = b(x)(g)$$

for all $g \in G, h \in N$. Therefore,

$$hb(x)(g) = b(x)(h)hb(x)(g) = b(x)(hg) = b(x)(g(g^{-1}hg)) = b(x)(g)$$

for all $g \in G, h \in N$. That is, all $b(x)(g)$ lie inside the N -fixed part of U_n . However, since all terms in the descending central series filtration of U_n have negative weight, we see that the N -fixed part reduces to the identity. Therefore, $b(x)(g) = e$ and $[a(x)] \in H^1(G_l, U_n)$ is trivial. \square

Note that the proof of the lemma uses the fact that the kernel of

$$H^1(G_l, U_n) \rightarrow H^1(N, U_n)$$

is the image of $H^1(G_l/N, U_n^N)$ even in a non-abelian situation.

Denote by

$$H_{f, \mathbb{Z}}^1(G, U_2) \subset H_f^1(G, U_2)$$

the *fine Selmer variety*, defined to be the intersection of the kernels of the localization maps

$$H_f^1(G, U_2) \rightarrow H^1(G_l, U_2)$$

for all $l \neq p$. Then the previous paragraph says that the image of

$$\mathcal{X}(\mathbb{Z}) \rightarrow H_f^1(G_l, U_2)$$

lies inside

$$H_{f, \mathbb{Z}}^1(G_l, U_2).$$

The action of \mathbb{Q}_p discussed above is G -equivariant for any of the groups G acting on U_2 , and hence, induces an action on $H_{(\cdot)}^1(\cdot, U_2)$ for any of the groups under discussion, which we will denote simply as left multiplication (since here, the danger of confusion with the original scalar multiplication does not arise). By the formula for $m(\lambda)$, at the level of cocycles,

$$\lambda a = \lambda a_1 + \lambda^2 a_2.$$

Note that this action preserves the condition

$$da_1 = (-1/2)[a_1, a_1].$$

2. CONSTRUCTION

Although we will not make use of this fact, the products to be constructed below can be viewed as Massey products in the associative algebra of continuous group cochains with values in a graded Lie algebra constructed as follows:

$$A = L_2^*(1) \oplus \mathbb{Q}_p(1) \oplus L_2.$$

A is a direct sum of five terms,

$$A_{-2} \oplus A_{-1} \oplus A_0 \oplus A_1 \oplus A_2,$$

where $A_1 = L_1$, $A_2 = L^3 \setminus L^2 \simeq \mathbb{Q}_p(1)$, $A_{-1} = L_1 \simeq A_1^*(1)$, $A_{-2} = \mathbb{Q}_p \simeq A_2^*(1)$, and $A_0 = \mathbb{Q}_p(1)$. The Lie bracket is the original one on $A_1 \oplus A_2$ and trivial on $A_{-2} \oplus A_{-1}$. A_0 is central. The bracket between the plus part and the minus part is defined as follows:

$$A_{-2} \otimes A_1 \rightarrow A_{-1}$$

and

$$A_{-2} \otimes A_2 \rightarrow A_0$$

are scalar multiplication, and

$$A_{-1} \otimes A_1 = L_1 \otimes L_1 \rightarrow A_0 = \mathbb{Q}_p(1)$$

is induced by the Lie bracket followed by the Weil pairing. Finally

$$[A_{-1}, A_2] = 0.$$

For the purposes of this paper, it is useful to observe that the graded-commutative multiplication thus defined is in fact associative. The only non-trivial triple product occurs between elements $c \in A_{-2}$, $x, y \in A_1$, where the associativity immediately

follows from the definition. So we can simply regard the graded Lie algebra as a graded associative algebra, and hence, avoid the discussion of Massey products for Lie algebras in this paper.

Using this, we can also put the structure of an associative graded algebra on cochains with values in A . The cochain complex $C(G, A)$ of a group G with values in A is defined in the standard way as

$$C^i(G, A) := \{c : G^i \rightarrow A\},$$

where the maps are required to be continuous. It is graded by assigning degree $i + j$ to $C^i(G, A_j)$. We define the product of $a \in C^i(G, A)$ and $b \in C^j(G, A)$ by

$$a \cup b(g_1, g_2, \dots, g_{i+j}) = a(g_1, \dots, g_i)g_1g_2 \cdots g_ib(g_{i+1}, \dots, g_{i+j}).$$

We must check associativity for $a \in C^i(G, A), b \in C^j(G, A), c \in C^k(G, A)$:

$$\begin{aligned} [a \cup (b \cup c)](g_1, g_2, \dots, g_{i+j+k}) &= a(g_1, \dots, g_i)g_1 \cdots g_i[b \cup c(g_{i+1}, \dots, g_{i+j+k})] \\ &= a(g_1, \dots, g_i)g_1 \cdots g_i[b(g_{i+1}, \dots, g_{i+j})g_{i+1} \cdots g_{i+j}c(g_{i+j+1}, \dots, g_{i+j+k})] \\ &= a(g_1, \dots, g_i)g_1 \cdots g_ib(g_{i+1}, \dots, g_{i+j})g_1 \cdots g_ig_{i+1} \cdots g_{i+j}c(g_{i+j+1}, \dots, g_{i+j+k}) \\ &= (a \cup b)(g_1, \dots, g_{i+j})g_1 \cdots g_ig_{i+1} \cdots g_{i+j}c(g_{i+j+1}, \dots, g_{i+j+k}) \\ &= [(a \cup b) \cup c](g_1, \dots, g_{i+j+k}). \end{aligned}$$

The differential on $C(G, A)$ is defined in the standard way: for $a \in C^n(G, A)$,

$$\begin{aligned} da(g_1, \dots, g_{n+1}) &= g_1a(g_2, \dots, g_{n+1}) \\ &+ \sum_{i=1}^n (-1)^i a(g_1, \dots, g_ig_{i+1}, \dots, g_{n+1}) + (-1)^{n+1}a(g_1, \dots, g_n). \end{aligned}$$

One may find in [24], I.4, the proof that we get thereby a differential graded algebra, i.e., that

$$d(a \cup b) = (da) \cup b + (-1)^n a \cup (db),$$

if $a \in C^n(G, A)$. However, since that reference treats homogeneous cochains, we check this directly when $a, b \in C^1(G, A)$, which is the only case we will need:

$$\begin{aligned} d(a \cup b)(g_1, g_2, g_3) &= g_1((a \cup b)(g_2, g_3)) - (a \cup b)(g_1g_2, g_3) + (a \cup b)(g_1, g_2g_3) - (a \cup b)(g_1, g_2) \\ &= g_1a(g_2)g_1g_2b(g_3) - a(g_1g_2)g_1g_2b(g_3) + a(g_1)g_1b(g_2g_3) - a(g_1)g_1b(g_2). \end{aligned}$$

Meanwhile,

$$\begin{aligned} (da) \cup b(g_1, g_2, g_3) &= da(g_1, g_2)g_1g_2b(g_3) = (g_1a(g_2) - a(g_1g_2) + a(g_1))g_1g_2b(g_3) \\ &= g_1a(g_2)g_1g_2b(g_3) - a(g_1g_2)g_1g_2b(g_3) + a(g_1)g_1g_2b(g_3) \end{aligned}$$

and

$$\begin{aligned} -a \cup db(g_1, g_2, g_3) &= -a(g_1)g_1(g_2b(g_3) - b(g_2g_3) + b(g_2)) \\ &= -a(g_1)g_1g_2b(g_3) + a(g_1)g_1b(g_2g_3) - a(g_1)g_1b(g_2), \end{aligned}$$

from which one easily reads off the desired equality.

(i) *Global construction.*

First note that

Lemma 2.1. $H^2(G_T, L_1) = 0$.

Proof. If we consider the localization map

$$0 \rightarrow \text{III}_T^2(L_1) \rightarrow H^2(G_T, L_1) \rightarrow \bigoplus_{v \in T} H^2(G_v, L_1),$$

we see that

$$H^2(G_v, L_1) \simeq H^0(G_v, L_1)^* = 0$$

(note that $L_1^*(1) \simeq L_1$) for all v . This is a consequence of the fact that the weight of $L_1^{I_v}$ is -2 for $v \neq p$, and at p ,

$$H^0(G_p, L_1) = \text{Hom}_{G_p}(\mathbb{Q}_p, L_1) = \text{Hom}_{MF}(\mathbb{Q}_p, D^{cr}(L_1)) = 0,$$

because L_1 is a crystalline representation ([8], 5.2, theorem (i)).

On the other hand, the kernel $\text{III}_T^2(L_1)$ is dual to the kernel $\text{III}_T^1(L_1)$ of the H^1 -localization

$$0 \rightarrow \text{III}_T^1(L_1) \rightarrow H^1(G_T, L_1) \rightarrow \bigoplus_{v \in T} H^1(G_v, L_1),$$

which then must lie inside the \mathbb{Q}_p -Selmer group

$$H_{f,0}^1(G, L_1) := (\varprojlim_n \text{Sel}(E)[p^n]) \otimes \mathbb{Q}_p.$$

However, because of our assumption that the Tate-Shafarevich group of E is finite [22], we have

$$E(\mathbb{Q}) \otimes \mathbb{Q}_p \simeq H_{f,0}^1(G, L_1).$$

Hence, since $\text{rank} E(\mathbb{Q}) = 1$, there is an injection

$$H_{f,0}^1(G, L_1) \hookrightarrow H^1(G_p, L_1),$$

from which we deduce that $\text{III}_T^1(L_1) = 0$. Therefore, $\text{III}_T^2(L_1) = 0$ and $H^2(G_T, L_1) = 0$. □

Note that the vanishing of H^2 requires the assumptions on the rank and the finiteness of III . We will now use this important fact to

(1) Construct refined Massey products for global cohomology; the key point is that for any global class $a \in H^1(G_T, L_1)$, the cup product with a class in $H^1(G_T, \mathbb{Q}_p)$ is necessarily zero, allowing us to begin the construction of Massey products.

(2) Use the rank one assumption to represent local cohomology $H^1(G_p, L_1)$ uniquely by a global class. This allows the construction of Massey products for local cohomology.

Let $\chi : G_T \rightarrow \mathbb{Z}_p^*$ be the p -adic cyclotomic character and $c := \log \chi : G_T \rightarrow \mathbb{Q}_p$, regarded as an element of $H^1(G_T, \mathbb{Q}_p)$. For any point $x \in \mathcal{X}(\mathbb{Z}_S)$, let $a(x)$ be a cocycle representing the class of $\pi_1^{u, \mathbb{Q}_p}(\bar{X}; b, x)$ in $H^1(G_T, U_2)$. Write

$$a(x) = a_1(x) + a_2(x)$$

as indicated in the previous section. Then $c \cup a_1(x)$ represents a cohomology class in $H^2(G_T, L_1)$. Since this group vanishes, we can find a cochain $b_x : G_T \rightarrow L_1$ such that

$$db_x = c \cup a_1(x).$$

Define a two-cochain

$$\phi_x : G_T \times G_T \rightarrow Z$$

by putting

$$\phi_x = b_x \cup a_1(x) - 2c \cup a_2(x).$$

Lemma 2.2. ϕ_x is a cocycle.

Proof. Since $a(x)_1$ and c are cocycles, we have

$$d\phi_x = db_x \cup a(x)_1 + 2c \cup da(x)_2 = c \cup a(x)_1 \cup a(x)_1 - c \cup a(x)_1 \cup a(x)_1 = 0.$$

□

Our construction of ϕ_x depends on the auxiliary cochain b_x , and hence, gives a class

$$[\phi_x] \in H^2(G_T, Z)/[H^1(G_T, L_1) \cup a_1(x)].$$

Lemma 2.3. The class $[\phi_x]$ is independent of the choice of cocycle $a(x)$.

Proof. Obviously, the subspace $H^1(G_T, L_1) \cup a_1(x)$ depends only on the class of $a_1(x)$, and hence, on the class of $a(x)$. Now we examine the action of U_2 . To reduce clutter, we will temporarily suppress x from the notation for the cochains. Write $u = u_1 + u_2$. Then

$$\begin{aligned} ua(g)g(u^{-1}) &= (u_1 + u_2) * (a_1(g) + a_2(g)) * (-gu_1 - gu_2) \\ &= (u_1 + a_1(g) + u_2 + a_2(g) + (1/2)[u_1, a_1(g)]) * (-gu_1 - gu_2) \\ &= a_1(g) + u_1 - gu_1 + a_2(g) + u_2 - gu_2 + (1/2)[u_1, a_1(g)] \\ &\quad - (1/2)[a_1(g), gu_1] - (1/2)[u_1, gu_1]. \end{aligned}$$

The L_1 -component of this expression is $a_1 - du_1$, where we view the element $u_1 \in L_1$ as a zero-cochain. Thus, the previous choice of b_x can be changed to $b_x + c \cup u_1$, since

$$d(c \cup u_1) = dc \cup u_1 - c \cup du_1 = -cdu_1.$$

The resulting two-cocycle changes to

$$\begin{aligned} (b_x + c \cup u_1) \cup (a_1 - du_1) - 2c \cup a_2 + 2c \cup du_2 - c \cup r + c \cup s + c \cup t \\ = \phi_x + [c \cup u_1 \cup a_1 - b_x \cup du_1 - c \cup u_1 \cup du_1 + 2c \cup du_2 - c \cup r + c \cup s + c \cup t], \end{aligned}$$

where r, s, t are the functions $G_T \rightarrow Z$ defined by

$$r(g) = [u_1, a_1(g)], \quad s(g) = [a_1(g), gu_1], \quad t(g) = [u_1, gu_1].$$

Within the discrepancy, the term $2c \cup du_2 = -2d(c \cup u)$ is clearly a coboundary. Also, we see that $t = u_1 \cup du_1$, ridding us of two terms. We have

$$c \cup u_1 \cup a_1(g, h) = [c \cup u_1(g), ga_1(h)] = [c(g)gu_1, ga_1(h)],$$

while

$$c \cup r(g, h) = c(g)gr(h) = c(g)g[u_1, a_1(h)] = c(g)[gu_1, ga_1(h)],$$

causing two more terms to cancel each other. Finally, it remains to analyze the difference $c \cup s - b_x \cup du_1$. But

$$d(b_x \cup u_1) = db_x \cup u_1 - b_x \cup du_1,$$

so that up to a coboundary, we can replace $b_x \cup du_1$ by $db_x \cup u_1 = c \cup a_1 \cup u_1$. We can then compute the value

$$c \cup a_1 \cup u_1(g, h) = [c \cup a_1(g, h), gh u_1] = [c(g)ga_1(h), gh u_1],$$

which is verified to be equal to

$$c \cup s(g, h) = c(g)gs(h) = c(g)g[a_1(h), hu_1] = c(g)[ga_1(h), gh u_1].$$

Therefore, the difference $c \cup s - b_x \cup du_1$ is a coboundary. □

Given a global cohomology class or cochain s , we will denote by s^l its localization at the prime l , that is, its restriction to G_l .

Lemma 2.4. *The subspace $H^1(G_T, L_1) \cup a_1(x)$ of $H^2(G_T, Z)$ is zero.*

Proof. Recall that $Z \simeq \mathbb{Q}_p(1)$. Because $a_1(x)$ is the class of a point and we are taking \mathbb{Q}_p -coefficients, $a_1(x)^l = 0$ for all $l \neq p$. Thus, for any $r \in H^1(G_T, L_1)$, we have $(r \cup a_1(x))^l = 0$ for all $l \neq p$. This is of course also true for the Archimedean component since p is odd. Thus, the only possible component of $r \cup a_1(x)$ that survives is at p , which then must be zero since

$$\sum_v (r \cup a_1(x))_v = 0,$$

from the exact sequence

$$0 \rightarrow H^2(G_T, \mathbb{Q}_p(1)) \hookrightarrow \bigoplus_v H^2(G_v, \mathbb{Q}_p(1)) \rightarrow \mathbb{Q}_p \rightarrow 0.$$

The injectivity on the left of the sequence also shows that $r \cup a_1(x) = 0$. □

The reciprocity sequence for H^2 in the proof will also be the main component in the proof of Theorem 0.1.

By the preceding lemma, we have a well-defined class

$$[\phi_x] \in H^2(G_T, Z).$$

Lemma 2.5. *Let $l \neq p$. Then*

$$[\phi_x]^l \in H^2(G_l, Z)$$

can be computed locally in the following sense: Choose any local representative $t(x)$ for the class $[a(x)]^l$, and let $s : G_l \rightarrow L_1$ be any local cochain such that $ds = c^l \cup t_1(x)$. Then

$$[\phi_x]^l = [s \cup t_1(x) - 2c^l \cup t_2(x)].$$

Proof. The class modulo

$$H^1(G_l, L_1) \cup t_1(x)$$

will clearly be independent of the choice of t and s . Since $[t_1(x)] = [a_1^l(x)]$, we have

$$H^1(G_l, L_1) \cup t_1(x) = H^1(G_l, L_1) \cup a_1(x).$$

But, as we pointed out above, $a_1^l(x)$ is the trivial class. Therefore, the class in $H^2(G_l, Z)$ is independent of the choices. In particular, local choices s and t will give the same class as the localization of the global choices a and b . □

(ii) *Local construction.*

We will now make use of a point $y \in E(\mathbb{Q})$ of infinite order. Since

$$E(\mathbb{Q}_p) \otimes \mathbb{Q}_p \simeq H_f^1(G_p, U_1)$$

[3], for any class $s \in H_f^1(G_p, U_2)$, its component $s_1 \in H_f^1(G_p, U_1)$ is a \mathbb{Q}_p multiple of $a_1^p(y)$:

$$s_1 = \lambda(s) a_1^p(y),$$

for some $\lambda(s) \in \mathbb{Q}_p$. In particular, $s_1 = x_1^p$ for some cocycle $x_1 : G_T \rightarrow L_1$ such that $[x_1]^l = 0$ for all $l \neq p$. By the theorem of Kolyvagin cited earlier, the equation

$$db = c \cup (\lambda(s)x_1)$$

has a solution $b^{glob} : G_T \rightarrow L_1$. Thus, we get a class

$$\psi^p(s) := [b^{glob,p} \cup s_1 - 2c^p \cup s_2] \in H^2(G_p, Z)/[\text{loc}_p(H^1(G_T, L_1)) \cup s_1]$$

since two choices of b^{glob} will differ by an element of $H^1(G_T, L_1)$. But

$$\text{loc}_p(H^1(G_T, L_1)) \cup s_1 = \text{loc}_p(H^1(G_T, L_1)) \cup a_1^p(y) = \text{loc}_p((H^1(G_T, L_1)) \cup a_1(y)) = 0$$

by Lemma 2.3. Therefore, we have a well-defined class

$$\psi^p(s) \in H^2(G_p, Z).$$

The following lemma is straightforward from the definitions:

Lemma 2.6. *Let $x \in \mathcal{X}(\mathbb{Z}_S)$. Then*

$$\psi^p(a^p(x)) = [\phi_x]^p.$$

Now we can give the

Proof of Theorem 0.1. If $x \in \mathcal{X}(\mathbb{Z})$, then we know that $[a^l(x)] = 0$ for all $l \neq p$. By Lemma 2.4, this implies that $[\phi_x]^l = 0$ for all $l \neq p$, and hence,

$$\psi^p(a^p(x)) = [\phi_x]^p = 0.$$

□

3. PRELIMINARY FORMULAS

Any class $s \in H_f^1(G_p, U_2)$ lies over the same point in $H_f^1(G_p, U_1)$ as $\lambda(s)a^p(y)$ for some number $\lambda(s)$ depending on the class.² By the exact sequence ([20], p.232)

$$0 \rightarrow H_f^1(G_p, Z) \rightarrow H_f^1(G_p, U_2) \rightarrow H_f^1(G, U_1),$$

the two classes then differ by the action of an element of $H_f^1(G_p, Z)$ which we denote by

$$\lambda(s)a^p(y) - s \in H_f^1(G_p, Z).$$

Using the point y , we get the following alternative description of the function ψ :

Lemma 3.1.

$$\psi^p(s) = \lambda(s)^2 \psi^p(y) + 2(c^p \cup (\lambda(s)a^p(y) - s)).$$

Proof. Let $b : G_T \rightarrow \Lambda_1$ be a solution of

$$db = c \cup a_1(y).$$

Then

$$d(\lambda(s)b) = c \cup (\lambda(s)a_1(y))$$

and

$$(\lambda(s)b)^p \cup s_1 = (\lambda(s)b)^p \cup (\lambda(s)a_1^p(y)) = \lambda(s)^2 b^p \cup a_1^p(y).$$

Therefore,

$$\begin{aligned} \psi^p(s) &= \lambda(s)^2 b^p \cup a_1^p(y) - 2c^p \cup s_2 \\ &= \lambda(s)^2 (b^p \cup a_1^p(y) - 2c^p \cup a_2^p(y)) + 2(\lambda(s)^2 c^p \cup a_2^p(y) - c^p \cup s_2) \\ &= \lambda(s)^2 \psi^p(y) + 2(c^p \cup (\lambda(s)a^p(y) - s)). \end{aligned}$$

□

²Take care that this multiplication now refers to the \mathbb{Q}_p -action discussed in the previous section.

Now fix the isomorphism $Z \simeq \mathbb{Q}_p(1)$ induced by the Weil pairing $\langle \cdot, \cdot \rangle$, that is, that takes $[x, y]$ to $\langle x, y \rangle$, which then induces an isomorphism

$$T : H^2(G_p, Z) \simeq \mathbb{Q}_p$$

and gives us a \mathbb{Q}_p -valued function

$$T \circ \psi^p : H_f^1(G_p, U_2) \rightarrow \mathbb{Q}_p.$$

We will sometimes suppress T from the notation and simply regard ψ^p as taking values in \mathbb{Q}_p . From the definition, we see that for any $\lambda \in \mathbb{Q}_p$,

$$\psi_y^p(\lambda a^p(y)) = \lambda^2 T(\phi_y^p),$$

while for $r \in H_f^1(G_p, Z)$, we have

$$\psi_y^p(r) = -T(c^p \cup r).$$

Thus, when we take $z \in \mathbb{Z}_p^*$ with a cohomology class

$$k(z) \in H_f^1(G_p, \mathbb{Q}_p(1))$$

coming from Kummer theory, which we identify with a class in $H_f^1(G_p, Z)$, then by [24], Proposition (7.2.12) and the diagram before Corollary (7.2.3), we get

$$\psi_y^p(z) = \pm \log \chi(Rec_p(z)),$$

where Rec_p is the local reciprocity map. Since $\chi(Rec_p(z)) = z$, we get

$$\psi_y^p(k(z)) = \pm \log z \in \mathbb{Q}_p.$$

In particular, the map is not identically zero. In fact, it is far from trivial on any fiber of

$$H_f^1(G_p, U_2) \rightarrow H_f^1(G_p, U_1).$$

Although we do not need this fact, with respect to the structure of $H_f^1(G_p, U_2)$ as an algebraic variety, ψ^p is in fact a non-zero algebraic function, as we see in a straightforward way by defining it for points in arbitrary \mathbb{Q}_p -algebras (as in [16]). Since there is a Coleman map

$$j_{2,loc}^{et} : \mathcal{X}(\mathbb{Z}_p) \rightarrow H_f^1(G_p, U_2)$$

with Zariski dense image for each residue disk [17], Theorem 0.1 yields the finiteness of $\mathcal{X}(\mathbb{Z})$. As mentioned in the introduction, the obvious task of importance is to compute the function

$$\psi^p \circ j_{2,loc}^{et}$$

on $\mathcal{X}(\mathbb{Z}_p)$, whose zero set is guaranteed to capture the global integral points.

There is a commutative diagram ([17], p. 120)

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}_p) & \xrightarrow{j_{2,loc}^{et}} & H_f^1(G, U_2) \\ & \searrow j_2^{dr/cr} & \downarrow \\ & & U_2^{DR}/F^0 \end{array}$$

bringing the de Rham fundamental group $U^{DR} = \pi_1^{DR}(X_{\mathbb{Q}_p}, b)$ and its quotient $U_2^{DR} = U^{DR}/U^3$ into our consideration. The map

$$H_f^1(G, U_2) \rightarrow U_2^{DR}/F^0$$

is a non-abelian analogue of the Bloch-Kato log map. There is actually a larger commutative diagram

$$\begin{array}{ccc} \mathcal{X}(\mathbb{Z}_p) & \xrightarrow{j_{loc}^{et}} & H_f^1(G, U) \\ & \searrow j^{dr/cr} & \downarrow \\ & & U^{DR}/F^0 \end{array}$$

out of which the level-two version is obtained by composing with the projection

$$U \rightarrow U_2.$$

The map j_{loc}^{et} is just a local version of the map recalled in the previous section, while $j^{dr/cr}$ associates to each point $x \in \mathcal{X}(\mathbb{Z}_p)$, the U^{DR} -torsor $\pi_1^{DR}(X_{\mathbb{Q}_p}; b, x)$, and hence, corresponds to a point $j^{dr/cr}(x) \in U^{DR}/F^0$ ([17], p. 112). The point is described explicitly as follows (loc. cit.). One chooses an element $p^H \in F^0 \pi_1^{DR}(X_{\mathbb{Q}_p}; b, x)$. On the other hand, there is a unique Frobenius invariant element $p^{cr} \in \pi_1^{DR}(X_{\mathbb{Q}_p}; b, x)$. Then $j^{dr/cr}(x)$ is the coset of the element u such that $p^{cr}u = p^H$.

In [17], section 1, Lemma 2 and Lemma 3, we gave a description of a universal pro-unipotent bundle with connection on $X_{\mathbb{Q}_p}$. Let α be an invariant differential 1-form on E and let β be a differential of the second kind with a pole only at e such that $[-1]^*(\alpha) = -\alpha$ and $[-1]^*(\beta) = -\beta$. (Of course the first condition is automatic.) Let

$$R := \mathbb{Q}_p \langle\langle A, B \rangle\rangle = \varprojlim \mathbb{Q}_p \langle A, B \rangle / I^n,$$

where $\mathbb{Q}_p \langle A, B \rangle$ is the free non-commutative \mathbb{Q}_p -algebra on the letters A, B , and $I \subset \mathbb{Q}_p \langle A, B \rangle$ is the augmentation ideal. Thus, $\mathbb{Q}_p \langle A, B \rangle$ is spanned by words w in A and B , while the elements of R are infinite formal linear combinations

$$\sum c_w w$$

in such words with coefficients $c_w \in \mathbb{Q}_p$. Using this we can construct the free $\mathcal{O}_{X_{\mathbb{Q}_p}}$ -module

$$\mathcal{R} := \mathcal{O}_{X_{\mathbb{Q}_p}} \otimes R$$

together with the connection

$$\nabla f = df - (A\alpha + B\beta)f,$$

for an element $f \in \mathcal{R}$. If we choose the element $1 \in \mathcal{R}_b = R$ as the initial condition, then the element $p^{cr}(1) \in \mathcal{R}_x$ corresponding to it is given by

$$G(x) = \sum_w \int_b^x a_w w,$$

where a_w is the symbol

$$\alpha^{n_1} \beta^{m_1} \dots \alpha^{n_k} \beta^{m_k}$$

if w is the word

$$A^{n_1} B^{m_1} \dots A^{n_k} B^{m_k},$$

and the integral symbol corresponds to iterated Coleman integration ([10], [2, Prop. 4.5]). This is normalized by the convention

$$d\left(\int \alpha a_w\right) = \left(\int a_w\right)\alpha, \quad d\left(\int \beta a_w\right) = \left(\int a_w\right)\beta.$$

To recall the detailed description, we need to choose a local coordinate z at $e \in E$ such that $d/dz = b$. Furthermore, fix Iwasawa's branch of the p -adic log. This determines a ring $A^{col}(]e])(\log z)$ of logarithmic Coleman functions in the residue disk $]e[$ of the origin of E . The connection (\mathcal{R}, ∇) has a canonical extension to a logarithmic connection $(\overline{\mathcal{R}}, \overline{\nabla})$ on $E_{\mathbb{Q}_p}$ [6] and there is a unique element ([2], Prop. 4.5)

$$G^b \in A^{col}(]e])(\log z) \otimes R$$

characterized by the property $\nabla G = 0$, together with the initial condition specifying that when we write

$$G^b = G_0^b + G_1^b \log z + G_2^b (\log z)^2 + \dots,$$

we have $G_0^b(0) = 1$. Then analytic continuation along the Frobenius map produces an element

$$G^x \in A^{col}(]x]) \otimes R$$

in the residue disk $]x[$ compatible with G^b , and

$$G(x) := G^x(x).$$

The individual definite iterated integral $\int_b^x a_w$ is then defined to be the coefficient of $[w]$ in $G(x)$.

There is a comultiplication

$$\Delta : R \rightarrow R \otimes R$$

determined by

$$\Delta(A) = A \otimes 1 + 1 \otimes A, \quad \Delta(B) = B \otimes 1 + 1 \otimes B,$$

with respect to which $G(x)$ is group-like, i.e., satisfies

$$\Delta(G(x)) = G(x) \otimes G(x).$$

Thus, $G(x)$ corresponds to a \mathbb{Q}_p point of $\pi_1^{DR}(X_{\mathbb{Q}_p}; b, x) = \text{Spec}(R^*)$, where

$$R^* := \varinjlim \text{Hom}(R/I^n, \mathbb{Q}_p).$$

The structure of R^* can also be elucidated as the free \mathbb{Q}_p -vector space generated by the functions f_w such that $f_w(w') = \delta_{ww'}$.

The de Rham fundamental group as well as the associated algebras R and R^* have models over \mathbb{Q} ,

$$\begin{aligned} &\pi_1^{DR}(X; b, x), \\ R_{\mathbb{Q}} &= \varprojlim_n \mathbb{Q}\langle A, B \rangle / I^n, \end{aligned}$$

$$R_{\mathbb{Q}}^* = \varinjlim \text{Hom}(\mathbb{Q}\langle A, B \rangle / I^n, \mathbb{Q}),$$

and of course the basis functions are defined over \mathbb{Q} . When these objects are base-changed to \mathbb{C} , we have the natural isomorphism

$$\pi_1^{DR}(X(\mathbb{C}); b, x) \simeq \pi_1^{DR}(X; b, x) \otimes_{\mathbb{Q}} \mathbb{C},$$

and $R_{\mathbb{C}}^* = R_{\mathbb{Q}}^* \otimes \mathbb{C}$ is identified with the coordinate ring of $\pi_1^{DR}(X(\mathbb{C}); b, x)$, where the isomorphism is induced by the map

$$\begin{aligned} I : \pi_1^{DR}(X(\mathbb{C}); b, x) &\rightarrow R_{\mathbb{C}}; \\ \gamma &\mapsto \int_{\gamma} a_w[w]. \end{aligned}$$

As in the non-Archimedean case, the integrals can simply be defined to be the coordinates of parallel transport along γ . If γ starts at the tangential base-point b , one chooses a branch of the logarithm so that $\log z$ is defined on an arc containing the portion of γ near e , and one finds the unique

$$G^b = G_0^b + G_1^b \log z + G_2^b (\log z)^2 + \dots,$$

such that $G_0^b(0) = 1$ and $\nabla G^b = 0$. One defines thus the parallel transport from b to $\gamma(\epsilon)$ for some small $\epsilon > 0$ to be the map

$$v \in R \mapsto G^b(\gamma(\epsilon))v.$$

(See [13], corollary 5 and section 6.3. There, the description is given for $\mathbf{P}^1 \setminus \{0, 1, \infty\}$, but the discussion of tangential base-points is purely local and can be used for any Riemann surface.) The parallel transport along γ is then defined to be the parallel transport from b to $\gamma(\epsilon)$ composed with the standard parallel transport from $\gamma(\epsilon)$ to $\gamma(1)$.

As described in [26] and [28], there is a Hodge filtration on $R_{\mathbb{Q}}$, which then induces one on R , and hence, on U^{DR} .

Lemma 3.2. $F^0 R_{\mathbb{Q}}/I^3$ is the \mathbb{Q} -vector space generated by B and B^2 .

Proof. It suffices to check this assertion over \mathbb{C} . By definition, $F^0 R_{\mathbb{Q}}/I^3$ is the annihilator of $F^1 \text{Hom}(R_{\mathbb{C}}/I^3, \mathbb{C})$. We need to prove that the latter is the space $(F')^1$ spanned by the f_w as w runs through the words containing at least one A . Now, by [11], section 1.2 and theorem 2.2.1, we have

$$R_{\mathbb{C}} \simeq H^0(B(\mathcal{A})),$$

where $B(\mathcal{A})$ is the reduced bar complex on the algebra \mathcal{A} of C^∞ differential forms on E with log poles at e . According to [11], section 4, and [12], Prop. 4.1., $F^1 H^0(B(\mathcal{A}))$ is spanned by elements of the form

$$\xi + \sum a_{jk} \phi_j \otimes \psi_k + c,$$

where c is a constant; ϕ_j as well as ξ are in $\mathcal{A}^{1,0}(\log(e))$; each of the ϕ_j and ψ_k are closed; and

$$d\xi + \sum a_{jk} \phi_j \wedge \psi_k = 0.$$

Since the isomorphism

$$H^0(B(\mathcal{A})) \simeq \varinjlim_n \text{Hom}(R_{\mathbb{C}}/I^n, \mathbb{C})$$

is induced by regarding both as functions on the space of paths from b to x via integration, it is clear that $(F')^1 \text{Hom}(R_{\mathbb{C}}/I^3, \mathbb{C})$ maps to $F^1 H^0(B(\mathcal{A}))$. Furthermore, since the Hodge structure on

$$\pi_1^{DR}(X(\mathbb{C}); b, x)$$

is a limit Hodge structure of that on

$$\pi_1^{DR}(X(\mathbb{C}); y, x)$$

(see [14], section 6) as y varies over points in $X(\mathbb{C})$, it suffices to calculate the Hodge filtration on usual (non-tangential) base-points. Consider an integral

$$\int_{\gamma} \xi + \sum a_{jk} \int_{\gamma} \phi_j \psi_k$$

for a path γ lying in $X(\mathbb{C})$ with the ϕ_j , ψ_k and ξ as above. First note that since the ϕ_j are closed and of type $(1, 0)$, they must satisfy

$$\bar{\partial}\phi_j = 0,$$

i.e., be holomorphic. Then, since they have at most a log pole at e , they must be holomorphic on $E(\mathbb{C})$, that is, be a multiple of α . Similarly if we write

$$\psi_k = \psi_k^{(1,0)} + \psi_k^{(0,1)}$$

in terms of its dz and $d\bar{z}$ components, we see that $\psi_k^{(1,0)}$ must be holomorphic, i.e., a multiple of α again. So $\int_\gamma \phi_j \psi_k^{(1,0)}$ belongs to the image of $(F')^1 \text{Hom}(R_{\mathbb{C}}/I^3, \mathbb{C})$.

Furthermore, since $\phi_j \wedge \psi_k^{(1,0)} = 0$, we still have

$$d\xi + \sum a_{jk} \phi_j \wedge \psi_k^{(0,1)} = 0.$$

That is to say, we may assume that $\psi_k = \psi_k^{(0,1)}$.

We note then that on $X(\mathbb{C})$, each ψ_k can be written

$$\psi_k = \mu_k + dt_k$$

for μ_k a linear combination of α and β , and t_k a C^∞ function. In a neighborhood W of e , we have

$$dt_k = \psi_k - \mu_k = g_k d\bar{z} - h_k dz/z^2,$$

where ψ_k is C^∞ and h_k is homomorphic. In particular, t_k must be of the form

$$t_k = l_k/z$$

with l_k a C^∞ function on W . We can thus write the original integral as

$$\begin{aligned} \int_\gamma \xi + \sum a_{jk} \int_\gamma \phi_j \psi_k &= \int_\gamma \xi + \sum a_{jk} \int_\gamma \phi_j (\mu_k + dt_k) \\ &= \int_\gamma (\xi + \sum t_k \phi_j) + \sum a_{jk} \int_\gamma \phi_j \mu_k. \end{aligned}$$

We clearly still must have

$$d(\xi + \sum t_k \phi_j) + \sum a_{jk} \phi_j \wedge \mu_k = 0.$$

But now, each $\phi_j \wedge \mu_k = 0$, and hence,

$$d(\xi + \sum t_k \phi_j) = 0.$$

Since $\xi + \sum t_k \phi_j$ is of type $(1, 0)$ with at most a log pole at e , it must then be holomorphic on E . That is, it is a multiple of α . So we see that $(F')^1 \text{Hom}(R_{\mathbb{C}}/I^3, \mathbb{C})$ surjects onto $F^1 H^0(B(\mathcal{A}))$, proving the desired compatibility of filtrations. \square

With respect to the basis $\{A, A^2, AB, BA\}$ of U_2^{DR}/F^0 , we can express $j_2^{dr/cr}$ as

$$j_2^{dr/cr}(x) = 1 + \int_b^x \alpha A + \int_b^x \alpha^2 A^2 + \int_b^x \alpha \beta AB + \int_b^x \beta \alpha BA.$$

This map as well is conveniently expressed in terms of the logarithm $\log U^{DR} \rightarrow L^{DR}$ as

$$\log j^{dr/cr}(x) = \int_b^x \alpha A + \left(\int_b^x \alpha \beta - (1/2) \left(\int_b^x \alpha \right) \left(\int_b^x \beta \right) \right) [A, B].$$

Introducing the notation

$$\log_\alpha(x) = \int_b^x \alpha, \quad \log_\beta(x) = \int_b^x \beta, \quad D_2(x) = \int_b^x \alpha\beta,$$

we can also write this as

$$\log j^{DR}(x) = \log_\alpha(x)A + (D_2(x) - (1/2)\log_\alpha(x)\log_\beta(x))[A, B].$$

Regarding the \mathbb{Q}_p -action, our choice of α and β implies that the automorphism of L_2^{DR} induced by the involution of section 1 is simply

$$A \mapsto -A, \quad B \mapsto -B,$$

so that A and B are basis elements compatible with the grading on L_2 . In particular, the \mathbb{Q}_p -action can be described as

$$m(\lambda)A = \lambda A, \quad m(\lambda)B = \lambda B, \quad m(\lambda)[A, B] = \lambda^2[A, B].$$

Given the class $a(x) \in H_f^1(G_p, U_2)$ of a point $x \in \mathcal{X}(\mathbb{Z}_p)$, the number λ such that $a_1(x) = \lambda a_1^p(y)$ can be written as

$$\lambda = \log_\alpha(x) / \log_\alpha(y),$$

since the logarithm is a group homomorphism. On the other hand, we have

$$\begin{aligned} \log j_2^{dr/cr}(x) &= \log_\alpha(x)A + (D_2(x) - (1/2)\log_\alpha(x)\log_\beta(x))[A, B], \\ \log \lambda j_2^{dr/cr}(y) &= \lambda \log_\alpha(y)A + \lambda^2(D_2(y) - (1/2)\log_\alpha(y)\log_\beta(y))[A, B] \\ &= \log_\alpha(x)A + \lambda^2(D_2(y) - (1/2)\log_\alpha(y)\log_\beta(y))[A, B]. \end{aligned}$$

So the element in Z^{DR} representing the difference is

$$\begin{aligned} &[(\log_\alpha(x) / \log_\alpha(y))^2(D_2(y) - (1/2)\log_\alpha(y)\log_\beta(y)) \\ &\quad - (D_2(x) - (1/2)\log_\alpha(x)\log_\beta(x))][A, B]. \end{aligned}$$

Using the (Bloch-Kato) exponential notation for the isomorphism

$$\text{Exp} : Z^{DR} \simeq H_f^1(G_p, Z),$$

we see by Lemma 2.7 that a formula for the function $\psi^p \circ j_{loc}^{et}$ is given by

$$\begin{aligned} \psi^p \circ j_{loc}^{et}(x) &= (\log_\alpha(x) / \log_\alpha(y))^2 T(\psi^p(y)) \\ &\quad + 2[(\log_\alpha(x) / \log_\alpha(y))^2(D_2(y) - (1/2)\log_\alpha(y)\log_\beta(y)) \\ &\quad - (D_2(x) - (1/2)\log_\alpha(x)\log_\beta(x))]T(c \cup \text{Exp}([A, B])). \end{aligned}$$

Therefore, obtaining a ‘concrete’ expression for this function reduces to the computation of a single

$$T(\psi^p(y))$$

and

$$T(c \cup \text{Exp}([A, B])).$$

The latter is found in a rather straightforward manner. The key point is that the map

$$H_1^{et}(\overline{\mathbb{G}}_{m, \mathbb{Q}_p}, \mathbb{Q}_p) \simeq Z \hookrightarrow U_2^{et}$$

is induced by the restriction functor

$$r : \text{Cov}(\bar{X}) \rightarrow \text{Cov}(\bar{T}^0)$$

mentioned in section 1. Similarly, the map

$$H_1^{DR}(\mathbb{G}_{m, \mathbb{Q}_p}) \simeq Z^{DR} \hookrightarrow U_2^{DR}$$

is induced by a restriction functor

$$r^{DR} : \text{Un}(X) \rightarrow \text{Un}(T^0),$$

on categories of unipotent bundles with connection. The construction of r^{DR} takes a bundle (V, ∇) and associates to it first the canonical extension

$$(\bar{V}, \bar{\nabla}),$$

which is a log connection

$$\bar{\nabla} : \bar{V} \rightarrow \Omega_E(\log e) \otimes \bar{V}$$

on E , and then its residue

$$\text{Res}(\nabla) : V_e \rightarrow V_e,$$

which is an endomorphism of the fiber V_e . The value $r^{DR}(V, \nabla)$ is then just the trivial bundle V_e on T^0 equipped with the connection

$$d - Nd/dt$$

for any choice of linear coordinate on T such that $t(0) = 0$. Let us compute r^{DR} for \mathcal{R}/I^3 . In an open neighborhood of e , we can solve the equation

$$dv = \beta$$

and make the gauge transformation induced by $1 - vB$. Then the connection form with respect to this gauge becomes

$$\begin{aligned} & (1 - vB)(\alpha A + \beta B)(1 + vB + v^2 B^2) + (-dvB)(1 + vB + vB^2) \\ &= (\alpha A + \beta B - v\alpha BA - v\beta B^2)(1 + vB + v^2 B^2) - dvB - vdvB^2 \\ &= \alpha A + \beta B - v\alpha BA - v\beta B^2 + v\alpha AB + v\beta B^2 - dvB - vdvB^2 \\ &= \alpha A + v\alpha[A, B] - vdvB^2 \end{aligned}$$

modulo I^3 . From this, we see that the residue is

$$\text{Res}(v\alpha)[A, B]$$

with $\text{Res}(v\alpha) \in \mathbb{Z}_p^*$. This residue can be easily identified with the Serre duality pairing $\langle \alpha, \beta \rangle$. In any case, the connection $r^{DR}(\mathcal{R}/I^3)$ is the bundle $\mathcal{O}_{T^0} \otimes R/I^3$ with connection

$$d - \text{Res}(v\alpha)[A, B]d/dt.$$

The universal unipotent connection on T^0 is

$$\mathcal{O}_{T^0} \otimes \mathbb{Q}_p[[C]]$$

with connection form

$$d - Cd/dt.$$

So the map

$$C \mapsto \text{Res}(v\alpha)[A, B]$$

realizes the map

$$\pi^{DR}(T^0, b) \rightarrow U_2^{DR}.$$

In particular, this map fits into the commutative diagram:

$$\begin{CD} \pi^{DR}(T_{\mathbb{Q}_p}^0, b) @>>> U_2^{DR}/F^0 \\ @V \text{Exp}^{-1} VV @VV \uparrow V \\ H_f^1(G_p, \pi_1^{\mathbb{Q}_p, et}(\bar{T}^0, b)) @>>> H_f^1(G_p, U_2). \end{CD}$$

We analyze the left vertical arrow. Fix the linear coordinate $t : T \rightarrow \mathbb{A}^1$ such that $t(0) = 0$ and $t(b) = 1$. This induces isomorphisms

$$\begin{aligned} \pi^{\mathbb{Q}_p, et}(\bar{T}^0, b) &\simeq \mathbb{Q}_p(1), \\ \pi^{DR}(T_{\mathbb{Q}_p}^0, b) &\simeq H_1^{DR}(\mathbb{G}_{m, \mathbb{Q}_p}). \end{aligned}$$

The isomorphism

$$H_f^1(G_p, \mathbb{Q}_p(1)) \simeq H_1^{DR}(\mathbb{G}_{m, \mathbb{Q}_p})$$

takes the class $k(x)$ of $x \in \mathbb{Z}_p^*$ to the class of

$$\int_1^x dt/tC = \log(x)C.$$

On the other hand,

$$T(c \cup k(x)) = c(\text{Rec}_p(x)) = \log \chi(x) = \log x.$$

Thus, we see that $T(c \cup \text{Exp}(C)) = 1$. Therefore, from the previous commutative diagram, we deduce:

Proposition 3.3.

$$T(c \cup \text{Exp}[A, B]) = \text{Res}(v\alpha)^{-1}.$$

The computation of $T(\psi^p(y))$ in general appears to be somewhat difficult. Perhaps some progress is possible through the theory of p -adic uniformization when p is a split-semi-stable prime, for which a generalization of the local Selmer theory will be necessary. In that case, it will be natural to take y to be the trace of a Heegner point coming from a Shimura curve uniformization, and some relationship between the various quantities and L -functions should emerge, such as

$$(\log_\alpha y)^2 = (1/2)(d^2/dk^2)L_p(E, k, k/2)_{k=2},$$

which appears in [1].

One case that is tractable right now is when we already have an integral point y of infinite order in hand, because then by Theorem 0.1, $T(\psi^p(y)) = 0$. The formula for $\psi^p \circ J_{loc}^{et}$ then immediately gives Corollary 0.2 as a consequence.

ACKNOWLEDGEMENTS

It is a great pleasure to express my profound gratitude to John Coates for innumerable mathematical discussions as well as for a continuum of moral support surrounding this research. Considerable benefit was derived also from communication with Henri Darmon, Christopher Deninger, and Gerd Faltings. Richard Hain continues to provide valuable advice on Hodge theory, and conversations with Bertand Toen were helpful during the completion of the manuscript.

This paper was largely written while the author was a guest of the SFB 478 at the University of Münster. The excellent academic and cultural environment of the city was an indispensable aid to the process of writing.

Finally, I am very grateful to an anonymous referee for a thorough reading that led to many valuable suggestions.

REFERENCES

- [1] Bertolini, Massimo; Darmon, Henri, Hida families and rational points on elliptic curves. *Invent. Math.* 168 (2007), no. 2, 371–431. MR2289868 (2008c:11076)
- [2] Besser, Amnon; Furusho, Hidekazu, The double shuffle relations for p -adic multiple zeta values. *Primes and knots*, 9–29, *Contemp. Math.*, 416, Amer. Math. Soc., Providence, RI, 2006. MR2276133 (2007i:11090)
- [3] Bloch, Spencer; Kato, Kazuya, L -functions and Tamagawa numbers of motives. *The Grothendieck Festschrift*, Vol. I, 333–400, *Progr. Math.*, 86, Birkhäuser Boston, Boston, MA, 1990. MR1086888 (92g:11063)
- [4] Coates, John; Kim, Minhyong, Selmer varieties for curves with CM Jacobians. Submitted. Available at the mathematics archive, arXiv:0810.3354 .
- [5] Deligne, Pierre, Le groupe fondamental de la droite projective moins trois points. *Galois groups over \mathbb{Q}* (Berkeley, CA, 1987), 79–297, *Math. Sci. Res. Inst. Publ.*, 16, Springer, New York, 1989. MR1012168 (90m:14016)
- [6] Deligne, Pierre, Équations différentielles à points singuliers réguliers. (French) *Lecture Notes in Mathematics*, Vol. 163. Springer-Verlag, Berlin-New York, 1970. MR0417174 (54:5232)
- [7] Deninger, Christopher, Higher order operations in Deligne cohomology. *Invent. Math.* 120 (1995), no. 2, 289–315. MR1329043 (96f:11085)
- [8] Fontaine, Jean-Marc, Sur certains types de représentations p -adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate. *Ann. of Math. (2)* 115 (1982), no. 3, 529–577. MR657238 (84d:14010)
- [9] Goldman, William M.; Millson, John J., The deformation theory of representations of fundamental groups of compact Kähler manifolds. *Inst. Hautes Etudes Sci. Publ. Math.* No. 67 (1988), 43–96. MR972343 (90b:32041)
- [10] Furusho, Hidekazu, p -adic multiple zeta values. I. p -adic multiple polylogarithms and the p -adic KZ equation. *Invent. Math.* 155 (2004), no. 2, 253–286. MR2031428 (2005b:11095)
- [11] Hain, Richard M., The de Rham homotopy theory of complex algebraic varieties. I. *K-Theory* 1 (1987), no. 3, 271–324. MR908993 (88h:14029)
- [12] Hain, Richard M., *Iterated Integrals and Algebraic Cycles: Examples and Prospects*, *Contemporary Trends in Algebraic Geometry and Algebraic Topology*, *Nankai Tracts in Mathematics*, vol. 5, World Scientific, 2002. MR1945356 (2004a:14009)
- [13] Hain, Richard M., *Periods of Limit Mixed Hodge Structures*, in *CDM 2002: Current Developments in Mathematics in Honor of Wilfried Schmid and George Lusztig*, edited by David Jerison, George Lusztig, Barry Mazur, Tom Mrowka, Wilfried Schmid, Richard Stanley and S.-T. Yau (2003), International Press. MR2059020 (2005e:14015)
- [14] Hain, Richard M.; Zucker, Steven, Unipotent variations of mixed Hodge structure. *Invent. Math.* 88 (1987), no. 1, 83–124. MR877008 (88i:32035)
- [15] Kato, Kazuya, *Lectures on the approach to Iwasawa theory for Hasse-Weil L -functions via B_{dR}* . I. *Arithmetic algebraic geometry* (Trento, 1991), 50–163, *Lecture Notes in Math.*, 1553, Springer, Berlin, 1993. MR1338860 (96f:11067)
- [16] Kim, Minhyong, The motivic fundamental group of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ and the theorem of Siegel. *Invent. Math.* 161 (2005), no. 3, 629–656. MR2181717 (2006k:11119)
- [17] Kim, Minhyong, The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.* 45 (2009), no. 1, pp. 89–133. (Proceedings of special semester on arithmetic geometry, Fall, 2006.) MR2512779
- [18] Kim, Minhyong, Remark on fundamental groups and effective Diophantine methods for hyperbolic curves. To be published in Serge Lang memorial volume. Available at mathematics archive, arXiv:0708.1115.
- [19] Kim, Minhyong, p -adic L -functions and Selmer varieties associated to elliptic curves with complex multiplication. *Annals of Math.* (to be published). Available at mathematics archive: arXiv:0710.5290 (math.AG)
- [20] Kim, Minhyong, and Tamagawa, Akio, The l -component of the unipotent Albanese map. *Math. Ann.* 340 (2008), no. 1, 223–235. MR2349775 (2009a:11132)

- [21] Kim, Minhyong; Hain, Richard M., A de Rham-Witt approach to crystalline rational homotopy theory. *Compos. Math.* 140 (2004), no. 5, 1245–1276. MR2081156 (2005g:14050)
- [22] Kolyvagin, Victor A., On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves. *Proceedings of the International Congress of Mathematicians, Vols. I, II (Kyoto, 1990)*, 429–436, Math. Soc. Japan, Tokyo, 1991. MR1159231 (93c:11046)
- [23] Navarro Aznar, V., Sur la théorie de Hodge-Deligne. *Invent. Math.* 90 (1987), no. 1, 11–76. MR906579 (88j:32037)
- [24] Neukirch, Jürgen; Schmidt, Alexander; Wingberg, Kay, Cohomology of number fields. Second edition. *Grundlehren der Mathematischen Wissenschaften*, 323. Springer-Verlag, Berlin, 2008. xvi+825 pp. MR2392026 (2008m:11223)
- [25] Olsson, Martin, Towards non-abelian p -adic Hodge theory in the good reduction case. Preprint. Available at <http://math.berkeley.edu/~molsson/>.
- [26] Olsson, Martin, The bar construction and affine stacks. Preprint. Available at <http://math.berkeley.edu/~molsson/>.
- [27] Sharifi, Romyar T., Massey products and ideal class groups. *J. Reine Angew. Math.* 603 (2007), 1–33. MR2312552 (2008e:11136)
- [28] Wojtkowiak, Zdzislaw, Cosimplicial objects in algebraic geometry. *Algebraic K-theory and algebraic topology (Lake Louise, AB, 1991)*, 287–327, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 407, Kluwer Acad. Publ., Dordrecht, 1993. MR1367304 (96m:14025)

DEPARTMENT OF MATHEMATICS, UNIVERSITY COLLEGE LONDON, GOWER STREET, LONDON, WC1E 6BT, UNITED KINGDOM AND THE KOREA INSTITUTE FOR ADVANCED STUDY, HOEGIRO 87, DONGDAEMUN-GU, SEOUL 130-722, KOREA