Proceedings of Symposia in Pure Mathematics

Principal bundles and reciprocity laws in number theory

Minhyong Kim

Abstract. We give a brief survey of some ideas surrounding non-abelian Poitou-Tate duality in the setting of arithmetic moduli schemes of principal bundles for unipotent fundamental groups and their Diophantine applications.

1. Principal bundles and their moduli

Moduli spaces of principal bundles (or torsors) have played a prominent role in geometry, topology, and mathematical physics over the last half-century [**2, 12, 21, 25**]. However, it would appear that arithmetic applications predate these developments by many decades. A prominent example is Weil's work on the Jacobian J_X of an algebraic curve X [**23**]. While its analytic construction had been known since the 19th century, Weil gave an algebro-geometric construction so that the inclusion $X \hookrightarrow J_X$ that sends x to the class of the line bundle $\mathcal{O}_X(x) \otimes \mathcal{O}_X(-b)$ might be used to study the arithmetic of X. In Weil's approach, when X is defined over a number field F, so is J_X. Furthermore, choosing an F-rational basepoint $b \in X(F)$, rationality is preserved by the inclusion, suggesting the possibiity of studying $X(F)$ via the superset $J_X(F)$. This research resulted in the Mordell-Weil theorem, stating that $J_X(F)$ is finitely-generated, a result which then was generalised to arbitrary abelian varieties. Weil hoped to prove that the geometric intersection $X \cap J_X(F)$ is finite, thereby proving the Mordell conjecture. However, the abelian nature of $J_X(F)$, a useful property in itself, turned out to be an obstruction more than a help when applied to the arithmetic of X. Nevertheless, the Jacobian was subsequently used by Siegel to prove the finiteness of integral points on affine curves over number fields, thereby convincing arithmeticians of the utility of this abstract construction.

Later, Weil attempted to move beyond the abelian framework by considering moduli spaces $Bun_n(X)$ of vector bundles of rank n over X [**24**]. Serre [**20**] describes this work in his obituary for Weil as 'a text presented as analysis, whose significance is essentially algebraic, but whose motivation is arithmetic.' He correctly stresses the visionary nature of the paper, written long before the advent of geometric invariant theory made it possible to give a systematic treatment of such moduli spaces. Today, they play an important role in various geometric versions of

1991 *Mathematics Subject Classification.* 14G10, 11G40, 81T45 .
Supported by grant EP/M024830/1 from the EPSRC.

the Langlands programme. On the other hand, this remarkable paper also failed to establish any direct link to the arithmetic of curves.

In fact, an important class of moduli spaces for arithmetic applications are those that involve the étale topology of the field F or that of a ring of S-integers $\mathcal{O}_{F,S}$ in F for a finite set S of primes. That is, one obtains algebraic moduli spaces from topological features that do not make direct reference to the algebraic structure of F or $\mathcal{O}_{F,S}$. This is analogous to the way in which the space of representations of the fundamental group of any topological space frequently has the structure of an algebraic variety or stack. In the following, we denote by $H^i(Z, \mathcal{F})$ the cohomology of a sheaf $\mathcal{F}$ in the étale topology of a scheme Z. When $Z = \mathrm{Spec}(R)$ for a ring R, we will follow the standard convention of also writing this as $H^i(R, \mathcal{F})$. For any (sheaf of) abelian group(s) $\mathcal{F}$, $\mathcal{F}[n]$ denotes the n-torsion subobject.

It isn't much of an exaggeration to state that most of the major developments in algebraic number theory of the last several decades have involved in one way or another the following moduli spaces of principal bundles:

(1) $H^1(\mathrm{Spec}(F), A)$ for an abelian variety A over F: The Weil-Chatelet group of A.

(2) $H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), A[n])$, where $A[n]$ is the n-torsion of A, which can be regarded as a locally constant sheaf on some ring of S-integers.

(3) $Ш(F, A) \subset H^1(\mathrm{Spec}(F), A)$, the Tate-Shafarevich group of A. This consists of the principal A-bundles on F that are locally trivial when pulled back to any of the completions $\mathrm{Spec}(F_v) \longrightarrow \mathrm{Spec}(F)$.

(4) $Sel_n(F, A) \subset H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), A[n])$, the n-Selmer group of A, defined by an exact sequence

$$0 \longrightarrow A(F)/nA(F) \longrightarrow Sel_n(F, A) \longrightarrow Ш(F, A)[n] \longrightarrow 0.$$

(5) Pro-finite, divisible, or rationalised versions of the constructions above. For example one might consider the pro-p group $H^1(\mathcal{O}_{F,S}, T_pA) = \varprojlim_n H^1(\mathcal{O}_{F,S}, A[p^n])$, the $\mathbb{Q}_p$-vector space $H^1(\mathcal{O}_{F,S}, V_pA) = H^1(\mathcal{O}_{F,S}, T_pA) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, or the divisible group $H^1(\mathcal{O}_{F,S}, A[p^\infty]) = \varinjlim_n H^1(\mathcal{O}_{F,S}, A[p^n])$.

In all these cases, because the coefficient sheaf is abelian, to view the cohomology as a 'moduli space' may strike the reader as unnatural. In recent years, however, non-abelian cohomology has emerged as a powerful tool for arithmetic geometry, requiring a willingness to consider an H^1 as a geometric object in its own right, especially in relation to non-abelian p-adic Hodge theory **[15]**.

In this article, we will review a rather concrete example, namely, the scheme

$$H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n)$$

of principal bundles for certain sheaves of algebraic groups U_n, which are $\mathbb{Q}_p$-pro-unipotent completions of étale fundamental groups of varieties. In particular, we will see how the geometry is best understood in terms of reciprocity laws or, equivalently, non-abelian extensions of Poitou-Tate duality. In contrast to moduli spaces like $Bun_n(X)$, such étale moduli spaces have the advantage of admitting non-abelian analogues of Abel-Jacobi maps, thereby rendering them useful for Diophantine geometry. In such applications as well, non-abelian Poitou-Tate dualities play a key role in the guise of explicit reciprocity laws.

One kind of important moduli space is that of principal bundles for a constant sheaf A of $p-$adic Lie groups, for example, $A = GL_n(\mathbb{Z}_p)$. In this case, the moduli

space of principal A-bundles on $\mathrm{Spec}(\mathcal{O}_{F,S})$ is the stack of Galois representations

$$\rho : \pi_1(\mathrm{Spec}(\mathcal{O}_{F,S})) \longrightarrow A$$

up to A-conjugation. The study of these spaces is of course one of the central research programmes of number theory. However, it is the view of the author that torsors for non-constant sheaves need to be studied on an equal footing and in a manner complementing and naturally generalising the constant case.

2. Some fundamental groups

Recall Grothendieck's construction of the fundamental group of a scheme X. A geometric point $b : \mathrm{Spec}(K) \longrightarrow X$, that is, a map from the spectrum of a separably closed field, determines a fiber functor

$$F_b : \mathrm{Cov}(X) \longrightarrow \mathrm{Sets}.$$

This goes from the category $\mathrm{Cov}(X)$ of étale covers of X to the category of sets by sending a cover

$$f : Y \longrightarrow X$$

to the fiber

$$Y_b := \{b' : \mathrm{Spec}(K) \longrightarrow Y \mid f \circ b' = b\}$$

over b. Using this, one defines the étale fundamental group of X to be the automorphism group of this fiber functor:

$$\pi_1(X, b) := \mathrm{Aut}(F_b).$$

Similarly, given two geometric points a, b, we get the étale torsor of paths

$$\pi_1(X; b, c) := \mathrm{Isom}(F_b, F_c).$$

Note that there is a natural right action of $\pi_1(X, b)$ on $\pi_1(X; b, c)$, turning it into a torsor.

We focus here on a linearised version **[11]**, where we replace the category $\mathrm{Cov}(X)$ by

$$\mathrm{Un}^{\mathbb{Q}_p}(X)$$

consisting of $\mathbb{Q}_p$-unipotent étale local systems on X. These are lisse $\mathbb{Q}_p$-sheaves $\mathcal{F}$ on X that admit filtrations

$$\mathcal{F} = \mathcal{F}^0 \supset \mathcal{F}^1 \supset \mathcal{F}^2 \supset \cdots \mathcal{F}^n \supset \mathcal{F}^{n+1} = 0$$

such that $\mathcal{F}^i/\mathcal{F}^{i+1}$ is constant. Then $\mathrm{Un}^{\mathbb{Q}_p}(X)$ is a Tannakian category, and a geometric point b now defines a fiber functor

$$F_b : \mathrm{Un}^{\mathbb{Q}_p}(X) \longrightarrow \mathrm{Vect}_{\mathbb{Q}_p}$$

to $\mathbb{Q}_p$-vector spaces by associating to a sheaf its stalk at b. We define the $\mathbb{Q}_p$-pro-unipotent fundamental group to be the tensor compatible automorphisms of this fiber functor

$$U = U(X, b) := \mathrm{Aut}^{\otimes}(F_b).$$

Recall that this means an element $g \in U(\mathbb{Q}_p)$ is a collection of automorphisms

$$g_{\mathcal{F}} : \mathcal{F}_b \longrightarrow \mathcal{F}_b$$

indexed by $\mathcal{F} \in \mathrm{Un}^{\mathbb{Q}_p}(X)$ that are compatible with maps of sheaves and such that $g_{\mathcal{F}\otimes\mathcal{F}'} = g_{\mathcal{F}} \otimes g_{\mathcal{F}'}$. Given two geometric points a and b, there is also a torsor of $\mathbb{Q}_p$-pro-unipotent paths

$$P(c) = U(X; b, c) := \mathrm{Isom}^{\otimes}(F_b, F_c).$$

The case we are interested in is when $X = X_0 \otimes \bar{F}$, where X_0 is a smooth variety defined over F. If we choose $b \in X_0(F)$, then $U(X, b)$ has the structure of a sheaf over $\mathrm{Spec}(\mathcal{O}_{F,S})$ for some finite set[1] S, and $H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U)$ acquires the structure of an affine pro-algebraic scheme over $\mathbb{Q}_p$ [**15**]. A further feature is a descending central series

$$U = U^1 \supset U^2 \supset U^3 \supset \cdots$$

with associated quotients $U_n = U/U^{n+1}$ that can be arranged in a tower

$$\cdots \longrightarrow U_3 \longrightarrow U_2 \longrightarrow U_1$$

and short exact sequences

$$1 \longrightarrow U_n^n \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow 1,$$

where $U_j^i = U^i/U^{j+1}$ for $j \geq i$. This induces a long exact sequence

$$0 \longrightarrow H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n^n) \xrightarrow{i_n} H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n) \xrightarrow{q_n} H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_{n-1}) \xrightarrow{\delta_{n-1}} H^2(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n^n),$$

whose interpretation is that the image of q_n is functorially identified with the kernel of δ_{n-1}, and the fibers of q_n are acted upon simply and transitively by $H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n^n)$. Each of the U_n are finite-dimensional algebraic groups and each $H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n)$ is a $\mathbb{Q}_p$-scheme of finite type. It should be noted that the U_n^n are vector groups, which are furthermore central in U_n. Among the motivations for studying these moduli spaces, it is especially important that a torsor $P(c)$ for $c \in X(\mathcal{O}_{F,S})$ defines a class in $H^1(\mathcal{O}_{F,S}, U)$, giving us a non-abelian Abel-Jacobi map

$$X(\mathcal{O}_{F,S}) \longrightarrow H^1(\mathcal{O}_{F,S}, U),$$
$$c \mapsto [P(c)].$$

Similarly, the pushout torsor

$$P_n(c) = U_n(X; b, c) := U(X; b, c) \times_{U(X,b)} U_n$$

defines an element of $H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n)$.

It is a fact that for each non-Archimedean place v, there is also a long exact sequence

$$0 \longrightarrow H^1(\mathrm{Spec}(F_v), U_n^n) \xrightarrow{i_n} H^1(\mathrm{Spec}(F_v), U_n) \xrightarrow{q_n} H^1(\mathrm{Spec}(F_v), U_{n-1}) \xrightarrow{\delta_{n-1}} H^2(\mathrm{Spec}(F_v), U_n^n).$$

To see this, using [**15**], Proposition 2 and the claim on page 641, it suffices to show that $H^0(G_v, U_n^n) = 0$ for all n. For this, note that U_n^n is a quotient of $V^{\otimes n}$ ([**1**], section 3.6), where V is the $\mathbb{Q}_p$-Tate module of the Albanese variety A of X. Thus,

[1]The set S will be taken large enough so that X_0 has a *good integral model*, i.e., an integral model $\mathcal{X}_0$ over $\mathcal{O}_{F,S}$ with a smooth compactification obtained by adjoining a divisor that has normal crossings relative to $\mathcal{O}_{F,S}$. Also, it should contain all places that divide p. We will assume throughout this paper that p is an odd prime over which the aforementioned smooth compactification of $\mathcal{X}_0$ has good reduction.

by the weight-monodromy conjecture for abelian varieties [**13**], if $v \nmid p$, then U_n^n admits a monodromy filtration

$$0 = M_{-n-1} \subset M_{-n} \subset \cdots \subset M_{n-1} \subset M_n = U_n^n$$

with Gr_i of weight $-n+i$. In particular, the inertia invariant subspace $[U_n^n]^{I_v} \subset M_0$ has weights between $-2n$ and $-n$, and hence, has trivial Frobenius invariants. For $v \mid p$, after passing to a field of semi-stable reduction for A, we apply the same argument to the filtered (ϕ, N)-module $D^{st}(U_n^n)$ following [**8**], where

$$D^{st}(\cdot) = ((\cdot) \otimes B^{st})^{G_v}$$

and B^{st} is Fontaine's semi-stable period ring [**9**]. That is, $D^{st}(V)$, and hence $D^{st}(U_n^n)$ again has a monodromy weight filtration, and

$$(U_n^n)^{G_v} = (D^{st}(U_n^n))^{N=0,\phi=1},$$

(because D^{st} is an equivalence of categories) rendering the argument identical to the $v \nmid p$ case.

3. Reciprocity laws

In the following, we will assume that p is odd. This will enable us to leave out the Archimedean places in the discussion of Poitou-Tate duality for H^1 below.

For each $v \in S$, we can pull back U_n and any U_n-torsor, inducing 'localisation' maps

$$H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n) \longrightarrow H^1(\mathrm{Spec}(F_v), U_n),$$

which come together to an S-localisation map

$$\mathrm{loc}_S^1(U_n) : H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n) \longrightarrow \prod_{v \in S} H^1(\mathrm{Spec}(F_v), U_n).$$

For the abelian sub-quotients, we also have the H^2-versions

$$\mathrm{loc}_S^2(U_n^n) : H^2(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n^n) \longrightarrow \prod_{v \in S} H^2(\mathrm{Spec}(F_v), U_n^n).$$

These localisation maps will be the main subject of our study. Even though it is possible to be more general, for the purposes of this exposition, we will **assume it is possible to choose S so that $\mathbf{loc}_S^i(U_n^n)$ is injective for all n and all $i = 1, 2$.** This appears to be an assumption that's not so easy to check, but for which we can find a good collection of examples. By using the local and global long exact sequences above, it is then straightforward to check inductively that the localization $\mathrm{loc}_S^1(U_n)$ is injective for each n.

We go on to describe a process for inductively finding equations that define the image of $\mathrm{loc}_S^1(U_n)$, limiting ourselves to a brief sketch since the details follow exactly the exposition of [**16**]. Let $G_{F,S} = \pi_1(\mathrm{Spec}(\mathcal{O}_{F,S}), \eta)$, where η comes from an algebraic closure $\bar{F}$ of F. If M is a finitely-generated $\mathbb{Z}_p$-module with continuous action of $G_{F,S}$ and we denote also by M the corresponding sheaf on $\mathrm{Spec}(\mathcal{O}_{F,S})$, by [**19**], Prop. II.2.9, the étale cohomology $H^i(\mathcal{O}_{F,S}, M)$ can be identified with the Galois cohomology $H^i(G_{F,S}, M)$. Similarly, $H^i(F_v, M) \simeq H^i(G_v, M)$, where $G_v = \mathrm{Gal}(\bar{F}_v/F_v)$.

We will need some bits of 'integral structures,' which we construct as follows. Let $\pi = \pi_1^p(X, b)$ be the pro-p étale fundamental group with basepoint b, that is, the maximal pro-p quotient of $\pi_1(X, b)$, which is also a sheaf over $\mathcal{O}_{F,S}$. Let π^n

denote its lower central series and $\pi_n^n := \pi^n/\pi^{n+1}$. Then we have $U_n^n \simeq \pi_n^n \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ [**11**]. Define

$$D(\pi_n^n) := \mathrm{Hom}_{cts}(\pi_n^n, \varinjlim_n \mu_{p^n}),$$

where μ_i is the sheaf of i-th roots of 1 and the subscript refers to the continuous homomorphisms. For each n, we have the localisation map

$$\mathrm{loc}_S^1(D(\pi_n^n)) : H^1(\mathcal{O}_{F,S}, D(\pi_n^n)) \longrightarrow \prod_{v\in S} H^1(F_v, D(\pi_n^n)).$$

Standard Poitou-Tate duality [**22**] says that we have an exact sequence

$$H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n^n) \longrightarrow \prod_{v\in S} H^1(\mathrm{Spec}(F_v), U_n^n) \xrightarrow{\mathrm{loc}_S^1(D(\pi_n^n))^* \circ D_S} H^1(\mathcal{O}_{F,S}, D(\pi_n^n))^\vee \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Here, $(\cdot)^\vee := \mathrm{Hom}_{cts}(\cdot, \mathbb{Q}/\mathbb{Z})$ is the Pontriagin dual. The second map is induced by a composition of the dual of localisation and local Tate duality (Op. Cit.):

$$\prod_{v\in S} H^1(\mathrm{Spec}(F_v), \pi_n^n) \simeq^{D_S} \prod_{v\in S} H^1(\mathrm{Spec}(F_v), D(\pi_n^n))^\vee \xrightarrow{\mathrm{loc}_S^1(D(\pi_n^n))^*} H^1(\mathcal{O}_{F,S}, D(\pi_n^n))^\vee.$$

Let us examine briefly the target of this map.

LEMMA 3.1. *Let M be a finitely-generated $\mathbb{Z}_p$-module with a continuous action of $G_{F,S}$. Then*

$$H^1(G_{F,S}, D(M))^\vee \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq H^1(G_{F,S}, M^*(1))^* \otimes \mathbb{Q}_p,$$

where $(\cdot)^*$ denotes the $\mathbb{Z}_p$-dual and $(\cdot)(1) := (\cdot) \otimes \mathbb{Z}_p(1) = (\cdot) \otimes \varprojlim_n (\mu_{p^n})$.

PROOF. Then there is an exact sequence

$$0 \longrightarrow M_{tor} \longrightarrow M \longrightarrow \bar{M} \longrightarrow 0,$$

where M_{tor} is the finite torsion subgroup and $\bar{M}$ is free. Thus, we get an exact sequence

$$0 \longrightarrow D(\bar{M}) \longrightarrow D(M) \longrightarrow D(M_{tor}) \longrightarrow 0.$$

Therefore, the natural map

$$H^1(G_{F,S}, D(\bar{M})) \longrightarrow H^1(G_{F,S}, D(M))$$

is an isogeny, that is, has finite kernel and cokernel. Hence, the map

$$H^1(G_{F,S}, D(M))^\vee \otimes \mathbb{Q}_p \longrightarrow H^1(G_{F,S}, D(\bar{M}))^\vee \otimes \mathbb{Q}_p$$

is an isomorphism. Meanwhile, we have $\bar{M}^* \simeq M^*$, and hence,

$$H^1(G_{F,S}, \bar{M}^*(1))^* \simeq H^1(G_{F,S}, M^*(1))^*.$$

Therefore, we may assume that M is free.

Then

$$\begin{aligned}\mathrm{Hom}_{cts}(M, \varinjlim_n \mu_{p^n}) = \varinjlim_n \mathrm{Hom}_{cts}(M, \mu_{p^n}) = \varinjlim_n \mathrm{Hom}_{cts}(M, \mathbb{Z}_p(1) \otimes_{\mathbb{Z}_p} \frac{1}{p^n}\mathbb{Z}/\mathbb{Z}) \\ = M^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p.\end{aligned}$$

Therefore,

$$H^1(G_{F,S}, D(M)) \simeq H^1(G_{F,S}, M^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p).$$

This time, considering the exact sequence

$$0 \longrightarrow M^*(1) \longrightarrow M^*(1) \otimes \mathbb{Q}_p \longrightarrow M^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

we see that the map

$$H^1(G_{F,S}, M^*(1)) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(G_{F,S}, M^*(1) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

is an isogeny. But we also have an isogeny

$$H^1(G_{F,S}, M^*(1)) \otimes \mathbb{Q}_p/\mathbb{Z}_p \simeq \mathrm{Hom}_{cts}(\mathbb{Z}_p, H^1(G_{F,S}, M^*(1)) \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

$$\longrightarrow \mathrm{Hom}(H^1(G_{F,S}, M^*(1))^*, \mathbb{Q}_p/\mathbb{Z}_p),$$

from which we obtain two isogenies

$$H^1(G_{F,S}, M^*(1))^* \longrightarrow (H^1(G_{F,S}, M^*(1)) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee$$

and

$$H^1(G_{F,S}, D(M))^\vee \longrightarrow (H^1(G_{F,S}, M^*(1)) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^\vee.$$

Hence, we end up with an isomorphism

$$H^1(G_{F,S}, D(M))^\vee \otimes \mathbb{Q}_p \simeq (H^1(G_{F,S}, M^*(1))^*) \otimes \mathbb{Q}_p.$$

□

Using the lemma, the Poitou-Tate exact sequence above can be rewritten as

$$H^1(\mathrm{Spec}(\mathcal{O}_{F,S}), U_n^n) \longrightarrow \prod_{v\in S} H^1(\mathrm{Spec}(F_v), U_n^n) \xrightarrow{\mathrm{loc}_S^1((U_n^n)^*(1))^* \circ D_S} H^1(\mathcal{O}_{F,S}, (U_n^n)^*(1))^*.$$

Here, the $(\cdot)^*$ now denotes the $\mathbb{Q}_p$-dual and the twist $(\cdot)(1)$ the tensor product with $\mathbb{Q}_p(1) = \mathbb{Z}_p(1) \otimes \mathbb{Q}_p$. Taking $n = 1$, this gives defining equations for $Im(\mathrm{loc}_S(U_1))$, in the sense that a basis $\{v_i\}$ for $H^1(\mathcal{O}_{F,S}, U_1^*(1)))$ will give a collection of functions on

$$\prod_{v\in S} H^1(\mathrm{Spec}(F_v), U_1)$$

whose common zero set is exactly this image.

Now assume $n \geq 2$ and that we have found defining equations ϕ_i for $Im(\mathrm{loc}_S(U_{n-1}))$. In the long exact sequence

$$0 \longrightarrow \prod_{v\in S} H^1(F_v, U_n^n) \xrightarrow{i_n^S} \prod_{v\in S} H^1(F_v, U_n) \xrightarrow{q_n^S} \prod_{v\in S} H^1(F_v, U_{n-1})$$

$$\xrightarrow{\delta_{n-1}^S} \prod_{v\in S} H^2(F_v, U_n^n),$$

consider

$$E_n := (q_n^S)^{-1}(Im(\mathrm{loc}_S^1(U_{n-1}))) \subset \prod_{v\in S} H^1(F_v, U_n).$$

Taking into account the injectivity of localisation at the H^1-level, we have a commutative diagram as follows:

$$\begin{array}{ccc} H^1(\mathcal{O}_{F,S}, U_n^n) & \hookrightarrow & \prod_{v\in S} H^1(F_v, U_n^n) \\ \downarrow & & \downarrow \\ H^1(\mathcal{O}_{F,S}, U_n) & \hookrightarrow & E_n \\ \downarrow{\scriptstyle q_n} & & \downarrow{\scriptstyle q_n^S} \\ \mathrm{loc}_S^1(U_{n-1})^{-1}(Im(q_n^S)) & \simeq & Im(H^1(\mathcal{O}_{F,S}, U_{n-1}) \cap Im(q_n^S) \end{array}$$

Note that because E_n is defined as a full inverse image, $\prod_{v\in S} H^1(F_v, U_n^n)$ still acts on it as in this diagram. Also, by our assumption about the injectivitity at the H^2 level, the map q_n in the diagram is surjective and gives $H^1(\mathcal{O}_{F,S}, U_n)$ the structure of an $H^1(\mathcal{O}_{F,S}, U_n^n)$-torsor over it. Also, $Im(q_n^S)$ is closed, since it's the kernel of the boundary map. Hence, $\mathrm{loc}_S^1(U_{n-1})^{-1}(Im(q_n^S))$ is an affine scheme. Therefore, we can choose a scheme-theoretic splitting

$$s_n : \mathrm{loc}_S^1(U_{n-1})^{-1}(Im(q_n^S)) \longrightarrow H^1(\mathcal{O}_{F,S}, U_n^n).$$

This allows us to define an algebraic map

$$r_n : E_n \longrightarrow \prod_{v\in S} H^1(F_v, U_n^n)$$

via the formula

$$x = \mathrm{loc}_S^1(U_n)(s_n(\mathrm{loc}_S^1(U_{n-1})^{-1}(q_n^S(x)))) + r_n(x).$$

That is, if we suppress the localisation maps from the notation, $r_n(x)$ is the $\prod_{v\in S} H^1(F_v, U_n^n)$ discrepancy between x and the splitting map evaluated at $q_n^S(x)$. We thus get a map

$$E_n \xrightarrow{r_n} \prod_{v\in S} H^1(F_v, U_n^n) \xrightarrow{\mathrm{loc}_S^1((U_n^n)^*(1))^* \circ D_S} H^1(\mathcal{O}_{F,S}, (U_n^n)^*(1))^\vee.$$

As in **[16]**, by Poitou-Tate duality applied to U_n^n, we get

Proposition 3.2. *The map*

$$loc_S^1(D(\pi_n^n))^* \circ D_S \circ r_n$$

is independent of the splitting s_n, and

$$Im(H^1(\mathcal{O}_{F,S}, U_n)) \subset E_n$$

is its kernel.

Since each E_n is a closed subscheme of $\prod_{v\in S} H^1(F_v, U_n)$, each r_n can be extended to

$$\tilde{r}_n : \prod_{v\in S} H^1(F_v, U_n)) \longrightarrow \prod_{v\in S} H^1(F_v, U_n^n).$$

From this, we get a sequence of maps

$$(\mathrm{loc}_S^1(D(\pi_n^n))^* \circ D_S \circ \tilde{r}_n)^* : H^1(\mathcal{O}_{F,S}, (U_n^n)^*(1)) \longrightarrow \mathcal{O}(\prod_{v\in S} H^1(F_v, U_n)).$$

The discussion above can be summarised as follows:

> [**Non-abelian Poitou-Tate duality**] The choice of extensions $\tilde{r}_n$ for $i \leq n$ above define a map
>
> $$\Psi : \bigoplus_{i=1}^{n} H^1(\mathcal{O}_{F,S}, (U_i^i)^*(1)) \longrightarrow \mathcal{O}(\prod_{v\in S} H^1(F_v, U_n))$$
>
> such that $(Im(\Psi))$ is the defining ideal of $Im(H^1(\mathcal{O}_{F,S}, U_n))$. The ideal $(Im(\Psi))$ does not depend on the choice of $\tilde{r}_n$.

4. Explicit reciprocity laws on curves

The main applications so far of the theory of the previous section are to explicit reciprocity laws on hyperbolic curves **[3, 6, 10]**, and we give a brief survey of illustrative examples. Some other works with further developments which we do not discuss include **[4]** and **[5]**. It should be noted that most of these examples do not make direct use of the reciprocity laws described here. However, reciprocity should be viewed as the organising principle explaining the numerical examples from a theoretical standpoint.

When X_0 is a hyperbolic curve defined over F with a good integral model (cf. footnote 1 in section 1) and compactification over $\mathcal{O}_{F,S}$, then one gets a diagram

$$\begin{array}{ccc} X_0(\mathcal{O}_{F,S}) & \longrightarrow & \prod_{v\in S} X_0(F_v) \\ \downarrow & & \downarrow{\scriptstyle j_n} \\ H^1(\mathcal{O}_{F,S}, U_n) & \longrightarrow & \prod_{v\in S} H^1(F_v, U_n) \end{array}$$

so that equations defining $Im(\mathrm{loc}_S^1(U_n))$ can be pulled back via j_n to give analytic defining equations for $X_0(\mathcal{O}_{F,T})$ inside $\prod_{v\in S} X_0(F_v)$ for various subsets $T \subset S$. In this discussion, we assume that the primes dividing p are not in T. Then the condition of integrality at $v \notin T$ defines subspaces **[15]** $H_f^1(F_v, U_n) \subset H^1(F_v, U_n)$, so that

$$X_0(\mathcal{O}_{F,T}) \subset [\prod_{v\in S} X_0(F_v)]_{n,T}$$

$$:= j_n^{-1}[Im(H^1(\mathcal{O}_{F,S}, U_n)) \cap [\prod_{v\in S\setminus T} H_f^1(F_v, U_n) \times \prod_{v\in T} H^1(F_v, U_n)]],$$

incorporating at once the condition of coming from global cohomology and that of being integral at $v \notin T$.

So far, this method has been tested only for $F = \mathbb{Q}$. One typically projects the zero set to $X_0(\mathbb{Z}_p)$, and gets a union of analytic sets depending on the equations. That is, one defines

$$X_0(\mathbb{Z}_p)_{n,T} := \mathrm{Pr}_p([\prod_{v\in S} X_0(\mathbb{Q}_v)]_{n,T})$$

where

$$\mathrm{Pr}_p : \prod_{v\in S} X_0(\mathbb{Q}_v) \longrightarrow X_0(\mathbb{Q}_p)$$

is the projection to the $\mathbb{Q}_p$ component, which is then a set that contains $X(\mathbb{Z}[1/T])$.

Here then are a few examples. We refer to the papers cited for precise explanations of the notation.

4.1. The projective line minus three points. (Joint work with Balakrishnan, Dan-Cohen, and Wewers **[3]**, as well as the paper of Dan-Cohen and Wewers **[10]**.)

Let $X_0 = \mathbb{P}^1\backslash\{0,1,\infty\}$. In this case, it is easy to check directly that $X_0(\mathbb{Z}[1/2]) = \{2,-1,1/2\}$. Using the reciprocity law, we find

$$X_0(\mathbb{Z}_p)_{4,\{2\}} \subset \{D_2(z)=0\}\cap\{D_4(z)=0\}.$$

Here,

$$D_2(z) = \ell_2(z) + (1/2)\log(z)\log(1-z)$$

and

$$D_4(z) = \zeta(3)\ell_4(z) + (8/7)[\log^3 2/24 + \ell_4(1/2)/\log 2]\log(z)\ell_3(z)$$
$$+[(4/21)(\log^3 2/24 + \ell_4(1/2)/\log 2) + \zeta(3)/24]\log^3(z)\log(1-z).$$

The log here refers to the p-adic logarithm and $\ell_k(z)$ the p-adic k-logarithm, which can be defined in a disk by a series

$$\ell_k(z) = \sum_{n=1}^{\infty}\frac{z^n}{n^k}$$

and analytically continued using Coleman integration. Numerically, this zero set appears to be exactly equal to $\{2,-1,1/2\}$.

4.2. Punctured elliptic curves. (Joint with Balakrishnan, Dan-Cohen, and Wewers **[3]**)

Let $X_0 = E\setminus O$ where E is a semi-stable elliptic curve of rank 0 and

$$|Ш(E)(p)| < \infty.$$

We use Coleman integration to define the p-adic logarithm on the elliptic curve:

$$\log(z) = \int_b^z (dx/y).$$

(b is a tangential base-point) as well as a dilogarithm:

$$D_2(z) = \int_b^z (dx/y)(xdx/y).$$

Let T be the set of primes of bad reduction. For each $l\in T$, let

$$N_l = \mathrm{ord}_l(\Delta_{\mathcal{E}}),$$

where $\Delta_{\mathcal{E}}$ is the minimal discriminant. Define a set

$$W_l := \{(n(N_l-n)/2N_l)\log l \mid 0\le n < N_l\},$$

and for each $w=(w_l)_{l\in S}\in W := \prod_{l\in S} W_l$, define

$$\|w\| = \sum_{l\in S} w_l.$$

With assumptions as above

$$X_0(\mathbb{Z}_p)_2 \subset \cup_{w\in W} Z(w),$$

where

$$Z(w) := \{z \in X_0(\mathbb{Z}_p) \mid \log(z) = 0,\ D_2(z) = \|w\|\}.$$

Of course,

$$X_0(\mathbb{Z}) \subset X_0(\mathbb{Z}_p)_2,$$

but depending on the reduction of E, the latter could be made up of a large number of $\Psi(w)$, creating potential for some discrepancy. In fact, so far, we have checked

$$X_0(\mathbb{Z}) = X_0(\mathbb{Z}_p)_2$$

for the prime $p = 5$ and 256 semi-stable elliptic curves of rank zero, some of which are listed in the following table.

Cremona label	number of $\|\|w\|\|$-values
1122m1	128
1122m2	384
1122m4	84
1254a2	140
1302d2	96
1506a2	112
1806h1	120
2442h1	78
2442h2	84
2706d2	120
2982j1	160
2982j2	140
3054b1	108

Hence, for example, for the curve $1122m2$,

$$y^2 + xy = x^3 - 41608x - 90515392$$

there are potentially 384 of the $Z(w)$'s that make up $X_0(\mathbb{Z}_p)_2$. Of these, all but 4 end up being empty, while the points in those $Z(w)$ consist exactly of the integral points

$$(752, -17800), (752, 17048), (2864, -154024), (2864, 151160).$$

4.3. A compact curve of genus 2. (Balakrishnan and Dogra, private communication, based on **[6]**)

Let X_0 be a smooth projective model of

$$y^2 = x^6 + 31x^4 + 31x^2 + 1,$$

a curve of genus 2, rank 4. Put $z_0 = (0, 1)$, $w = (-7, 440)$. Let $E/\mathbb{Q}$ denote the rank 2 elliptic curve

$$y^2 = x^3 + 31x^2 + 31x + 1$$

with Mordell-Weil generators $P_1 = (-29, 28), P_2 = (-15, 56)$, and let

$$f_1, f_2 : X_0 \longrightarrow E$$

be defined by $f_1(x,y) = (x^2, y)$ and $f_2(x,y) = (1/x^2, y/x^3)$.a Let $k_1 = \log_E(P_1)$, $k_2 = \log_E(P_2)$, $\omega_i = x^i dx/2y$, and

$$\begin{aligned}
F_2(z) &= \log_E(f_2(z)) \\
F_3(z) &= -\frac{1}{4}x(z) + \int_{z_0}^{z}(-\omega_0\omega_3 + 31\omega_1\omega_2 + 2\omega_1\omega_4) \\
&\quad - \frac{1}{2}\left(\int_{z_0}^{z}\omega_0\right)\left(\int_{-z_0}^{z_0}\omega_3\right) + \frac{31}{2}\left(\int_{z_0}^{z}\omega_1\right)\left(\int_{-z_0}^{z_0}\omega_2\right) \\
&\quad + \left(\int_{z_0}^{z}\omega_1\right)\left(\int_{-z_0}^{z_0}\omega_4\right) \\
F_4(z) &= \int_{z_0}^{z}\omega_0\omega_1 - \omega_1\omega_0 \\
a_3 &= F_3(w) \\
a_4 &= F_4(w) - \frac{1}{4}\left(3k_1k_2 + k_1^2\right).
\end{aligned}$$

Then

$$X_0(\mathbb{Q}) = X_0(\mathbb{Z}) \subset X_0(\mathbb{Z}_p)_2 \subset \{a_4F_3(z) - a_3\left(F_4(z) - \frac{k_1}{4}F_2(z)\right) = 0\}.$$

Searching numerically among the zeros reveals the following set of rational points:

$X_0(\mathbb{F}_3)$	$x(z) \in \mathbb{Z}_3$	$z \in X_0(\mathbb{Q})$
$(0, \pm 1)$	$O(3^8)$	$(0, \pm 1)$
	$2 \cdot 3 + 2 \cdot 3^3 + 2 \cdot 3^5 + 3^7 + O(3^8)$	
	$3 + 2 \cdot 3^2 + 2 \cdot 3^4 + 2 \cdot 3^6 + 3^7 + O(3^8)$	
$(1, \pm 2)$	$1 + O(3^8)$	$(1, \pm 8)$
	$1 + 2 \cdot 3 + O(3^8)$	$(7, \pm 440)$
	$1 + 3 + 2 \cdot 3^3 + 3^4 + 2 \cdot 3^5 + 3^7 + O(3^8)$	$(\frac{1}{7}, \pm\frac{440}{343})$
$(2, \pm 2)$	$2 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5 + O(3^6)$	$(-7, \pm 440)$
	$2 + 3 + 2 \cdot 3^2 + 3^4 + O(3^6)$	$(-\frac{1}{7}, \pm\frac{440}{343})$
	$8 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5 + O(3^6)$	$(-1, \pm 8)$
$\infty^{\pm}$	$\frac{2}{3} + 1 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + O(3^7)$	
	$3^{-1} + 1 + 2 \cdot 3^5 + O(3^6)$	
	$\infty^{\pm}$	$\infty^{\pm}$

5. Analogies to gauge theory

Once again, let X_0/F and let $\mathbb{A}_F$ be the ring of adeles. Philips Candelas and Xenia de la Ossa have communicated to me the viewpoint that

$$X_0(F) \subset X_0(\mathbb{A}_F)$$

should be thought of from the physicist's perspective as the 'space of classical paths' sitting inside the space of quantum paths, which themselves can be quite jagged. While this viewpoint may appear fanciful from a strictly mathematical perspective, it appears to fit in well with the formalism of this paper.

As described in **[17]**, there is a universal unipotent lisse sheaf $\mathcal{P} \longrightarrow X_0$ with the property that given any point $c : \mathrm{Spec}(F) \longrightarrow X_0$, we have

$$P(c) = c^*\mathcal{P}.$$

Similarly, a local point $c_v : \mathrm{Spec}(F_v) \longrightarrow X_0$ gives rise to a local torsor $P(c_v) = c_v^*(\mathcal{P})$. In short, the univeral torsor $\mathcal{P}$ is responsible for converting the 'classical paths' $X(F)$ into global torsors on $\mathrm{Spec}(F)$, and the quantum path $(c_v) \in X(\mathbb{A}_F)$ into a collection of local torsors. That is, it associates to classical and quantum paths classical and quantum gauge fields on $\mathrm{Spec}(F)$.

In the previous section, we have emphasised a fixed finite set of places, but of course, it would have been straightforward, as in [**16**], to study an adelic localisation

$$\varinjlim_{S} H^1(\mathcal{O}_{F,S}, U_n) \xrightarrow{\mathrm{loc}_{\mathbb{A}_F}} {\prod}' H^1(F_v, U_n),$$

except the restricted direct product requires some care to define properly. When this is done, we would again have a map

$$\bigoplus_{i=1}^{n} \varinjlim_{S} H^1(\mathcal{O}_{F,S}, (U_n^n)^*(1)) \longrightarrow \mathcal{O}({\prod}' H^1(F_v, U_n))$$

whose image cuts out the global torsors. From this point of view, each element of a $H^1(\mathcal{O}_{F,S}, (U_n^n)^*(1))$ gives an 'equation of motion' satisfied by the 'classical fields', which then can be translated into equations for classical paths via the non-abelian Abel-Jacobi map. However, the gauge-theoretic formulation of this analogy appears to be more natural than the one involving paths.

From an arithmetic viewpoint, the importance of this analogy is somewhat captured by the computations of the previous section. Whenever it's possible to describe the global image explicitly, one obtains analytic equations defining global points inside spaces of local points. However, many of the methods used so far have been somewhat ad hoc. On the other hand, there is indication that physicists (cf. [**14**]) have a better intuition for such localisation maps, at least in the setting of principal bundles on 3-manifolds with boundary. There, localisation corresponds to restriction of principal bundles to a boundary two-manifold. It is this intuition that would be useful to translate into an arithmetic setting. A beginning has been made in [**18**] and [**7**].

Acknowledgement: I am grateful for the organisers of the AMS summer institute for the invitation to write this paper. I am also grateful to two anonymous referees for their helpful comments and corrections.

References

[1] Andreatta, Fabrizio; Iovita, Adrian; and Minhyong Kim A p-adic nonabelian criterion for good reduction of curves. Duke Math. J. Volume 164, Number 13 (2015), 2597–2642.

[2] Atiyah, Michael F.; Bott, Raoul The Yang-Mills equations over Riemann surfaces. Philos. Trans. Roy. Soc. London Ser. A 308 (1983), no. 1505, 523âĂŞ615.

[3] Balakrishnan, Jennifer, Dan-Cohen, Ishai, Kim, Minhyong, Wewers, Stefan A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves. arXiv:1209.0640

[4] Balakrishnan, Jennifer S.; Besser, Amnon Coleman-Gross height pairings and the p-adic sigma function. J. Reine Angew. Math. 698 (2015), 89–104.

[5] Balakrishnan, Jennifer S.; Besser, Amnon; Mueller, J.S. Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves, Journal fuer die reine und angewandte Mathematik, 720 (2016), 51–79.

[6] Balakrishnan, Jennifer, Dogra, Netan Quadratic Chabauty and rational points I: p-adic heights. arXiv:1601.00388

[7] Chung, Hee-Joong; Kim, Dohyeong; Kim, Minhyong; Park, Jeehoon; Yoo, Hwajong Arithmetic Chern-Simons Theory II. arXiv:1609.03012 [math.NT].

[8] Coleman, Robert; Iovita, Adrian The Frobenius and monodromy operators for curves and abelian varieties. Duke Math. J. 97 (1999), no. 1, 171–215.
[9] Colmez, Pierre; Fontaine, Jean-Marc Construction des représentations p-adiques semi-stables. Invent. Math. 140 (2000), no. 1, 1–43.
[10] Dan-Cohen, Ishai, Wewers, Stefan Mixed Tate motives and the unit equation. arXiv:1311.7008
[11] 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.
[12] Donaldson, Simon K. An application of gauge theory to four-dimensional topology. J. Differential Geom. 18 (1983), no. 2, 279–315.
[13] Grothendieck, Alexandre. *Séminaire de Géométrie Algébrique du Bois Marie - 1967-69 - Groupes de monodromie en géométrie algébrique* - (SGA 7), vol. 1. Lecture notes in mathematics. 288. Berlin; New York: Springer-Verlag.
[14] Gukov, Sergei Three-dimensional quantum gravity, Chern-Simons theory, and the A-polynomial. Comm. Math. Phys. 255 (2005), no. 3, 577–627.
[15] 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.
[16] Kim, Minhyong Diophantine geometry and non-abelian reciprocity laws I. Documenta Mathematica (to be published), and arXiv:1312.7019
[17] Kim, Minhyong The unipotent Albanese map and Selmer varieties for curves. Publ. Res. Inst. Math. Sci. 45 (2009), no. 1, 89–133.
[18] Kim, Minhyong Arithmetic Chern-Simons Theory I. arXiv:1510.05818 [math.NT].
[19] Milne, James *Arithmetic Duality Theorems*. 2nd ed., available from www.jamesmilne.org (2006).
[20] Serre, Jean-Pierre André Weil 6 May 1906-6 August 1998 Biographical Memoirs of Fellows of the Royal Society, Vol. 45, (Nov., 1999), pp. 521–529
[21] Simpson, Carlos T. Higgs bundles and local systems. Inst. Hautes Études Sci. Publ. Math. No. 75 (1992), 5–95.
[22] Tate, John Duality theorems in Galois cohomology over number fields. 1963 Proc. Internat. Congr. Mathematicians (Stockholm, 1962) pp. 288–295
[23] Weil, André L'arithmétique sur les courbes algèbriques. Acta Math. 52 (1929), no. 1, 281–315.
[24] Weil, André Généralisation des fonctions abéliennes. J. Math Pur. Appl. 17 (1938), no. 9, 47–87.
[25] Witten, Edward Quantum field theory and the Jones polynomial. Comm. Math. Phys. 121 (1989), no. 3, 351–399.

Mathematical Institute, University of Oxford and The Korea Institute for Advanced Study