Principal Bundles and Reciprocity Laws

Minhyong Kim

Simons Symposium, May, 2017

Some background on principal bundles in arithmetic

X/F an (smooth proper) algebraic curve of genus g over a number field F.

Weil: Algebraic construction of

$$J_F = Bun^0(X, \mathbb{G}_m),$$

the Jacobian of F.

Motivation: $b \in X(F)$ defines and embedding

$$X(F) \hookrightarrow J(F);$$

$$a \mapsto \mathcal{O}(a) \otimes \mathcal{O}(b)^{-1}.$$

Failed to apply J_F to the study of $X(F)$ when $g > 1$. However, Siegel later used J_F to prove finiteness of integral points on affine curves. Later, it was used in an entirely different way in Faltings's proof of the Mordell conjecture.

Some background on principal bundles in arithmetic

Later, Weil constructed

$$Bun(X, GL_n)$$

hoping to apply it to the Mordell conjecture. Enormously influential in geometry: work of Narasimham-Seshadri, Atiyah-Bott, Donaldson, Hitchin, Simpson, Witten, ...

One point of view emerging from the geometry is that spaces like $Bun(X, G)$ and variants can be important invariants of X itself (for manifolds more general than Riemann surfaces), especially in work of Donaldson and Witten.

But also indirect application to Diophantine problems via the Langlands programme.

Some background on reciprocity

F: number field.

We have the reciprocity map

$$rec : \mathbb{G}_m(\mathbb{A}_F) \longrightarrow G_F^{ab}$$

and the Takagi-Artin reciprocity law:

$$rec|\mathbb{G}_m(F) = 0.$$

Gives a defining equation for global points inside adelic points.

Some background on reciprocity

Leads to a generalisation to *class field theory with non-abelian coefficients*.

When X/F is a smooth variety satisfying some mild technical conditions on cohomology, we have a filtration

$$X(\mathbb{A}_F) = X(\mathbb{A}_F)_1 \supset X(\mathbb{A}_F)_2 \supset X(\mathbb{A}_F)_3 \supset X(\mathbb{A}_F)_4 \supset \cdots$$

and a sequence of maps

$$rec_n : X(\mathbb{A}_F)_n \longrightarrow \mathfrak{G}_n(F, X)$$

with $X(\mathbb{A}_F)_n = rec_{n-1}^{-1}(0)$.

Some background on reciprocity

Here,

$$\mathfrak{G}_n(F, X) := \mathrm{Hom}[H^1(G_F, D(T_n)), \mathbb{Q}/\mathbb{Z}],$$

where

$$T_n = \pi_1(\bar{X}, b)^{[n]}/\pi_1(\bar{X}, b)^{[n+1]}$$

and

$$D(T_n) = \varinjlim_{m} \mathrm{Hom}(T_n, \mu_m).$$

Some background on reciprocity

Non-abelian Artin reciprocity law:

$$X(F) \subset \cap_{n=1}^{\infty} X(A_F)_n.$$

Would like to apply this to the Diophantine geometry of X.

For example, projecting onto $X(F_v)$, we get a filtration

$$X(F_v) \supset X(F_v)_2 \supset X(F_v)_3 \supset X(F_v)_4 \supset \cdots$$

on v-adic points of X.

Some background on reciprocity

Conjecture

Suppose $F = \mathbb{Q}$, p is odd, and X is compact. Then

$$\cap_{n=1}^{\infty} X(\mathbb{Q}_p)_n = X(\mathbb{Q}).$$

For affine curves, can formulate $S-$integral analogues

$$X(\mathbb{Z}_p)_S \supset X(\mathbb{Z}_p)_{S,2} \supset X(\mathbb{Z}_p)_{S,3} \supset X(\mathbb{Z}_p)_{S,4} \supset \cdots .$$

such that

$$X(\mathbb{Z}[1/S]) \subset \cap_{n=1}^{\infty} X(\mathbb{Z}_p)_{S,n}$$

and conjecture something similar.

Explicit reciprocity laws: Examples

[Dan-Cohen, Wewers]

For $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$, consider

$$X(\mathbb{Z}_p)_{\{2\}} \supset X(\mathbb{Z}_p)_{\{2\},2} \supset X(\mathbb{Z}_p)_{\{2\},3} \supset X(\mathbb{Z}_p)_{\{2\},4} \supset \cdots .$$

We have

$$X(\mathbb{Z}_p)_{\{2\},3}$$

$$\subset [\cup_{m,n}\{z \mid \log(z) = n\log(2), \log(1-z) = m\log(2)\}] \cap \{D_2(z) = 0\},$$

where

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

and

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

Explicit reciprocity laws: Examples

Also,

$$
\begin{gathered}
X(\mathbb{Z}_p)_{\{2\},5} \\
\subset [\cup_{m,n}\{z \mid \log(z) = n\log(2), \log(1-z) = m\log(2)\}] \\
\cap\{D_2(z) = 0\} \cap \{D_4(z) = 0\},
\end{gathered}
$$

where

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

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

Numerically, this appears to be equal to $\{2, -1, 1/2\} = X(\mathbb{Z}[1/2])$.

Explicit reciprocity laws: Examples

[N. Dogra and J. Balakrishnan]

$X : y^2 = x^6 + 31x^4 + 31x^2 + 1$, a curve of genus 2, rank 4.

$z_0 = (0, 1)$, $w = (-7, 440)$, $\omega_i = x^i dx/2y$.

$E/\mathbb{Q}$: rank 2 elliptic curve

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

with Mordell-Weil generators

$$P_1 = (-29, 28), P_2 = (-15, 56).$$

$k_1 = \log_E(P_1)$, $k_2 = \log_E(P_2)$.

We have a map

$$f : X \longrightarrow E;$$

$$(x, y) \mapsto (1/x^2, y/x^3).$$

Explicit reciprocity laws: Examples

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

Explicit reciprocity laws: Examples

Then
$$X(\mathbb{Q}) \subset a_4 F_3(z) - a_3\left(F_4(z) - \frac{k_1}{4}F_2(z)\right) = 0.$$

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

Explicit reciprocity laws: Examples

$(2, \pm 2)$	$2 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5 + O(3^6)$	$(-7, \pm 440)$
	$2 + 3 + 2 \cdot 3^2 + 3^4 + O(3^6)$ $8 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 2 \cdot 3^5 + O(3^6)$	$(-\frac{1}{7}, \pm \frac{440}{343})$ $(-1, \pm 8)$
$\infty^{\pm}$	$\frac{2}{3} + 1 + 2 \cdot 3 + 2 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + O(3^7)$ $3^{-1} + 1 + 2 \cdot 3^5 + O(3^6)$ $\infty^{\pm}$	 $\infty^{\pm}$

For example,

$$a_4 F_3(-1/7, 440/343) - a_3 F_4(-1/7, 440/343)$$

$$-a_3 \frac{k_1}{4} F_2(-1/7, 440/343) = 0$$

Arithmetic principal bundles

Previous formulas all follow from a study of moduli of arithmetic principal bundles.

$M = \mathrm{Spec}(\mathcal{O}_{F,S})$, S a set of places.

We study

$$H^1(M, A),$$

the isomorphism classes of principal A bundles, for various sheaves of groups A.

This includes:

–$A = V$, a $\mathbb{Z}_p$ or $\mathbb{Q}_p$ Galois representation.
–$A = \pi_1(\bar{X}, b)$ or $U(\bar{X}, b)$, a profinite fundamental group or pro-unipotent fundamental group;
–$A = GL_n(\mathbb{Z}_p)$ or $GL_n(\mathbb{Q}_p)$, a constant group.

Arithmetic principal bundles

Because $H^1(M, A)$ is difficult, we try to make use of

$$H^1(\partial M, A) := \prod_{v \in S} H^1(\mathrm{Spec}(F_v), A)$$

and the map

$$loc_S : H^1(M, A) \longrightarrow H^1(\partial M, A) := \prod_{v \in S}{}' H^1(\mathrm{Spec}(F_v), A)$$

For example, if A is a $\mathbb{Q}_p$-algebraic group, one often has formulas like

$$H^1(\mathrm{Spec}(F_v), A) = (A/N_v A)^{Fr_v}$$

or

$$H^1_f(\mathrm{Spec}(F_v), A) = D^{cr}(A)/[F^0 + D^{cr}(A)^{\phi_v}].$$

Arithmetic principal bundles and reciprocity laws

The localisation loc_S is often an inclusion, for example, if S is the set of *all* places. From this point of view, a major problem is to find equations defining the image of loc_S.

These are *reciprocity laws.*

When $A = V$, a Galois representation, let $c \in H^1(M, V^*(1))$. We get thereby a map

$$\phi : H^1(\partial M, V) \simeq H^1(\partial M, V^*(1))^* \xrightarrow{loc_S^*} H^1(M, V^*(1))^* \longrightarrow \mathbb{Q}_p.$$

Then $\phi(loc_S(H^1(M, V))) = 0$, and Artin reciprocity can be (essentially) deduced from this statement applied to $V = \mathbb{Q}_p(1)$ for various p.

A well-known case is when $X = E$, an elliptic curve, and $F = \mathbb{Q}$.

Then $V = T_p(E) \otimes \mathbb{Q}_p$, and get an element $c \in H^1(M, V)$ via the method of Euler systems.

The function

$$H^1(\partial M, V) \simeq H^1(\partial M, V^*(1))^* \xrightarrow{loc_S^*} H^1(M, V^*(1))^* \longrightarrow \mathbb{Q}_p.$$

is non-zero iff $L(E, 1) \neq 0$, which implies the finiteness of $X(\mathbb{Q})$ in that case.

Arithmetic principal bundles and reciprocity laws

A natural extension is $A = U(\bar{X}, b)$, the $\mathbb{Q}_p$-pro-unipotent fundamental group of a smooth variety X.

Then we have a diagram

$$\begin{tikzcd}
X(M) \arrow[r] \arrow[d, "j"'] & X(\partial M) \arrow[d, "j_\partial"'] \\
H^1(M, U) \arrow[r, "loc_S"] & H^1(\partial M, U)
\end{tikzcd}$$

where the vertical map sends a point a to the homotopy classes of paths

$$U(\bar{X}; b, a).$$

In this case, finding one equation ϕ vanishing on the image of loc_S has consequences for the Diophantine geometry of X, because $\phi \circ j_\partial$ is a locally-analytic function on $X(\partial M)$ vanishing on $X(M)$.

Arithmetic principal bundles and reciprocity laws

When X is a hyperbolic curve, we get a tower of diagrams

$$\begin{tikzcd}
X(M) \arrow[r] \arrow[d, "j"'] & X(\partial M) \arrow[d, "j_\partial"'] \\
H^1(M, U_n) \arrow[r, "loc_S"] & H^1(\partial M, U_n)
\end{tikzcd}$$

indexed by n, inducing subsets

$$X(\partial M)_n := j_\partial^{-1}(loc_S(H^1(M, U_n))$$

and a filtration

$$X(\partial M) = X(\partial M)_1 \supset X(\partial M)_2 \supset X(\partial M)_3 \supset X(\partial M)_4 \supset \cdots$$

coming from an iterative description of $loc_S(H^1(M, U_n))$.

Arithmetic principal bundles: Speculation

Main objects of interest are intersections:

$$loc_S[H^1(M, A)] \cap H^1_f(\partial M, A).$$

Quite close to a Lagrangian intersection inside $H^1(\partial M, A)$.

Can also replace by the Lagrangian intersection

$$loc_S[H^1(M, T^*A(1))] \cap H^1_f(\partial M, T^*A(1))$$

inside

$$H^1(\partial M, T^*A(1)) = H^1(\partial M, A \ltimes (LieA)^*(1)).$$

Following three-manifold topology, we might believe such intersections to be closely related to Chern-Simons theory on $\bar{M} = \mathrm{Spec}(\mathcal{O}_F)$, or on arithmetic moduli spaces of bundles on $\bar{M}$. This is, roughly, the subject of the Atiyah-Floer conjecture.

Arithmetic principal bundles: Chern-Simons functionals

Assume F imaginary. Have Chern-Simons functional on

$$H^1(\bar{M}, A)$$

for finite A. (Or p-adic A, which we will not discuss here.)

Choose $c \in H^3(A, \mathbb{Z}/n)$.

Then

$$\mathbb{CS}_c : \rho \mapsto \mathrm{Inv}(\rho^*(c)) \in \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

where

$$\mathrm{Inv} : H^3(\bar{M}, \mathbb{Z}/n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

(Depends also on trivialisation $\mathbb{Z}/n \simeq \mu_n$.)

Arithmetic principal bundles: Chern-Simons functionals

Simple case: $A = \mathbb{Z}/n$.

$Id : A \simeq \mathbb{Z}/n$ gives a class $\alpha \in H^1(A, \mathbb{Z}/n)$.

The boundary map of the exact sequence

$$0 \longrightarrow \mathbb{Z}/n \longrightarrow \mathbb{Z}/n^2 \longrightarrow \mathbb{Z}/n \longrightarrow 0$$

gives a class $\delta(\alpha) \in H^2(A, \mathbb{Z}/n)$.

Thus, we have a natural class

$$c := \alpha \cup \delta\alpha \in H^3(A, \mathbb{Z}/n).$$

so that

$$\mathbb{CS}_c(\rho) = \mathrm{Inv}(\rho^*(\alpha) \cup \delta(\rho^*(\alpha))).$$

Arithmetic principal bundles: Chern-Simons functionals

Example: [w/ Heejoong Chung, Dohyeong Kim, Jeehoon Park, and Hwajong Yoo]

Let $n = 2$, $p \equiv 1 \mod 4$ prime, and t a square-free integer such that $\left(\frac{t}{p}\right) = -1$.

For $F = \mathbb{Q}(\sqrt{-pt})$, $F(\sqrt{p})$ is unramified over F, and corresponds to a $\rho \in H^1(\mathrm{Spec}(\mathcal{O}_F), \mathbb{Z}/2)$.

In this case,

$$\mathbb{CS}_c(\rho) = 1/2.$$

Arithmetic principal bundles: Chern-Simons functionals

These computations are done using a 'glueing formula':

–There is a $\mathbb{Q}_p$-torsor $\mathcal{T}$ on $H^1(\partial M, A)$ consisting of trivialisations of the cocycle $(\rho|\partial M)^*(c) \in Z^3(\partial M, A)$.

– The two 'manifolds with boundary' $M^+ = M$ and $M^- := \prod_{v\in S} \mathrm{Spec}(\mathcal{O}_{F,v})$ define sections

$$\mathbb{CS}_c^+(\rho), \mathbb{CS}_c^-(\rho) \in \mathcal{T}_{(\rho|\partial M)}$$

via trivialisations over M^+ and M^-.

–The difference between the two is $\mathbb{CS}_c(\rho) \in \mathbb{Q}_p$.

–Need to compute the trivialisations explicitly to compute this difference.

Arithmetic principal bundles: Chern-Simons functionals

Can define also the mod n Chern-Simons invariant

$$Z_c(\bar{M}, A) := \sum_{\rho \in H^1(\bar{M}, A)} \exp(2\pi i \mathbb{CS}_c(\rho)).$$

Can define p-adic Chern-Simons functionals in suitable circumstances. However, difficult to define a p-adic Chern-Simons invariant of $\bar{M}$.

'Computing' the Chern-Simons functionals

Recall the perfect pairing

$$\langle \cdot , \cdot \rangle : H^1(\bar{M}, \mathbb{Z}/n) \times \mathrm{Ext}^2_{\bar{M}}(\mathbb{Z}/n, \mathbb{G}_m) \longrightarrow H^3(\bar{M}, \mathbb{Z}/n) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

Thus, for every ideal class I, there is a mod n class

$$[I]_n \in \mathrm{Ext}^2_{\bar{M}}(\mathbb{Z}/n, \mathbb{G}_m).$$

There is also the cup product

$$H^1(\bar{M}, \mathbb{Z}/n) \times H^2(\bar{M}, \mathbb{Z}/n) \longrightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

which induces a map

$$H^2(\bar{M}, \mathbb{Z}/n) \longrightarrow \mathrm{Ext}^2_{\bar{M}}(\mathbb{Z}/n, \mathbb{G}_m).$$

'Computing' the Chern-Simons functionals

Define the operator

$$d : H^1(\bar{M}, \mathbb{Z}/n) \xrightarrow{\delta} H^2(\bar{M}, \mathbb{Z}/n) \longrightarrow \mathrm{Ext}^2_{\bar{M}}(\mathbb{Z}/n, \mathbb{G}_m).$$

to be the composition.

We can use this to define a pairing on $H^1(\bar{M}, \mathbb{Z}/n)$,

$$(\rho_1, \rho_2) := \langle \rho_1, d\rho_2 \rangle.$$

Thus, $\mathbb{CS}_c(\rho) = (\rho, \rho)$.

Assume $\mu_{n^2} \subset F$.

Lemma

$$(\rho_1, \rho_2) = (\rho_2, \rho_1)$$

'Computing' the Chern-Simons functionals

Define an ideal to be *n-homologically trivial* if

$$[I]_n \in Im(d) \subset \mathrm{Ext}^2_{\bar{M}}(\mathbb{Z}/n, \mathbb{G}_m).$$

We can define a mod n height pairing on n-homologically trivial ideals:

$$ht_n(I, J) := \langle d^{-1}[I]_n, [J]_n \rangle = (d^{-1}[I]_n, d^{-1}[J]_n).$$

Lemma

This pairing is well-defined.

'Computing' the Chern-Simons functionals

Now we take $n = p$ prime, $K := \mathrm{Ker}(d)$, $a = \dim H^1(X, \mathbb{Z}/p)$, $b = \dim K$. Denote by $\bar{d}$ the induced isomorphism

$$\bar{d} : H^1(X, \mathbb{Z}/p)/K \simeq Im(d).$$

Proposition

Let $\{\xi_j\}$ be a finite set of homologically trivial ideals. Then

$$\sum_{\rho \in H^1(X,\ \mathbb{Z}/p)} \exp[2\pi i((\rho,\rho) + \sum_j \langle \rho, [\xi_j]_p \rangle)]$$

$$= p^{(a+b)/2} \left(\frac{\det(\bar{d})}{p} \right) i^{[\frac{(a-b)(p-1)^2}{4}]} \exp[-2\pi i(\frac{1}{4} \sum_{i,\ j} ht_p(\xi_i, \xi_j))]$$