

Fundamental groups and Diophantine geometry



X : compact Riemann surface of genus $g \geq 2$.

J_X : Jacobian of X .

$$\begin{aligned} J_X &= H_1(X, \mathbb{Z}) \setminus H^0(\Omega_X)^* \\ &= H_1(X, \mathbb{Z}) \setminus H_1(X, \mathbb{C}) / F^0 \end{aligned}$$

Recall that the cohomology of X , $H^1(X, \mathbb{C})$ has two step *Hodge filtration*

$$H^1(X, \mathbb{C}) \supset F^1 H^1(X, \mathbb{C}) = H^0(X, \Omega_X)$$

$H_1(X, \mathbb{C})$ has a dual filtration, such that

$$F^0 H_1 = (F^1 H^1)^\perp.$$

In particular,

$$H^0(X, \Omega_X)^* \simeq H_1(X, \mathbb{C})/F^0.$$

J_X is a *linearization/abelianization* of X .

Other interpretations:

$$J_X = \mathbb{Z}[X]_0 / (\text{rational equivalence})$$

$$J_X \sim \text{Sym}^g(X)$$

X itself embeds into J_X . For this we need to choose a basepoint $b \in X$. Then there is an embedding

$$i_b : X \hookrightarrow J_X$$

The *Albanese map* .

Interpretation

$$x \mapsto [\alpha \mapsto \int_b^x \alpha]$$

$$(J_X = H_1(X, \mathbb{Z}) \setminus H^0(\Omega_X)^*)$$

$$x \mapsto [x] - [b]$$

$$(J_X = \mathbb{Z}[X]_0 / (\text{rational equivalence}))$$

Third interpretation:

$$H_1(X, \mathbb{Z}) \backslash H_1(X, \mathbb{C}) / F^0$$

classifies extensions:

$$E : 0 \rightarrow H_1(X) \rightarrow E \rightarrow \mathbb{Z} \rightarrow 0$$

Each point x determines

$$E(x) : 0 \rightarrow H^1(X)(1) \rightarrow H^1(X \setminus \{b, x\})(1) \rightarrow \mathbb{Z} \rightarrow 0$$

$(H^1(X)(1) \simeq H_1(X))$

and

$$i_b(x) = [E(x)]$$

Note: Such extensions equivalent to *torsors* for $H_1(X)$.

Weil: algebraic construction of J_X .

If X is a smooth projective algebraic curve defined over \mathbb{Q} , J becomes a smooth projective variety also defined over \mathbb{Q} .

If $b \in X(\mathbb{Q})$ is a rational point, then i_b is an algebraic map defined over \mathbb{Q} .

Consequence (Weil's main motivation):

$$X(\mathbb{Q}) \hookrightarrow J_X(\mathbb{Q})$$

Latter set is an abelian group, making it easier to study.

Weil was interested in:

Finiteness of $X(\mathbb{Q})$.

Obviously,

$$J_X(\mathbb{Q}) \text{ finite} \Rightarrow X(\mathbb{Q}) \text{ finite}$$

But, unfortunately, $J_X(\mathbb{Q})$ not finite in general.

For example, take E to be the projective curve of genus 1 with affine model

$$x^3 + y^3 = 1729$$

Then $E(\mathbb{Q})$ is infinite. Can construct

$$X \rightarrow E$$

ramified cover of genus ≥ 2 . There is a finite-to-one map $E(\mathbb{Q}) \rightarrow J_X(\mathbb{Q})$.

J_X is a group, making it easier to study than X , but this same fact gives it many rational points. (Can add points to get new points.)

This is the *only* reason for the infinitude of $J_X(\mathbb{Q})$, i.e.,

$J_X(\mathbb{Q})$ is finitely generated.

Gives rise to ideas like:

$\Gamma \subset J_X$ finitely generated $\Rightarrow X \cap \Gamma$ finite?

(Lang 60's.)

Never quite worked in the right way. Rather, deduced from Faltings' theorem. Nevertheless, inspired much interesting research. (Mordell-Lang conjecture.)

Idea:

$$X(\mathbb{Q}) \subset \Gamma \subset J_X$$

Γ a more manageable object than $X(\mathbb{Q})$. Try to prove *analytically* that

$$X(\mathbb{C}) \cap \Gamma$$

is finite.

What does one gain from J_X ? (Quite a lot.)

- $X(\mathbb{Q})$ is quite sparse compared to genus 0 and 1. (Mumford)

-Can sometimes construct a quotient

$$J_X \rightarrow A$$

such that $X \rightarrow A$ is finite-to-one and $A(\mathbb{Q})$ is finite. (Mazur's work on $X_0(N)$.)

-If

$$\text{rank } J_X(\mathbb{Q}) < g$$

get finiteness of $X(\mathbb{Q})$. (Chabauty)

Chabauty's method:

$$\begin{array}{ccccc}
 X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) & & \\
 \downarrow & & \downarrow & \searrow & \\
 J_X(\mathbb{Q}) & \hookrightarrow & J_X(\mathbb{Q}_p) & \xrightarrow{\log} & T_e J_X(\mathbb{Q}_p) \\
 & & & & \downarrow \alpha \\
 & & & & \mathbb{Q}_p
 \end{array}$$

α : linear function on the g -dimensional \mathbb{Q}_p -vector space $T_e J_X$ such that $\alpha \circ \log$ vanishes on $J_X(\mathbb{Q})$.

So $f_\alpha := \alpha \circ \log|_{X(\mathbb{Q}_p)}$ vanishes on $X(\mathbb{Q})$.

Note: $T_e J_X(\mathbb{Q}_p) = H_1^{DR}(X_{\mathbb{Q}_p})/F^0$

But we can calculate f_α differently.

α is a differential form on X and

$$X(\mathbb{Q}_p) = \cup_i D_i,$$

a union of residue disks. Then

$$f_\alpha|_{D_i} = f_i(z_i),$$

where $f_i(z_i)$ is an integral of $\alpha|_{D_i} = a_i dz_i$. That is

$$f_\alpha(z) = \int_b^z \alpha.$$

Such a $f_i(z_i)$ has only finitely many zeros.

Nevertheless, a study of J_X by itself does not seem to yield a general finiteness theorem for $X(\mathbb{Q})$.

In fact, Faltings' eventual proof did not use the Mordell-Weil theorem.

Recall: J_X parametrizes degree zero line bundles on X .

It is *homological* in nature.

Weil pointed this out in the 30's in the first paper concerning vector bundles on curves. Spoke of necessity of non-abelian constructions, related to vector bundles on the one hand, and homotopy theory on the other.

Predicted applications to arithmetic.

Plausible that he had $X(\mathbb{Q})$ in mind.

Grothendieck (60's): arithmetic theory of the fundamental group, unifying usual π_1 with Galois theory.

Definition of arithmetic π_1 uses the category $Cov(X)$ of étale maps $Y \rightarrow X$.

The point b determines a functor

$$F_b : Cov(X) \rightarrow \text{Finite Sets}$$

$$\begin{array}{ccc} Y & & Y_b \\ \downarrow & \mapsto & \downarrow \\ X & & b \end{array}$$

and

$$\hat{\pi}_1(X, b) := Aut(F_b)$$

An element $g \in \hat{\pi}_1(X, b)$ consists of a collection

$$\{g_Y\}$$

indexed by objects $Y \rightarrow X$ in $Cov(X)$ where

$$g_Y \in \text{Aut}(Y_b)$$

and whenever we have a map of the category

$$\begin{array}{ccc} Y & \rightarrow & Y' \\ \downarrow & & \downarrow \\ X & = & X \end{array}$$

The following diagram commutes:

$$\begin{array}{ccc} Y_b & \xrightarrow{g_Y} & Y_b \\ \downarrow & & \downarrow \\ Y'_b & \xrightarrow{g_{Y'}} & Y'_b \end{array}$$

When applied to a complex variety X , get the pro-finite completion of usual $\pi_1(X, b)$.

Can also recover the Galois group of a field using same definition.

Many applications, e.g., Deligne's proof of Riemann hypothesis.

But usage is indirect, in that the arithmetic of X is controlled by $\hat{\pi}_1$ of some other variety (a parameter space).

Contrast with the usage of $H_1(X)$ for study of X .

In 80's Grothendieck proposed direct relations.

Starting from the arrow

$$f : X \rightarrow \text{Spec}(\mathbb{Q})$$

get a fiber

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

and from that an exact sequence of fundamental groups:

$$0 \rightarrow \hat{\pi}_1(\bar{X}, b) \rightarrow \hat{\pi}_1(X, b) \xrightarrow{f_*} \Gamma \rightarrow 0$$

$$(\Gamma = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}))$$

A point $x \in X(\mathbb{Q})$ is interpreted as a section of the map f :

$$x : \text{Spec}(\mathbb{Q}) \rightarrow X$$

Hence, gives rise to a splitting

$$x_* : \Gamma \rightarrow \hat{\pi}_1(X, b)$$

(up to conjugacy) of the exact sequence.

The *Section Conjecture* says that this is a bijection:

$$X(\mathbb{Q}) \simeq \text{splittings up to conjugacy}$$

Grothendieck's remark:

section conjecture $\stackrel{?}{\Rightarrow}$ Faltings' theorem

Brief comments on map

$$X(\mathbb{Q}) \rightarrow \text{splittings}$$

In our set-up, there is already one splitting b_* coming from the point b . Gives rise to an action of Γ on $\hat{\pi}_1(\bar{X}, b)$.

Any other splitting $s : \Gamma \rightarrow \hat{\pi}_1(X, b)$ is related to b_* by a map c_s from Γ to $\hat{\pi}_1(\bar{X}, b)$:

$$s(\gamma) = b_*(\gamma)c_s(\gamma)$$

c_s defines a class in $H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$ and every class arises in this way.

So we want

$$X(\mathbb{Q}) \simeq H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

Key issue is surjectivity.

Interesting to compare with genus 1 situation.

E elliptic curve, endowed with origin $o \in E$.

Still have

$$0 \rightarrow \hat{\pi}_1(\bar{E}, o) \rightarrow \hat{\pi}_1(E, o) \rightarrow \Gamma \rightarrow 0$$

and map

$$E(\mathbb{Q}) \rightarrow H^1(\Gamma, \hat{\pi}_1(\bar{E}, o)).$$

But here,

$$\hat{\pi}_1(\bar{E}, o) = H_1(\bar{E}, \hat{\mathbb{Z}})$$

and the image lies inside

$$H_g^1(\Gamma, H_1(\bar{E}, \hat{\mathbb{Z}})) \subset H^1(\Gamma, H_1(\bar{E}, \hat{\mathbb{Z}}))$$

defined by local 'Selmer' conditions.

The analogue of the section conjecture in this case is

$$E(\mathbb{Q}) \otimes \hat{\mathbb{Z}} \simeq H_g^1(\Gamma, H_1(\bar{E}, \hat{\mathbb{Z}}))$$

which is part of the conjecture of Birch and Swinnerton-Dyer: finiteness of the Shafarevich-Tate group.

Another (important) remark on map:

Point $x \in X(\mathbb{Q})$ actually determines the set of *étale paths* from b to x .

$$\hat{\pi}_1(\bar{X}; x, b) := \text{Isom}(F_b, F_x)$$

This is a *torsor* for $\hat{\pi}_1(\bar{X}, b)$, via the composition of paths action:

$$(p, \gamma) \in \hat{\pi}_1(\bar{X}; x, b) \times \hat{\pi}_1(\bar{X}, b) \mapsto p \circ \gamma$$

Carries a compatible action of Γ .

Action of $\gamma \in \Gamma$ on $g = \{g_Y\}$ in $\hat{\pi}_1(\bar{X}; x, b)$.

Recall: g consists of compatible bijections

$$g_Y : Y_b \rightarrow Y_x$$

for each covering

$$Y \rightarrow X$$

Such a covering can be conjugated with γ to

$$\gamma(Y) \rightarrow X$$

$\gamma(g)$:

$$\begin{array}{ccc} Y_b & \xrightarrow{\gamma(g)_Y} & Y_x \\ \simeq \downarrow & & \uparrow \simeq \\ \gamma(Y)_b & \xrightarrow{g_{\gamma(Y)}} & \gamma(Y)_x \end{array}$$

Such torsors for $\hat{\pi}_1(\bar{X}, b)$ are classified by

$$H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

That is, the map $X(\mathbb{Q}) \rightarrow H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$ simply sends x to the class

$$[\hat{\pi}_1(\bar{X}; x, b)] \in H^1(\Gamma, \hat{\pi}_1(\bar{X}, b))$$

Suggests important role of path spaces.

Relation between $\hat{\pi}_1$ and Diophantine geometry still unclear.

However,

$$\pi_1^M$$

the *motivic* fundamental group, appears to be directly related to Diophantine geometry.

π_1^M has many components.

One component, the De Rham fundamental group of $X_{\mathbb{Q}_p}$, uses the category

$$\text{Un}(X_{\mathbb{Q}_p})$$

of unipotent vector bundles with flat connection.

That is, the objects are (\mathcal{V}, ∇) , vector bundles \mathcal{V} on $X_{\mathbb{Q}_p}$ equipped with flat connections

$$\nabla : \mathcal{V} \rightarrow \Omega_{X/S} \otimes \mathcal{V}$$

that admit a filtration

$$\mathcal{V} = \mathcal{V}_n \supset \mathcal{V}_{n-1} \supset \cdots \supset \mathcal{V}_1 \supset \mathcal{V}_0 = 0$$

by sub-bundles stabilized by the connection, such that

$$(\mathcal{V}_{i+1}/\mathcal{V}_i, \nabla) \simeq (\mathcal{O}_{X_{\mathbb{Q}_p}}^r, d)$$

Associated to $b \in X$ get

$$e_b : \mathrm{Un}(X_{\mathbb{Q}_p}) \rightarrow \mathrm{Vect}_{\mathbb{Q}_p}$$

The *De Rham fundamental group*

$$U^{DR} := \pi_{1,DR}(X_{\mathbb{Q}_p}, b)$$

is the pro-unipotent pro-algebraic group that represents

$$\mathrm{Aut}^{\otimes}(e_b)$$

(Tannaka dual)

and the path space

$$P^{DR}(x) := \pi_{1,DR}(X; x, b)$$

represents

$$\mathrm{Isom}^{\otimes}(e_b, e_x)$$

The pro-unipotent p-adic étale fundamental group

$$U^{et}$$

and étale path spaces

$$P^{et}(x)$$

defined in the same way using the category of unipotent \mathbb{Q}_p local systems.

When equipped with suitable structures, these path spaces carry serious applications to Diophantine geometry.

Structures:

$P^{DR}(x)$ carries a Hodge filtration and crystalline Frobenius endomorphism.

$P^{et}(x)$ carries a Γ action. Can restrict to an action of $G_p := \text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Can study *variation* of these structures with x and try to cull out the global points.

Fundamental diagram (non-abelian method of Chabauty):

$$\begin{array}{ccccc}
 X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) & & \\
 \downarrow & & \downarrow & \searrow & \\
 H_g^1(\Gamma, U^{et}) & \rightarrow & H_g^1(G_p, U^{et}) & \xrightarrow{D} & U^{DR}/F^0 \\
 & & & & \downarrow \alpha \\
 & & & & \mathbb{Q}_p
 \end{array}$$

$H_g^1(\cdot, U^{et})$: classifying space for U^{et} -torsors.

U^{DR}/F^0 : classifying space for U^{DR} -torsors.

Vertical arrows: $x \mapsto [P^{et}(x)]$

Southeast arrow: $x \mapsto [P^{DR}(x)]$

D : map associating to a U^{et} -torsor a U^{DR} -torsor using non-abelian p-adic Hodge theory.

Actually, a compatible tower:

$$\begin{array}{ccc}
 \parallel & & \downarrow \\
 X(\mathbb{Q}_p) & \rightarrow & U_{n+1}^{DR}/F^0 \\
 \parallel & & \downarrow \\
 X(\mathbb{Q}_p) & \rightarrow & U_n^{DR}/F^0 \\
 \parallel & & \downarrow \\
 \vdots & \vdots & \vdots \\
 \parallel & & \downarrow \\
 X(\mathbb{Q}_p) & \rightarrow & U_2^{DR}/F^0
 \end{array}$$

$$Z^1 = U, \quad Z^{n+1} = [U, Z^n], \quad U_n = Z^n \setminus U.$$

$$U_2^{DR} = H_1^{DR}(X_p) := (H_{DR}^1(X_p))^*.$$

j_2^{DR} : log of the usual Albanese map with respect to the basepoint b .

Fundamental diagram (finite level):

$$\begin{array}{ccccc}
 X(\mathbb{Q}) & \hookrightarrow & X(\mathbb{Q}_p) & & \\
 \downarrow & & \downarrow & \searrow & \\
 H_g^1(\Gamma, U_n^{et}) & \rightarrow & H_g^1(G_p, U_n^{et}) & \xrightarrow{D} & U_n^{DR}/F^0 \\
 & & & & \downarrow \alpha \\
 & & & & \mathbb{Q}_p
 \end{array}$$

Underlying concept:

Motivic unipotent Albanese map

$$X \rightarrow \mathcal{C}^M$$

$$x \mapsto [P^M(x)]$$

\mathcal{C}^M : classifying space for $\pi_1^M(X, b)$ -torsors.

Conjecture: For some n

$$\dim H_g^1(\Gamma, U_n^{et}) < \dim U_n^{DR}/F_0$$

Conjecture implies Faltings theorem, via existence of algebraic function α that vanish on the image of $X(\mathbb{Q})$.

$$\alpha \circ D|X(\mathbb{Q}_p)$$

is expressed using *p-adic iterated integrals*.

Key point is that inside U_n^{DR}/F^0 ,

$$\text{Im}(X(\mathbb{Q})) \subset \text{Im}(H_g(\Gamma, U_n^{et}))$$

and

$$\text{Im}(H_g^1(\Gamma, U_n^{et})) \cap \text{Im}(X(\mathbb{Q}_p))$$

is finite, assuming conjecture.

Reminiscent of Lang's strategy.

Conjecture is implied by (a part of) the Bloch-Kato conjectures (generalization of Birch and Swinnerton-dyer):

$$K_{2r-n-1}^{(r)}(X^n) \otimes \hat{\mathbb{Z}} \simeq H_g^1(\Gamma, H^n(\bar{X}^n, \hat{\mathbb{Z}}(r)))$$

This should be viewed as a ‘linearized section conjecture.’

That is:

‘linearized section conjecture’

⇒ Faltings’ theorem.

At present, can prove conjecture only in certain affine analogues.

$$\mathbf{P}^1 \setminus \{0, 1, \infty\}$$

(involves multiple p-adic polylogarithms) and rank one CM elliptic curves minus the origin (elliptic polylogarithm).

Get cases of Siegel's theorem.

Regardless of the precise status, seems to confirm the insight of Weil, Grothendieck, and Lang.