Fundamental groups, polylogarithms, and Diophantine geometry

X: smooth variety over $\mathbb{Q}$. So X defined by equations with rational coefficients.

$$\begin{array}{ccccc} & & \text{Arithmetic of } X & & \\ & \nearrow & & \nwarrow & \\ \text{Topology} & & & & \text{Geometry} \end{array}$$

Serious aspects of the input from topology have been *homological* in nature.

-Machinery of homological algebra.

-(co-)homology theories of arithmetic nature.

These days, immediately associate to X at least four different cohomology groups:

-$H^i(X(\mathbb{C}), \mathbb{Q})$: Singular cohomology of topological space given by the complex points of X.

-$H^i(\bar{X}, \mathbb{Q}_p)$: Étale cohomology with p-adic coefficients.

-$H^i_{DR}(X) = H^i(X, \Omega^\bullet_X)$: The algebraic De Rham cohomology of X.

-$H^i_{cr}(X \bmod p, \mathbb{Q}_p)$: The crystalline cohomology of X mod p.

All have ‘formally similar’ linear structures. Also, ‘compatible’ in many ways, e.g.

$$H^i(\bar{X}, \mathbb{Q}_p) \simeq H^i(X(\mathbb{C}), \mathbb{Q}) \otimes \mathbb{Q}_p$$

Supposedly accounted for by a theory of ‘motives’:

$$\begin{array}{ccc} \text{Varieties} & \longrightarrow & \text{Motives} \\ & \searrow & \downarrow \\ & & \text{Vector Spaces} \end{array}$$

These homological invariants have an astounding array of deep applications. Recall, for example, that étale cohomology of a variety over a finite field has all the information about the number of points.

Even deeper applications for varieties over $\mathbb{Q}$.

$H^i(\bar{X}, \mathbb{Q}_p)$ carries a natural action of Gal$(\bar{\mathbb{Q}}/\mathbb{Q})$.

Applied in two ways:

Structure of of Gal$(\bar{\mathbb{Q}}/\mathbb{Q})$ $\leftrightarrow$ arithmetic structure of X.

For this talk, the most relevant direction is $\rightarrow$.

One kind of application: Certain X do not *exist* because they would give rise to impossible representations.

-The theorem of Wiles: Elliptic curves of the form $y^2 = x(x-a^p)(x+b^p)$ where $a^p+b^p=c^p$.

- A theorem of Fontaine: There are no abelian schemes over $\mathbb{Z}$.

Reminiscent of classical geometric impossibility theorems.

Profound applications to Diophantine problems (related to above): Study of $X(\mathbb{Q})$, the set of $\mathbb{Q}$-points of X. Main subject of today's lecture.

Remarkable ingredient of these applications: get X to *parametrize* other geometric objects.

$$\begin{array}{c} Z \\ \downarrow \\ X \end{array}$$

$$
\begin{array}{ccc}
x \in X(\mathbb{Q}) & \mapsto & Z_x \\
 & & \downarrow \\
 & & H^i(\bar{Z}_x, \mathbb{Q}_p)
\end{array}
$$

Non-existence of the representations $H^i(\bar{Z}_x, \mathbb{Q}_p)$ $\rightarrow$ emptiness (more or less) of $X(\mathbb{Q})$: Wiles via correspondence of Frey-Hellegouarche.

Finiteness of the representations $H^i(\bar{Z}_x, \mathbb{Q}_p) \rightarrow$ finiteness of $X(\mathbb{Q})$: Faltings via Kodaira-Parshin construction. Here, important input from the geometry of moduli spaces.

Older idea (Weil): get X to parametrize geometric objects *intrinsic* to X.

X smooth projective curve of genus ≥ 2. By fixing base point $x \in X$, get a family of line bundles parametrized by X.

$$y \in X \leftrightarrow \mathcal{O}(x - y)$$

Family of all line bundles of degree zero on X form a variety J, the Jacobian of X, and the above defines an embedding

$$j_1 : X \hookrightarrow J$$

the Abel-Jacobi map.

Weil tried to use this to prove that $X(\mathbb{Q})$ is finite (Mordell's conjecture). Would follow, for example, if $J(\mathbb{Q})$ were finite.

Unfortunately, only managed to prove that $J(\mathbb{Q})$ is finitely-generated.

Idea of Lang (60's): Try to prove a geometric statement.

$\Gamma \subset J$ *any* finitely generated abelian group. Then $X \cap \Gamma$ should be finite.

Only deduced as a *consequence* of Faltings' theorem.

A more recent philosophy: J is too linear an object to yield finiteness of $X(\mathbb{Q})$. (Note that the parametrization used by Faltings is not linear in any way.)

Related fact: J is constructed out of homology. Over $\mathbb{C}$:

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

There is also a homological interpretation of j_1.

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

is a classifying space for certain Hodge structures, namely, extensions of the trivial Hodge structure

$$\mathbb{Z}$$

by

$$H_1(X,\mathbb{Z}) = H^1(X,\mathbb{Z})(1).$$

The map j_1 sends the point y to the class of

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

Would like to 'lift' the construction of the Jacobian into an *intrinsic* non-linear parameter space.

$$H_1 = \pi_1/[\pi_1, \pi_1]$$

Try to apply *homotopy* to Diophantine geometry.

We propose to study a 'lift' of the Abel-Jacobi map that associates to a point $y \in X$, the set $\pi_1(X; x, y)$ suitably completed and enriched.

That is, study path spaces parametrized by X.

Try to prove finiteness of $X(\mathbb{Q})$ by proving finiteness of these path spaces (cf. occurrence of Galois representations in theorems of Faltings and Wiles).

The $\pi_1(X; x, y)$ are *torsors* for $\pi_1(X; x)$, sets equipped with a transitive free action of $\pi_1(X; x)$. This torsor structure will be compatible with all the extra structure to be discussed, e.g., Hodge structure, Galois action, 'crystalline structure',...

One source for this line of thought. Grothedieck's *section conjecture*: Postulates relation between the study of fundamental groups and Diophantine geometry for compact hyperbolic curves.

For general schemes Z and geometric point

$$z \hookrightarrow Z,$$

there is a notion of a pro-finite fundamental group

$$\pi_1^f(Z, z).$$

Depends only on a category $Cov(Z)$ of finite covering spaces of Z in an appropriate sense.

Consider functor F_z that associates to

$$\begin{array}{cc} & Y \\ & \downarrow \\ z \hookrightarrow & Z \end{array}$$

the fiber Y_z. Then

$$\pi_1^f(Z, z) = Aut(F_z)$$

The pro-finite fundamental group has many of the properties of the usual fundamental group, e.g., covariance for maps of pointed schemes.

Also when we view a scheme

$$\begin{array}{c} X \\ \downarrow \\ \text{Spec}(\mathbb{Q}) \end{array}$$

as a fiber bundle with base Spec($\mathbb{Q}$), then $\bar{X}$ is the fiber over the geometric point

$$\text{Spec}(\bar{\mathbb{Q}}) \rightarrow \text{Spec}(\mathbb{Q})$$

$$\begin{array}{ccc} \bar{X} & \hookrightarrow & X \\ \downarrow & & \downarrow \\ \text{Spec}(\bar{\mathbb{Q}}) & \hookrightarrow & \text{Spec}(\mathbb{Q}) \end{array}$$

and we get an exact sequence:

$$0 \to \pi_1^f(\bar{X}) \to \pi_1^f(X) \to \pi_1^f(\mathrm{Spec}(\mathbb{Q})) \to 0$$

The last fundamental group can be canonically identified with $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

A point $\mathrm{Spec}(\mathbb{Q}) \to X$ gives rise to a splitting

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \pi_1^f(X)$$

of the exact sequence.

The section conjecture says *all* splittings can be obtained this way.

In short, splitting are hard to construct. Only way is via (arithmetic-)geometry.

Compares with various ideas about representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Also very hard to construct. Given a few natural constraints, they should all come from geometry: Conjecture of Fontaine and Mazur.

Section conjecture belongs to a vast program of ‘anabelian geometry’. Contributions by Pop, Nakamura, Tamagawa, Mochizuki,...

Sample classical theorem (Neukirch and Uchida): F and K number fields Then there is a bijection

$$Isom(F, K)$$

$$\simeq Isom(\mathrm{Gal}(\bar{F}/F), \mathrm{Gal}(\bar{K}/K))/\text{conjugation}$$

For example, for $F = K = \mathbb{Q}$, all automorphisms of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ are inner.

However, section conjecture appears to be very difficult. No progress!

Nevertheless, inspiring in that it suggests a direct link between Diophantine problems and the study of the fundamental group.

A non-conjectural link comes from the theory of the *motivic* fundamental group (Deligne).

Origins in the theory of $\mathbb{C}$-unipotent completions of fundamental groups of topological spaces.

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

Universal pro-unipotent algebraic group over $\mathbb{C}$ to which π maps. Very close to homology and rational homotopy theory. Pro-algebraic group which is a topological invariant of $X(\mathbb{C})$. However, carries extra structure reflecting the geometry of $X(\mathbb{C})$.

One construction: Consider the completed group algebra

$$\mathbb{C}[[\pi_1]] = \varprojlim \mathbb{C}[\pi_1]/I^n$$

where $I \subset \mathbb{C}[\pi_1]$ is the augmentation ideal. $\mathbb{C}[[\pi_1]]$ actually has the structure of a Hopf algebra with comultiplication

$$\Delta : \mathbb{C}[[\pi_1]] \rightarrow \mathbb{C}[[\pi_1]] \otimes \mathbb{C}[[\pi_1]]$$

induced naturally by the map that takes an element $g \in \pi_1$ to $g \otimes g$. Then π_1^{DR} consists of the group-like elements in $\mathbb{C}[[\pi_1]]$, i.e., all γ such that $\Delta(\gamma) = \gamma \otimes \gamma$.

From the point of view of π_1^{DR}, we have

$$\mathbb{C}[[\pi_1]] = U(Lie(\pi_1^{DR}))$$

Can also carry out this construction for path spaces to get $\pi_1^{DR}(X;x,y)$, an algebraic variety over $\mathbb{C}$.

Key point is that the spaces $\pi_1^{DR}(X;x,y)$ carry Hodge structures in appropriate sense.

$\mathbb{C}[[\pi_1(X;x,y)]]$ has natural Hodge filtration $F^{\cdot}$:

$$\mathbb{C}[[\pi_1(X;x,y)]] = F^0 \supset F^1 \supset F^2 \cdots$$

which, in turn, gives rise to a Hodge filtration of $\pi_1^{DR}(X;x,y)$ by subvarieties (subgroups when $x = y$)

$$F^0 \subset F^{-1} \subset F^{-2} \subset \cdots .$$

Also has an integral lattice $L \subset \pi_1^{DR}(X;x,y)$ given by the image of the usual topological paths.

Can classify these triples

$$(\pi_1^{DR}(X;,x,y),F^{\cdot},L)$$

and observe how they vary with y.

Classifying space:

$$UAlb := L\backslash\pi_1^{DR}(X,x)/F^0$$

Also have unipotent Albanese map

$$j : X \to UAlb$$

$$y \mapsto [(\pi_1^{DR}(X;,x,y),F^{\cdot},L)]$$

Example: $X = \mathbf{P}^1 - \{0, 1, \infty\}$.

Then $\mathbb{C}[[\pi_1]] = \mathbb{C}[[A, B]]$, the non-commutative power-series in two variables. For each words w in A, B, have an element of the continuous dual α_w such that $\alpha_w(w) = 1$ and $\alpha_w(v) = 0$ for all other words v. Also, $F^0 = 0$. Have map

$$j : X \rightarrow L \backslash \pi_1^{DR}(X)$$

or a multi-valued map $X \rightarrow \pi_1^{DR}(X)$. Can compute $\alpha_w \circ j$ explicitly.

For w of the form

$$w = A^{k_1-1}BA^{k_2-1}B \cdots BA^{k_m-1}B,$$

($k_1 > 1$) we have

$P_w := \alpha_w \circ j = \Sigma_{n_1>n_2>\cdots>n_m} z^{n_1}/n_1^{k_1}n_2^{k_2}\cdots n_m^{k_m}$

a multiple polylogarithm. The multiple polylogarithms are coordinates of the unipotent Albanese map.

P_w have appear to have an astounding array of relations with arithmetic, geometry, representation theory, physics, etc.

Same formula define p-adic analytic functions on a disk in $X(\mathbb{Q}_p)$. p-adic multiple polylogarithms. Can extend naturally to all of $X(\mathbb{C}_p)$. (Theory of Coleman functions and integration.)

Theorem 1 *Fix a ring* $\mathbb{Z}[1/S]$ *of* S*-integers. There exists a non-trivial linear combination* $f = \Sigma_w c_w P_w$ *of* p*-adic multiple polylogarithms such that* $f = 0$ *on* $X(\mathbb{Z}[1/S])$.

Corollary 2 *(Theorem of Siegel)* $X(\mathbb{Z}[1/S])$ *is finite.*

Comes from an analogue of above discussion for $p-$adic Hodge theory.

Basic idea of proof is a diagram:

$$\begin{array}{ccc} X(\mathbb{Z}[1/S]) & \rightarrow & \pi_1^{DR}(X \otimes \mathbb{Q}_p, x) \\ \downarrow & & \uparrow \\ H^1_f(\Gamma_S, \pi_1^{et}(\bar{X}, x) \otimes \mathbb{Q}_p) & \rightarrow & H^1_f(G_p, \pi_1^{et}(\bar{X}, x) \otimes \mathbb{Q}_p) \end{array}$$

The left vertical map associates to a point y the space $\pi_1^{et}(\bar{X}; x, y) \otimes \mathbb{Q}_p$ of unipotent étale paths from x to y, which is a *global* object. The set

$$H^1_f(\Gamma_S, \pi_1^{et}(\bar{X}, x) \otimes \mathbb{Q}_p)$$

constructed from non-abelian Galois cohomology is a classifying space for such global objects and has the natural structure of a pro-algebraic variety. One uses Galois cohomology computations to show that the image of

$$H^1_f(\Gamma_S, \pi_1^{et}(\bar{X}, x) \otimes \mathbb{Q}_p) \rightarrow \pi_1(X, x) \otimes \mathbb{Q}_p$$

is 'small' and eventually, has finite intersection with the image of $X(\mathbb{Q}_p)$. In some sense, Lang's idea is realized.

Can carry out a similar construction for higher genus curves. However, cannot control Galois cohomology in the same way, so cannot control a priori image of

$$C : H^1_f(\Gamma_S, \pi_1^{et}(\bar{X}, x) \otimes \mathbb{Q}_p) \rightarrow \pi_1^{DR}(X \otimes \mathbb{Q}_p, x)/F^0$$

However, there is a conjecture of Jannsen from the theory of mixed motives:

For any smooth projective variety V,

$$H^2(\Gamma_S, H^n(\bar{V}, \mathbb{Q}_p(r))) = 0$$

for $r \geq n + 2$. Corresponds to the philosophy that 'there are no two extensions in the category of mixed motives.' Jannsen's conjecture is implied by Beilinson's conjecture on the bijectivity of the regulator map and a p-adic analogue.

On the other hand, Jannsen's conjecture implies that the image of C is small. This in turn implies Faltings' theorem.

Theory of mixed motives is related to Diophantine geometry via L-functions. Gives info about linearized Diophantine invariants, i.e, conjectures of Birch and Swinnerton-Dyer, Bloch, Beilinson,...

Faltings' theorem is a non-linear statement. Doesn't 'fit in' to the motivic philosophy.

But a link is provided via the (non-linear) theory of the fundamental group.

Realizes in a small way Grothendieck's intuition.