Introduction to the Langlands programme through Grothendieck's new geometry

Laurent Lafforgue

(Huawei Paris Research Center, Boulogne-Billancourt, France)

Domodossola, July 18-22, 2022

I. From arithmetic to algebra and geometry

II. From arithmetic geometry to algebraic topology

III. From arithmetic algebraic topology to harmonic analysis

I. From arithmetic to algebra and geometry

Basic definition of arithmetic:

Study of

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$$

endowed with their natural structures

$$\begin{cases} \bullet & \text{addition,} \\ \bullet & \text{multiplication,} \end{cases}$$

$$\Rightarrow \begin{cases} \bullet & \mathbb{Z} \text{ is a commutative ring,} \\ \bullet & \mathbb{Q} \text{ is the fraction field of } \mathbb{Z}, \end{cases}$$

- induced notion of prime number,
- order relation,
- induction principle which is

$$\begin{cases} \text{any subset of } \mathbb{N} \text{ which contains } 0 \\ \text{and is stable by the map } n \mapsto n+1 \\ \text{is equal to } \mathbb{N}. \end{cases}$$

$\mathbb{Z}$ in the context of commutative rings:

$\mathbb{Z}$ is an object of the category consisting in

$$\begin{cases} \text{objects} = \text{commutative rings}, \\ \text{morphisms} = \text{homomorphisms of commutative rings}, \\ \text{composition law} = \text{composition of maps}. \end{cases}$$

Reminder. – *A category $\mathcal{C}$ consists in*

- *a collection $\mathrm{Ob}(\mathcal{C})$ of objects,*
- *for any pair of objects X, Y, a set $\mathrm{Hom}(X, Y)$ whose elements are called "morphisms" or "arrows"*

$$X \xrightarrow{u} Y \quad \text{or} \quad u : X \longrightarrow Y \,,$$

- *for any triple of objects, a composition law*

$$\begin{cases} \mathrm{Hom}(X, Y) \times \mathrm{Hom}(Y, Z) \longrightarrow \mathrm{Hom}(X, Z) \,, \\ (X \xrightarrow{f} Y, Y \xrightarrow{g} Z) \longmapsto (X \xrightarrow{g \circ f} Z) \end{cases}$$

such that

- $h \circ (g \circ f) = (h \circ g) \circ f$ *for any* $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$,
- *any object X has a "identity morphism" $X \xrightarrow{\mathrm{id}_X} X$ verifying* $\mathrm{id}_X \circ f = f, \forall f : Y \to X$, *and* $g \circ \mathrm{id}_X = g, \forall g : X \to Y$.

A characterization of $\mathbb{Z}$ in the category of commutative rings:

$\mathbb{Z}$ is an "initial" object of the category of commutative rings.

Reminder. –

- An initial object [resp. terminal object] of a category $\mathcal{C}$ is an object $\emptyset$ [resp. 1] of $\mathcal{C}$ such that, for any object X of $\mathcal{C}$, there exists a unique morphism
$$\emptyset \longrightarrow X \qquad [\text{resp. } X \to 1]\,.$$
- If a category $\mathcal{C}$ has an initial object [resp. terminal object], it is unique up to unique "isomorphism".
- An isomorphism in a category $\mathcal{C}$ is a morphism
$$f : X \longrightarrow Y$$
such that there exists a (unique) reverse morphism
$$g = f^{-1} : Y \longrightarrow X$$
verifying $\quad g \circ f = \mathrm{id}_X \quad$ and $\quad f \circ g = \mathrm{id}_Y$.

Remark. – $(\mathbb{N}, 0, \bullet + 1)$ is an initial object of the category of sets N endowed with an element $0 \in N$ and a map $S : N \to N$. This is the induction principle.

Commutative rings of finite presentation:

Definition. –

A commutative ring A is called "finitely presentable" if it can be defined by a finite family of generators and relations:

$$A \cong \mathbb{Z}[T_1, \cdots, T_k]/(P_1, \cdots, P_r)$$

$\Vert$ *ideal generated by r polynomials*

Lemma. –

Any commutative ring can be written as a filtering colimit of finitely presentable commutative rings.

Basic definition of algebraic number theory:

Study of

- finitely presentable commutative rings,
- the morphisms between such rings.

Remark. –

For any commutative ring A, a morphism

$$\mathbb{Z}[T_1, \cdots, T_k]/(P_1, \cdots, P_r) \longrightarrow A$$

is a family of elements

$$a_1, \cdots, a_k \in A$$

verifying the equations

$$\begin{cases} P_1(a_1, \cdots, a_k) = 0\,, \\ \qquad \cdots\cdots \\ P_r(a_1, \cdots, a_k) = 0\,. \end{cases}$$

A key remark relating arithmetic and geometry:

The category of commutative rings contains

- not only $\mathbb{Z}$ and finitely presentable $\mathbb{Z}[T_1, \cdots, T_k]/(P_1, \cdots, P_r)$,
- but also rings of the form

$$\mathbb{C}[T_1, \cdots, T_k]/(P_1, \cdots, P_r)$$

which can be understood as the
rings of polynomial functions on affine complex algebraic varieties

$$V \hookrightarrow \mathbb{C}^k$$

defined by polynomial equations

$$P_i(T_1, \cdots, T_k) = 0\,, \quad 1 \leq i \leq r\,.$$

Remark. –
A ($\mathbb{C}$-valued) point of such a variety is
a morphism $\mathbb{C}[T_1, \cdots, T_k]/(P_1, \cdots, P_r) \to \mathbb{C}$.

On the other hand:
A point of a set V can be seen as a map

$$\{\bullet\} \longrightarrow V\,.$$

Algebraic Gelfand duality:

Definition. – *The category of affine complex algebraic varieties is defined by*

- *objects* V_A = *commutative rings* A *endowed with a structure morphism*

  $$\mathbb{C} \longrightarrow A$$

  which makes A *"finitely presentable" over* $\mathbb{C}$,

- *morphisms of varieties* $V_A \longrightarrow V_B$ = *morphisms of commutative rings*

  $$B \longrightarrow A$$

  which respect the structure morphisms:

  $$\begin{array}{ccc} B & \longrightarrow & A \\ & \nwarrow \quad \nearrow & \\ & \mathbb{C} & \end{array}$$

Remark. – In particular

- $V_{\mathbb{C}}$ = point variety,
- points of a variety V_A are morphisms

$$V_{\mathbb{C}} \longrightarrow V_A .$$

The category of affine schemes:

Reminder. – *The "opposite" $\mathcal{C}^{\rm op}$ of a category $\mathcal{C}$ is defined as*

- $\mathrm{Ob}(\mathcal{C}^{\rm op}) = \mathrm{Ob}(\mathcal{C})$,
- *for any objects* X, Y,

$$\mathrm{Hom}_{\mathcal{C}^{\rm op}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$$

$$(X \xrightarrow{f^{\rm op}} Y) \leftarrow\!\shortmid (Y \xrightarrow{f} X)$$

- *for any morphisms* $(Z \xrightarrow{g} Y \xrightarrow{f} X)$ *of* $\mathcal{C}$,

$$(f \circ g)^{\rm op} = g^{\rm op} \circ f^{\rm op} .$$

Definition. – *The opposite of the category of commutative rings is the category* Aff *of "affine schemes".*

Any commutative ring A
corresponds by definition to an affine scheme $\mathrm{Spec}(A)$
which represents a "geometric way" to think about A.
$\mathrm{Spec}(\mathbb{Z})$ in particular
is the "geometric representation" of $\mathbb{Z}$.

Notions of points:

Points in a category:

Definition. – *If X, V are objects of a category $\mathcal{C}$, a V-valued point of X is a morphism of $\mathcal{C}$*

$$V \longrightarrow X .$$

The set of V-valued points of X can be denoted

$$X(V) = \mathrm{Hom}(V, X) .$$

Remarks. –

- Any morphism $X \to Y$ induces a map
$$X(V) \longrightarrow Y(V) .$$
- Any morphism $V' \to V$ induces a map
$$X(V) \longrightarrow X(V') .$$

Meaningful examples. – If $\mathcal{C}$ is a "geometric" category (ex: smooth manifolds, analytic varieties, algebraic varieties), an S-valued point of a geometric object X

$$S \longrightarrow X \quad \text{is a "}S\text{-parametrized" point.}$$

Determination of objects by their points:

Yoneda's lemma. –
Let $\mathcal{C}$ = *category,*

$\widehat{\mathcal{C}}$ = *category of "presheaves"*

$$P : \begin{cases} X \text{ object of } \mathcal{C} \longmapsto P(X) = \text{set}, \\ (X \xrightarrow{u} Y) \text{ morphism of } \mathcal{C} \longmapsto (P(Y) \xrightarrow{P(u)} P(X)) = \text{map}, \\ \text{such that} \\ P(v \circ u) = P(u) \circ P(v), \quad \forall\, u, v, \\ P(\mathrm{id}_X) = \mathrm{id}_{P(X)}, \quad \forall\, X\,, \end{cases}$$

y = *"Yoneda functor" defined by*

$$X \longmapsto y(X) \quad = \quad \text{presheaf of points of } X$$
$$\begin{cases} V \longmapsto y(X)(V) = X(V)\,, \\ (V' \to V) \longmapsto (X(V) \to X(V'))\,. \end{cases}$$

Then

$$y : \mathcal{C} \longrightarrow \widehat{\mathcal{C}}$$

is "fully faithful", meaning that for any X, Y = *objects of* $\mathcal{C}$

$$\mathrm{Hom}_{\mathcal{C}}(X, Y) \xrightarrow{\sim} \mathrm{Hom}_{\widehat{\mathcal{C}}}(y(X), y(Y))\,.$$

Corollary. –
In an arbitrary category $\mathcal{C}$,
any object X is determined
by the functor of its points

$$y(X) = \begin{cases} V \longmapsto X(V)\,, \\ (V' \to V) \longmapsto (X(V) \to X(V'))\,. \end{cases}$$

up to unique isomorphism of $\mathcal{C}$.

Definition. –
If $\mathcal{C}$ = category,
an object P of $\widehat{\mathcal{C}}$, i.e. a presheaf,
is called "representable"
if it is isomorphic to some $y(X)$, $X \in \mathrm{Ob}(\mathcal{C})$.

Consequence of Yoneda's lemma:
If P is "representable",
its "representing object" X in $\mathcal{C}$
is determined up to unique isomorphism of $\mathcal{C}$.

Categorical points of affine schemes:

- If $X = \mathrm{Spec}(A)$
  and $V = \mathrm{Spec}(B)$,
  a V-valued point of X is a ring homomorphism

$$A \longrightarrow B\,.$$

- In particular, if

$$A = \mathbb{Z}[T_1, \cdots, T_k]/(P_1, \cdots, P_r)\,,$$

  a V-valued point of X is a solution

$$(b_1, \cdots, b_k) \in B^k$$

  of the family of polynomial equations

$$P_i(b_1, \cdots, b_k) = 0\,, \quad 1 \leq i \leq r\,.$$

- Interpretation:
  In this context, “Yoneda’s lemma” yields
  some kind of duality between
  systems of equations and systems of solutions.

Algebraic and geometric points of affine schemes:

Definition. –
An algebraic point of an affine scheme $X = \mathrm{Spec}(A)$
is a categorical point

$$\mathrm{Spec}(K) \longrightarrow X = \mathrm{Spec}(A)$$

valued in a field K.

Definition. –
A geometric point of $X = \mathrm{Spec}(A)$ *is an algebraic point*

$$\mathrm{Spec}(\overline{K}) \longrightarrow X = \mathrm{Spec}(A)$$

valued in a field $\overline{K}$
which is algebraically closed.

Topological points of (affine) schemes:

- From schemes to toposes:

  - To any (affine) scheme X one associates its "Zariski topos"
  $$\widehat{O(X)}_{\mathrm{Zar}}.$$
  - To any morphism of (affine) schemes $X \xrightarrow{f} Y$, one associates a "morphism of toposes"
  $$\widehat{O(X)}_{\mathrm{Zar}} \longrightarrow \widehat{O(Y)}_{\mathrm{Zar}}.$$

- Points of toposes:

  - For any topos $\mathcal{E}$, one can define the category of its "points"
  $$\mathrm{pt}(\mathcal{E})\ .$$
  - Any morphism of toposes $\mathcal{E}' \longrightarrow \mathcal{E}$ defines a "functor" between categories of points
  $$\mathrm{pt}(\mathcal{E}') \longrightarrow \mathrm{pt}(\mathcal{E})\ .$$

Characterization of topological points of affine schemes:

Proposition. –

(i) *Let $X = \mathrm{Spec}(A)$ be an affine scheme.*
Then the category $\mathrm{pt}(X)$
of points of its Zariski topos is

$$\begin{cases} \text{objects} = \text{prime ideals } p \subset A, \\ \text{morphisms } (p \to q) = \text{inclusion relations } q \subseteq p. \end{cases}$$

(ii) *For any morphism of affine schemes*

$$X = \mathrm{Spec}(A) \longrightarrow Y = \mathrm{Spec}(B)$$

corresponding to a ring homomorphism

$$B \xrightarrow{u} A\,,$$

the associated functor

$$\mathrm{pt}(X) \longrightarrow \mathrm{pt}(Y)$$

is defined by

$$\begin{array}{ccc} p & \longmapsto & u^{-1}(p) \\ \| & & \| \\ \text{prime ideal of } A & & \text{prime ideal of } B. \end{array}$$

Algebraic and topological points:

- Any algebraic point of $X = \mathrm{Spec}(A)$

$$\mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(A)$$

  defines a topological point

$$p = \mathrm{Ker}(A \longrightarrow K)\,.$$

- Any topological point of $X = \mathrm{Spec}(A)$

$$p \subset A$$

  defines an algebraic point

$$\mathrm{Spec}(\kappa_p) \longrightarrow X = \mathrm{Spec}(A)$$

  where

$$\kappa_p = \mathrm{Frac}(A/p) = \text{“residue field” at } p.$$

Most important example: The points of $\mathrm{Spec}(\mathbb{Z})$ are

- prime integers p, with residue fields

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}\,,$$

- the ideal (0), with residue field

$$\mathbb{Q}\,.$$

The notion of dimension of a scheme:

Definition. – *The dimension d of a scheme X is the maximum length of a sequence of morphisms*

$$p_0 \longrightarrow p_1 \longrightarrow \cdots \longrightarrow p_d$$

in the category of its topological points $\mathrm{pt}(X)$.

Remark. –
If $X = \mathrm{Spec}(A)$, $p_0 \longrightarrow p_1 \longrightarrow \cdots \longrightarrow p_d$
is a decreasing sequence of prime ideals of A

$$p_0 \supset p_1 \supset \cdots \supset p_d \,.$$

Key examples. –

- If K is a field,
$$\dim(\mathrm{Spec}(K[T_1, \cdots, T_d])) = d \,.$$
- One has
$$\dim(\mathrm{Spec}(\mathbb{Z})) = 1 \,,$$
which means that $\mathrm{Spec}(\mathbb{Z})$ is a curve!
- More generally,
$$\dim(\mathrm{Spec}(\mathbb{Z}[T_1, \cdots, T_d])) = d + 1 \,.$$

Families of scheme morphisms: open and closed morphisms

Definition. – *A morphism of affine schemes*

$$\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

is called "open" if B is deduced from A by formally inverting some element $f \in A$

$$A[X]/(f \cdot X - 1) \xrightarrow{\sim} B\,.$$

Remark. – In that case, there is an induced bijection

$$\{\text{primes ideals of } B\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{prime ideals of } A \\ \text{which do not contain } f \end{array} \right\}.$$

Definition. – *A morphism of affine schemes*

$$\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

is called "closed" if B is a quotient of A

$$A/I \xrightarrow{\sim} B$$

by some ideal $I \subseteq A$.

Families of scheme morphisms: finite morphisms

Definition. –
A morphism of affine schemes

$$\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

is called "finite"
if B, considered as a module over A,
is finitely generated.

Remarks. –

- Any "closed" morphism is "finite".
- For any finite morphism

  $$\mathrm{Spec}(B) \xrightarrow{p} \mathrm{Spec}(A),$$

  its fiber

  $$p^{-1}(x)$$

  over any topological, geometric or algebraic point

  $$x \quad \text{of} \quad \mathrm{Spec}(A)$$

  is finite.

Families of scheme morphisms: flat morphisms

Definition. –
A module M over a commutative ring A
is called "flat" if, for any morphism of A-modules

$$N_1 \xrightarrow{u} N_2 \,,$$

the induced morphism

$$M \otimes_A \operatorname{Ker}(u) \longrightarrow \operatorname{Ker}(M \otimes_A N_1 \longrightarrow M \otimes_A N_2)$$

is an isomorphism.

Definition. –
A morphism of affine schemes

$$\operatorname{Spec}(B) \longrightarrow \operatorname{Spec}(A)$$

is called "flat"
if B, considered as a module over A, is flat.

Example. –
Any open morphism is flat.

Families of scheme morphisms: smooth and étale morphisms

Definition. – *A morphism of affine schemes*

$$\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$$

is called "smooth of relative dimension d" if

(1) *it is flat,*

(2) *it is finitely presentable*

$$A[T_1, \cdots, T_k]/(P_1, \cdots, P_r) \xrightarrow{\sim} B\,,$$

(3) *considering the matrix of partial derivatives*

$$\left(\frac{\partial P_i}{\partial T_j}\right)_{\substack{1 \le i \le r \\ 1 \le j \le k}},$$

its $(k-d+1) \times (k-d+1)$-minors are 0 in $A[T_1, \cdots, T_k]/(P_1, \cdots, P_r)$, and its $(k-d) \times (k-d)$-minors generate the maximal ideal (1).

Definition. – *A morphism is "étale" if it is smooth of dimension 0.*

Example. – A morphism $\mathrm{Spec}(A[X]/P(X)) \to \mathrm{Spec}(A)$ is "étale" if and only if

$$(P, P') = A[X]\,.$$

Quick reminder on categories of sheaves:

Reminder. –

(i) *Any "Grothendieck topology" J on a category* $\mathcal{C}$ *defines a full subcategory of J-sheaves*

$$\widehat{\mathcal{C}}_J \hookrightarrow \widehat{\mathcal{C}} = \left\{ \begin{array}{c} \textit{category of presheaves } P \\ \mathrm{Ob}(\mathcal{C}) \ni X \mapsto \text{set } P(X) \\ (X \xrightarrow{u} Y) \mapsto \text{map } P(Y) \to P(X) \end{array} \right\}.$$

(ii) *The embedding functor* $j_* : \widehat{\mathcal{C}}_J \hookrightarrow \widehat{\mathcal{C}}$ *has a "left-adjoint" called the "sheafification functor"*

$$j^* : \widehat{\mathcal{C}} \longrightarrow \widehat{\mathcal{C}}_J$$

verifying $j^* \circ j_*(F) \xrightarrow{\sim} F$ *for any J-sheaf F.*

Remarks. –

- There is an associated "canonical functor" $\ell = j^* \circ y : \mathcal{C} \xrightarrow{\text{Yoneda}} \widehat{\mathcal{C}} \xrightarrow{\text{sheafification}} \widehat{\mathcal{C}}_J$.
- If $\mathcal{C} \xrightarrow{y} \widehat{\mathcal{C}}$ factorises as $\mathcal{C} \xrightarrow{\ell} \widehat{\mathcal{C}}_J \xhookrightarrow{j_*} \widehat{\mathcal{C}}$, J is called "subcanonical".
- If K is a topology finer than J, we have $\widehat{\mathcal{C}}_K \hookrightarrow \widehat{\mathcal{C}}_J \hookrightarrow \widehat{\mathcal{C}}$.

Topologies on the category of schemes:

Definition. –

The Zariski [resp. étale, resp. flat] topology on the category of affine schemes

$$\mathrm{Aff}$$

is defined by calling a sieve on an object X

a "covering sieve"

if it contains a finite family of morphisms

$$X_i \longrightarrow X\,, \quad 1 \leq i \leq k$$

such that

$$\begin{cases} (1) & \textit{each } X_i \to X \textit{ is open [resp. étale, resp. flat].} \\ (2) & \textit{any topological point of } X \textit{ is an image} \\ & \textit{of a topological point of at least one } X_i. \end{cases}$$

Remark. –

We have the refinement ordering of topologies

$$\text{Zariski} \subset \text{étale} \subset \text{flat.}$$

Sheaf properties of representables:

Proposition. –
The Grothendieck topologies on Aff

Zariski, étale, flat

are "subcanonical", so that

$$y : \mathrm{Aff} \xhookrightarrow{\text{Yoneda}} \widehat{\mathrm{Aff}}$$

factorises as

$$\mathrm{Aff} \xhookrightarrow{\ \ell\ } \widehat{(\mathrm{Aff})}_{\text{flat}} \hookrightarrow \widehat{(\mathrm{Aff})}_{\text{étale}} \hookrightarrow \widehat{(\mathrm{Aff})}_{\text{Zariski}} \hookrightarrow \widehat{\mathrm{Aff}}\,.$$

Remark. –
As a consequence, a presheaf

$$P = \begin{cases} X = \mathrm{Spec}(A) & \longmapsto \quad \text{set } P(X)\,, \\ (X \xrightarrow{u} Y) & \longmapsto \quad \text{map } P(Y) \xrightarrow{P(u)} P(X)\,, \end{cases}$$

can be representable only if it is a sheaf
for the flat, and a fortiori étale and Zariski, topology.

The general notion of scheme:

Definition. – *A scheme is an object of*

$$\widehat{(\mathrm{Aff})}_{\mathrm{flat}} \hookrightarrow \widehat{(\mathrm{Aff})}_{\text{étale}} \hookrightarrow \widehat{(\mathrm{Aff})}_{\mathrm{Zariski}} \hookrightarrow \widehat{\mathrm{Aff}}$$

which can be written as a colimit of a diagram

$$\varinjlim_{D} y(X_d)$$

of representable objects $y(X_d)$, $X_d = \mathrm{Spec}(A_d)$,
whose transition morphisms

$$X_{d'} \longrightarrow X_d$$

are open morphisms.

Proposition. –
Finite products $X_1 \times \cdots \times X_n$
and fiber products $X \times_S Y$
are well-defined in the category of schemes

$$\mathrm{Sch}$$

as well as in the category of affine schemes

$$\mathrm{Aff}\,.$$

Projective schemes:

Lemma. –
For any integer $d \geq 0$*, the* *sheafification* *of the presheaf*

$$X = \mathrm{Spec}(A) \longmapsto (A^{d+1} - \{0\})/A^{\times}$$

for the *Zariski* *(or, equivalently,* *étale* *or* *flat*) *topology*
is a *scheme*

$$\mathbb{P}^d$$

called the *projective space* *of dimension* d.

Definition. –
A morphism of schemes

$$X \longrightarrow S$$

is called "projective" if it can be factorized as

$$X \hookrightarrow S \times \mathbb{P}^d \longrightarrow S$$

for some $d \geq 0$ *and some* *closed* *morphism*

$$X \hookrightarrow S \times \mathbb{P}^d .$$

“Meaningful” functions in algebraic geometry:

- Is it natural to consider some numerical functions in algebraic geometry?

  Yes, if they are defined from geometry.

- What could be their domains?
  $\rightarrow$ Possible answer: sets of points s of some schemes S.

- How could we imagine to associate numerical values to the points s of some scheme S?

  $\rightarrow$ Possible answer: consider the fibers

$$X \times_S s$$

  of some schemes $X \rightarrow S$,
  and associate numbers to these fibers.

Counting functions for finitely presentable schemes:

Lemma. –

(i) *If S is a scheme finitely presentable over $\mathbb{Z}$, closed topological points of S are topological points s whose residue field κ_s is finite.*

(ii) *If $X \to S$ is projective (or more generally finitely presentable), then for any closed point s of S with $\kappa_s = \mathbb{F}_{q_s}$, the set*

$$(X \times_S s)(\mathbb{F}_{q_s})$$

is finite, as well as more generally the sets

$$(X \times_S s)(\mathbb{F}_{q_s^n})$$

(where $\mathbb{F}_{q_s^n}$ = unique finite extension of $\mathbb{F}_{q_s}$ of dimension n).

Consequence. –

One can consider as "meaningful functions"

$$\begin{array}{ccc} s & \longmapsto & \text{cardinality } \#(X \times_S s)(\mathbb{F}_{q^s}) \\ \| & & \text{or the formal power series} \\ \text{closed point of } S & & 1 + \sum_{n \geq 1} \# (X \times_S s)(\mathbb{F}_{q_s^n}) \cdot Z^n . \end{array}$$

A general loose but very deep question:

Do "meaningful functions" in algebraic geometry have special properties?

- Some properties have been predicted by André Weil (and later proved by Dwork, Grothendieck, Deligne). His first conjecture was that all formal power series

$$1 + \sum_{n \geq 1} (X \times_S s)(\mathbb{F}_{q_s^n}) \cdot Z^n$$

  are rational functions of the form

$$P_s(Z)/Q_s(Z)$$

  for $P_s, Q_s =$ polynomials in Z with constant coefficient 1.
- Robert Langlands has predicted that these functions can all be related to "automorphic representations" which are objects of harmonic analysis over "reductive groups" with coefficients in some "arithmetic rings".

Grothendieck's theory of étale fundamental groups:

Definition. – *For an arbitrary scheme X, let*

$$\mathrm{Cov}_X$$

be the category of schemes over X

$$X' \xrightarrow{p} X$$

whose structure morphism p is étale and finite.

Theorem. –
Suppose X is connected.
Let $\overline{x}$ be a geometric point of X.
Consider the fiber functor

$$\begin{array}{rcl} \mathrm{Cov}_X & \longrightarrow & \{\textit{finite sets}\}, \\ (X' \xrightarrow{p} X) & \longmapsto & p^{-1}(\overline{x}) = X' \times_X \overline{x}. \end{array}$$

Then:

(i) *The symmetries of the fiber functor form a profinite (topological) group $\pi_1(X, \overline{x})$.*

(ii) *The fiber functor induces an equivalence of categories*

$$\mathrm{Cov}_X \xrightarrow{\sim} \{\textit{finite sets endowed with a continuous action of } \pi_1(X, \overline{x})\}.$$

Relation with Galois theory:

Observation. –

If $X = \mathrm{Spec}(K)$ *for a field* K
and $\overline{x} = \mathrm{Spec}(\overline{K})$
for an algebraically closed field $\overline{K}$ *containing* K*,*

we have:

(i) *Grothendieck's group*

$$\pi_1(X, \overline{x})$$

is the automorphism group
of the algebraic closure of K *in* $\overline{K}$*.*

(ii) *The equivalence of categories*

$$\mathrm{Cov}_X \xrightarrow{\sim} \{\text{finite sets} + \text{continuous action of } \pi_1(X, \overline{x})\}$$

is a reformulation of Galois theory.

Relation with Poincaré theory:

Theorem. –
If X is a complex algebraic variety,
the functor

$$\begin{array}{ccc} (X' \to X) & \longmapsto & (X'(\mathbb{C}) \to X(\mathbb{C})) \\ \mathrm{Cov}_X & \longrightarrow & \left\{ \begin{array}{c} \textit{category of } \underline{\textit{finite}} \\ \underline{\textit{locally trivial covers}} \textit{ of } X(\mathbb{C}) \\ \textit{in the } \underline{\textit{topological sense}} \end{array} \right\} \end{array}$$

in an equivalence of categories.

Corollary. –
If $\overline{x} \in X(\mathbb{C})$, the Grothendieck group

$$\pi_1(X, \overline{x})$$

identifies with the profinite completion
of the Poincaré fundamental group

$$\pi_1(X(\mathbb{C}), \overline{x}) \, .$$

Galois groups of finite fields:

Theorem. –
Let $\mathbb{F}_q$ = finite field and $\mathbb{F}_{q^n}$ = finite extension of degree n of $\mathbb{F}_q$.
Then:

(i) *The Frobenius map*

$$\begin{array}{rcccl} \mathrm{Fr}_q & : & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_{q^n} \\ & & a & \longmapsto & a^q \end{array}$$

is an automorphism of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

(ii) *It generates the group of all automorphisms, so that we get an isomorphism*

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Aut}(\mathbb{F}_{q^n}/\mathbb{F}_q)\,, \\ k & \longmapsto & \mathrm{Fr}_q^k\,. \end{array}$$

Corollary. – *If $\overline{\mathbb{F}}_q$ = algebraic closure of $\mathbb{F}_q$, the element*

$$\mathrm{Fr}_q \in \mathrm{Aut}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$$

generates an isomorphism

$$\varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}} \xrightarrow{\sim} \mathrm{Aut}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \pi_1(\mathbb{F}_q, \overline{\mathbb{F}}_q)\,.$$

The central question of agebraic number theory and arithmetic algebraic geometry:

What can be known about

$$\pi_1(\mathbb{Q}, \overline{\mathbb{Q}})?$$

$\rightarrow$ Hint:

Langlands predicted that
irreducible linear representations of the group

$$\pi_1(\mathbb{Q}, \overline{\mathbb{Q}})$$

can be related to some
"automorphic" representations
of reductive groups with coefficients
in some arithmetic rings.

II. From arithmetic geometry to algebraic topology

Reminder of the central question we have met:

What can be known about the Galois group

$$\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q}) = \pi_1(\mathbb{Q}, \overline{\mathbb{Q}}) = \pi_1(\mathbb{Q}, \mathbb{C})$$

if $\overline{\mathbb{Q}}$ is the field of algebraic complex numbers

$$\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}\ ?$$

Reminder of Galois' equivalence:

$$(X \to \mathrm{Spec}(\mathbb{Q})) \longmapsto \mathrm{Hom}(\mathrm{Spec}(\overline{\mathbb{Q}}), X) = \mathrm{Hom}(\mathrm{Spec}(\mathbb{C}), X)$$

$$\mathrm{Cov}_{\mathrm{Spec}(\mathbb{Q})} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{category of finite sets} \\ \text{endowed with a continuous} \\ \text{action of } \pi_1, (\mathbb{Q}, \overline{\mathbb{Q}}) \end{array} \right\}$$

$$\|$$

category of finite étale covers of $\mathrm{Spec}(\mathbb{Q})$

which induces

$$\left\{ \begin{array}{c} \text{category of} \\ \text{“number fields” } E \\ \| \\ \text{finite field extensions of } \mathbb{Q} \end{array} \right\}^{\mathrm{op}} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{category of finite sets} \\ \text{endowed with a continuous} \\ \text{transitive action of } \pi_1(\mathbb{Q}, \overline{\mathbb{Q}}) \end{array} \right\}$$

Basic principle to get information about Galois groups:

- Consider a field E
  (for instance $E = \mathbb{Q}$ or $E =$ number field)
  and an algebraic closure $\overline{E}$ of E.
- Consider algebraic varieties X over E

$$X \longrightarrow \mathrm{Spec}(E)\,,$$

  and their "geometrizations"

$$\overline{X} = X \times_{\mathrm{Spec}(E)} \mathrm{Spec}(\overline{E}) = X \otimes_E \overline{E}\,.$$

- Then the Galois group

$$\mathrm{Aut}(\overline{E}/E)$$

  naturally acts on $\overline{X}$
  and on "algebraic invariants"
  that can be associated to $\overline{X}$.

$\rightarrow$ Hope: Get information on $\mathrm{Aut}(\overline{E}/E)$
through its natural actions
on "refined enough" algebraic invariants of $\overline{X}$
for "well chosen" algebraic varieties X over E.

The first fundamental example of "algebraic invariant" of algebraic varieties:

- One can associate to any scheme S the category of finite étale covers of S

$$\mathrm{Cov}_S \, .$$

- If a group G acts on S, it yields a group morphism

$$G \longrightarrow \{\text{group of self-equivalences } \mathrm{Cov}_S \xrightarrow{\sim} \mathrm{Cov}_S\} \, .$$

Lemma. – *If S is connected, and $\overline{s}$ is a geometric point of S, the equivalence*

$$\mathrm{Cov}_S \xrightarrow{\sim} \{\textit{finite continuous actions of } \pi_1(S, \overline{s})\}$$

yields an isomorphism

$$\left\{ \frac{\textit{group of self-equivalences}}{\textit{of } \mathrm{Cov}_S} \right\} \xrightarrow{\sim} \mathrm{Out}(\pi_1(S, \overline{s}))$$

$$= \mathrm{Aut}(\pi_1(S, \overline{s})) / \left\{ \frac{\textit{subgroup of}}{\textit{inner automorphisms}} \right\} .$$

- If G acts on S, there is an induced morphism $G \to \mathrm{Out}(\pi_1(S, \overline{s}))$.

Application to "geometric" algebraic varieties:

- Let X be an algebraic variety over a field E,

$$\overline{X} = X \otimes_E \overline{E} \qquad \text{and} \qquad \overline{x} \in X(\overline{E}) \, .$$

Corollary. – *If $\overline{X} = X \otimes_E \overline{E}$ is connected, there is a canonical morphism*

$$\mathrm{Aut}(\overline{E}/E) \longrightarrow \mathrm{Out}(\pi_1(\overline{X}, \overline{x})) \, .$$

Remark. – If $E \subset \mathbb{C}$, $\pi_1(\overline{X}, \overline{x})$ is the profinite completion of the Poincaré fundamental group $\pi_1(X(\mathbb{C}), \overline{x})$.
So the group

$$\mathrm{Out}(\pi_1(\overline{X}, \overline{x}))$$

only depends on the topology of $X(\mathbb{C})$,
while the group $\mathrm{Aut}(\overline{E}/E)$ is an arithmetic object.

Question. – If $E = \mathbb{Q}$, are there algebraic varieties X over $\mathbb{Q}$ such that

$$\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Out}(\pi_1(\overline{X}, \overline{x})) \quad \text{is injective?}$$

Answer (consequence of Belyi's theorem):
It already works for $X = \mathbb{P}^1 - \{0, 1, \infty\}$!

Bringing morphisms into the picture:

- Any morphism of schemes
$$X_1 \xrightarrow{u} X_2$$
induces a functor
$$\begin{array}{ccc} (X_2' \to X_2) & \longmapsto & (X_1' = X_2' \times_{X_2} X_1 \to X_1) \\ \mathrm{Cov}_{X_2} & \xrightarrow{u^*} & \mathrm{Cov}_{X_1}\,. \end{array}$$
- If a group G acts on X_1 and X_2
and respects u in the sense that $u \circ g = g \circ u$, $\forall\, g \in G$,
the induced homomorphism
$$G \longrightarrow \left\{ \begin{matrix} \text{self-equivalences} \\ \text{of } \mathrm{Cov}_{X_1} \end{matrix} \right\} \times \left\{ \begin{matrix} \text{self-equivalences} \\ \text{of } \mathrm{Cov}_{X_2} \end{matrix} \right\}$$
factorizes through the subgroup of pairs of self-equivalences
$$(\mathrm{Cov}_{X_1} \xrightarrow[\sim]{\rho_1} \mathrm{Cov}_{X_1}, \mathrm{Cov}_{X_2} \xrightarrow[\sim]{\rho_2} \mathrm{Cov}_{X_2})$$
which are compatible with $u^* : \mathrm{Cov}_{X_2} \to \mathrm{Cov}_{X_1}$ in the sense that
$$u^* \circ \rho_2 \cong \rho_1 \circ u^*\,.$$

Application to diagrams of algebraic varieties:

- Let D be a diagram consisting in

$$\begin{cases} \text{algebraic varieties } X_d \text{ defined over a field } E, \\ \text{morphisms } X_d \xrightarrow{u_\alpha} X_{d'} \text{ defined over } E. \end{cases}$$

- Let $\overline{E}$ be an algebraic closure of E,

$$\overline{X}_d = X_d \otimes_E \overline{E} \qquad \text{with} \qquad \overline{x}_d \in X_d(\overline{E})\,.$$

Proposition. – *The natural homomorphism*

$$\mathrm{Aut}(\overline{E}/E) \longrightarrow \prod_d \left\{ \begin{matrix} \textit{self-equivalences} \\ \textit{of } \mathrm{Cov}_{\overline{X}_d} \end{matrix} \right\} = \prod_d \mathrm{Out}(\pi_1(\overline{X}_d, \overline{x}_d))$$

factorizes through the subgroup of families of self-equivalences which are compatible with all functors

$$u_\alpha^* : \mathrm{Cov}_{X_{d'}} \longrightarrow \mathrm{Cov}_{X_d}\,.$$

Question. – Are there diagrams D such that

$$\mathrm{Aut}(\overline{E}/E) \xrightarrow{\sim} \{\text{subgroup of compatible self-equivalences}\}\,?$$

$\rightarrow$ Grothendieck proposed a suggestion when $E = \mathbb{Q}$.
$\rightarrow$ This would provide a purely topological characterization of $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$!

Finite étale covers as objects of toposes:

- So far, we have considered the invariants of schemes

$$X \longmapsto \mathrm{Cov}_X\,,$$
$$(X \xrightarrow{u} Y) \longmapsto (u^* : \mathrm{Cov}_Y \to \mathrm{Cov}_X)\,.$$

They can be interpreted in terms of toposes:

Proposition. –

(i) *For any scheme X, the category of its finite étale covers* Cov_X *identifies with the full subcategory of*

$$\begin{cases} \bullet \quad \mathrm{Fl}_X = \text{(small) fppf ("faithfully flat of finite presentation") topos,} \\ \bullet \quad \text{or } \mathrm{Et}_X = \text{(small) "étale" topos of } X \end{cases}$$

consisting in objects which are "locally constant and finite", i.e. locally isomorphic to finite sums of copies of X

$$\bullet \cong \coprod_{I = \text{finite set}} \ell(X) \qquad \text{(where } \ell = \text{canonical functor).}$$

(ii) *For any scheme morphism $X \xrightarrow{u} Y$, the induced functor*

$$u^* : \mathrm{Cov}_Y \longrightarrow \mathrm{Cov}_X$$

is induced by the topos morphism

$$(u^*, u_*) : \mathrm{Fl}_X \longrightarrow \mathrm{Fl}_Y\,,$$
$$\text{or} \quad \mathrm{Et}_X \longrightarrow \mathrm{Et}_Y\,.$$

A few words on the definition of étale and flat toposes:

Definition. – *The (small) fppf [resp. étale] topos of a scheme X is the category of sheaves on the site defined in the following way:*

- *The objects of the underlying category are finitely presentable morphisms from affine schemes*

$$X' = \operatorname{Spec}(A') \longrightarrow X$$

  which are flat [resp. étale].

- *The morphisms of the underlying category are commutative triangles*

$$\begin{array}{ccc} X_2' = \operatorname{Spec}(A_2') & \longrightarrow & X_1' = \operatorname{Spec}(A_1') \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

  of flat [resp. étale] morphisms.

- *Covering sieves on an object $(X' \to X)$ are sieves which contain a finite family of morphisms*

$$X_i' \longrightarrow X' , \qquad 1 \leq i \leq k ,$$

such that any topological point of X' is an image of a point of at least one X_i'.

Linearization of group actions or sheaves:

- Consider a finite étale cover $X' \xrightarrow{p} X$.
  If X is connected and $\overline{x}$ is a geometric point, $(X' \xrightarrow{p} X)$ corresponds to a finite set I endowed with an action of $\pi_1(X, \overline{x})$.
- The decomposition of I into orbits,
  corresponds to the decomposition of X into connected components.
  In particular, there is an equivalence

$$X' \text{ connected} \Leftrightarrow \text{the action of } \pi_1(X, \overline{x}) \text{ on } I \text{ is transitive.}$$

  In that case, X' or I can be called an "atom".
- Choose a finite field or ring

$$\Lambda = \mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z} \quad \text{or} \quad \Lambda = \mathbb{Z}/\ell^m\mathbb{Z} \quad (\ell = \text{prime number}).$$

  The free Λ-space or Λ-module on I, $\bigoplus_{i \in I} \Lambda$,
  is endowed with an induced action of $\pi_1(X, \overline{x})$.
  It corresponds to a Λ-linear object of the category Cov_X
  which is the push-forward

$$P_* \Lambda \quad \text{by} \quad X' \xrightarrow{p} X$$

  of the constant sheaf Λ on X'.

Breaking atoms after linearization:

- Even if a finite étale cover

$$(X' \xrightarrow{p} X) \longleftrightarrow I + \text{action of } \pi_1(X, \overline{x})$$

is an "atom",
and Λ is a finite field, its linearization

$$p_* \Lambda \longleftrightarrow \left(\bigoplus_{i \in I} \Lambda \right) + \text{action of } \pi_1(X, \overline{x})$$

will break as direct sums (or non trivial extensions) of smaller linear components.

- The smallest components (which cannot be broken further) can be called the "irreducible components" of

$$p_* \Lambda \longleftrightarrow \left(\bigoplus_{i \in I} \Lambda \right) + \text{action of } \pi_1(X, \overline{x}) \, .$$

Linear invariants of toposes: categories of linear sheaves

- A topos is by definition a category $\mathcal{E}$ which is equivalent
$$\mathcal{E} \xrightarrow{\sim} \widehat{\mathcal{C}}_J$$
to the category $\widehat{\mathcal{C}}_J$ of "sheaves" on some site
$$(\mathcal{C}, J) = \begin{cases} \mathcal{C} = \text{underlying category,} \\ J = \text{Grothendieck topology on } \mathcal{C}. \end{cases}$$
- A morphism of toposes $\mathcal{E}' \xrightarrow{f} \mathcal{E}$ is by definition a pair of adjoint functors
$$(\mathcal{E} \xrightarrow{f^*} \mathcal{E}', \mathcal{E}' \xrightarrow{f_*} \mathcal{E})$$
such that
$$\begin{cases} f_* \text{ respects arbitrary limits,} \\ f^* \text{ respects arbitrary colimits and finite limits.} \end{cases}$$

Definition. – *For any ring Λ, one can associate:*

(i) *To any topos $\mathcal{E}$, the Λ-linear category $\mathrm{Mod}_\Lambda(\mathcal{E})$ of Λ-linear objects of $\mathcal{E}$ (= sheaves of Λ-modules), which is abelian (kernels and cokernels are well-defined).*

(ii) *To any morphism $\mathcal{E}' \xrightarrow{f} \mathcal{E}$ of toposes, Λ-linear functors*
$$f^* : \mathrm{Mod}_\Lambda(\mathcal{E}) \longrightarrow \mathrm{Mod}_\Lambda(\mathcal{E}')$$
$$f_* : \mathrm{Mod}_\Lambda(\mathcal{E}') \longrightarrow \mathrm{Mod}_\Lambda(\mathcal{E}) .$$

Linear invariants of toposes: cohomology:

Proposition. – *Let Λ be a ring and $(\mathcal{E}' \xrightarrow{f} \mathcal{E})$ a topos morphism.*

(i) *The pull-back functor*

$$f^* : \mathrm{Mod}_\Lambda(\mathcal{E}) \longrightarrow \mathrm{Mod}_\Lambda(\mathcal{E}')$$

respects all kernels and cokernels.

(ii) *The push-forward functor*

$$f_* : \mathrm{Mod}_\Lambda(\mathcal{E}') \longrightarrow \mathrm{Mod}(\mathcal{E})$$

respects all kernels, but not cokernels.
It has well-defined cohomology functors

$$R^i f_* : \mathrm{Mod}_\Lambda(\mathcal{E}') \longrightarrow \mathrm{Mod}(\mathcal{E}) , \quad i \geq 1 ,$$

completing $R^0 f_* = f_*$.

Remarks. –

- Any topos $\mathcal{E}$ has a unique topos morphism $\mathcal{E} \xrightarrow{p} \mathrm{Set}$, so it has the Λ-modules invariants

$$R^i p_* p^* \Lambda = H^i(\mathcal{E}, \Lambda) , \quad i \geq 0 .$$

- Any topos morphism $\mathcal{E}' \xrightarrow{f} \mathcal{E}$ induces Λ-linear maps

$$f^* : H^i(\mathcal{E}, \Lambda) \longrightarrow H^i(\mathcal{E}', \Lambda) .$$

The étale topos of fields:

Proposition. –
Consider a field E,
an algebraic closure $\overline{E}$ of E, defining a geometric point $\overline{x}$ of $\mathrm{Spec}(E)$.
Then the fiber functor

$$\overline{x}^* : \mathrm{Et}_E = \mathrm{Et}_{\mathrm{Spec}(E)} \longrightarrow \mathrm{Set}$$

induces an equivalence of the étale topos of E

$$\mathrm{Et}_E \xrightarrow{\sim} \{\textit{sets} + \textit{continuous action of } \pi_1(E, \overline{E}) = \mathrm{Aut}(\overline{E}/E)\}.$$

Corollary. – *Let Λ be a ring.*

(i) *Any algebraic variety $(X \xrightarrow{p} \mathrm{Spec}(E))$ over E has well-defined Λ-linear cohomology invariants*

$$R^i p_* \Lambda = H^i_{\text{ét}}(X, \Lambda)$$

which are Λ-modules endowed with a continuous action of $\mathrm{Aut}(\overline{E}/E)$.

(ii) *Any morphism of algebraic varieties $(X \xrightarrow{f} Y)$ over E induces Λ-linear morphisms*

$$f^* : H^i_{\text{ét}}(Y, \Lambda) \longrightarrow H^i_{\text{ét}}(X, \Lambda)$$

which respect the actions of $\mathrm{Aut}(\overline{E}/E)$.

From étale to ℓ-adic cohomology:

- **Basic fact**: As Galois groups $\mathrm{Aut}(\overline{E}/E)$ are profinite, cohomology invariants of algebraic varieties X over E
$$H^i_{\text{ét}}(X, \Lambda)$$
are non trivial and interesting only when Λ is finite.
- **More refined fact**: The study of the case of curves over E shows that the
$$H^i_{\text{ét}}(X, \Lambda)$$
are well-behaved only when $\mathbb{Q} \subseteq E$
or $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \subseteq E$ and p is invertible in Λ.

Definition. – *Choose a prime number ℓ which is invertible in E.*
We associate to any algebraic variety X over E
its ℓ-adic cohomology invariants
$$H^i(X, \mathbb{Q}_\ell) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim_m H^i_{\text{ét}}(X, \mathbb{Z}/\ell^m\mathbb{Z})$$
which are finite-dimensional $\mathbb{Q}_\ell$-spaces
endowed with a continuous action of $\mathrm{Aut}(\overline{E}/E)$.

Remark. – Any morphism $X \xrightarrow{f} Y$ of algebraic varieties over E
induces $\mathbb{Q}_\ell$-linear maps which respect the actions of $\mathrm{Aut}(\overline{E}/E)$
$$H^i(Y, \mathbb{Q}_\ell) \longrightarrow H^i(X, \mathbb{Q}_\ell).$$

Compatibility with fiber formation :

Theorem. – *Consider a projective scheme over a base scheme* S

$$X \xrightarrow{p} S\,.$$

Suppose $S \to \mathrm{Spec}(\mathbb{Z})$ *factorises through* $\mathrm{Spec}(\mathbb{Z}[\frac{1}{\ell}])$ *for some prime* ℓ.
Then for any $m \geq 1$*, any* $i \geq 0$*, and any algebraic point*

$$s = \mathrm{Spec}(k) \longrightarrow S\,,$$

the fiber at s of the $\mathbb{Z}/\ell^m\mathbb{Z}$*-linear cohomology sheaf*

$$s^* R^i p_* \mathbb{Z}/\ell^m\mathbb{Z}$$

identifies with the cohomology invariants

$$H^i(\overline{X}_s, \mathbb{Z}/\ell^m\mathbb{Z})$$

of the fiber $X_s = X \times_S s$ *of* $X \xrightarrow{p} S$ *over* $s = \mathrm{Spec}(k)$.

Remarks. –

- The fibers $s^* R^i p_* \mathbb{Z}/\ell^m\mathbb{Z} = H^i(\overline{X}_i, \mathbb{Z}/\ell^m\mathbb{Z})$ are finite $\mathbb{Z}/\ell^m\mathbb{Z}$-module endowed with an action of $\mathrm{Aut}(\overline{k}/k)$.
- If $k = \mathbb{F}_q$ is finite, $\mathrm{Aut}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is generated by Fr_q and identifies with $\widehat{\mathbb{Z}}$.

More in the case of smooth projective morphisms:

Theorem. – *Consider as before a projective morphism of schemes*

$$X \xrightarrow{p} S \quad \textit{over some} \quad \mathrm{Spec}(\mathbb{Z}[\tfrac{1}{\ell}])\,.$$

Suppose the morphism p is also smooth.
Then all cohomology sheaves

$$R^i p_* \mathbb{Z}/\ell^m\mathbb{Z}$$

are $\mathbb{Z}/\ell^m\mathbb{Z}$-linear objects of Cov_S
which are locally free over $\mathbb{Z}/\ell^m\mathbb{Z}$.
If S is connected and $\overline{s}$ is a geometric point of S,
they can be viewed as free $\mathbb{Z}/\ell^m\mathbb{Z}$-modules
endowed with a continuous action of $\pi_1(S, \overline{s})$.

Remark. – As a consequence, the ℓ-adic cohomology sheaves

$$\mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \varprojlim_{m \geq 1} R^i p_* \mathbb{Z}/\ell^m\mathbb{Z}$$

can be viewed as finite-dimensional $\mathbb{Q}_\ell$-vector spaces
endowed with a continuous action of $\pi_1(S, \overline{s})$.

Poincaré duality:

Theorem. – *Consider an algebraic variety over a field K*

$$X \longrightarrow \mathrm{Spec}(K)$$

and a prime ℓ invertible in K. Then:

(i) *If* $\dim(X) \leq d$, *all cohomology invariants*

$$H^i(\overline{X}, \mathbb{Z}/\ell^m\mathbb{Z})$$

are 0 *in degrees $i > 2d$.*

(ii) *If $\overline{X} = X \otimes_K \overline{K}$ is connected of dimension d, all*

$$H^{2d}(\overline{X}, \mathbb{Z}/\ell^m\mathbb{Z})$$

are free of rank 1 *over $\mathbb{Z}/\ell^m\mathbb{Z}$.*

(iii) *If furthermore X is projective and smooth over K, there are perfect pairings*

$$H^i(\overline{X}, \mathbb{Z}/\ell^m\mathbb{Z}) \times H^{2d-i}(\overline{X}, \mathbb{Z}/\ell^m\mathbb{Z}) \longrightarrow H^{2d}(\overline{X}, \mathbb{Z}/\ell^m\mathbb{Z}) .$$

Remark. – As a consequence, all of this also applies to the $H^i(\overline{X}, \mathbb{Q}_\ell)$.
In particular, the $\mathbb{Q}_\ell$-linear representations of $\mathrm{Aut}(\overline{K}, K)$

$$H^i(\overline{X}, \mathbb{Q}_\ell) \quad \text{and} \quad H^{2d-i}(\overline{X}, \mathbb{Q}_\ell)$$

are dual to each other.

Action of correspondences

- If a monoid M acts by endomorphisms on an algebraic variety over a field K, then M^{op} acts on the $H^i(\overline{X}, \mathbb{Z}/\ell^m\mathbb{Z})$ and $H^i(\overline{X}, \mathbb{Q}_\ell)$.

Proposition. –
Suppose X is an algebraic variety over a field K and ℓ a prime invertible in K.
Suppose C is a "correspondence", i.e. a formal linear combination of schemes $\Gamma \to X \times X$ whose first projection $\mathrm{pr}_1 : \Gamma \to X$ is finite and étale.
Then C acts on all

$$H^i(\overline{X}, \mathbb{Z}/\ell^m\mathbb{Z}) \qquad \text{and} \qquad H^i(\overline{X}, \mathbb{Q}_\ell)\,.$$

Moreover, these actions are compatible with composition.

Intertwining Galois actions and correspondences:

Corollary. – *Suppose an algebraic variety X over a field K (with $\ell \neq 0$ in K) is endowed with an algebra homomorphism*

$$\mathcal{H} \longrightarrow \{\text{algebra of correspondences on } X\}.$$

Then all cohomology invariants

$$H^i(\overline{X}, \mathbb{Z}/\ell^m\mathbb{Z}) \qquad \text{and} \qquad H^i(\overline{X}, \mathbb{Q}_\ell)$$

are endowed with

- *a continuous action of $\mathrm{Aut}(\overline{K}, K)$,*
- *an action of the algebra $\mathcal{H}$,*

that commute with each other.

Consequence. – *All irreducible components of the $H^i(\overline{X}, \mathbb{Q}_\ell)$ have the form:*

$$\underset{\substack{\text{irreducible representation}\\ \text{of } \mathrm{Aut}(\overline{K}/K)}}{\sigma} \otimes \underset{\substack{\text{irreducible representation}\\ \text{of } \mathcal{H}}}{\pi}$$

Correspondences of irreducible representations:

- Any action by correspondences
  of an algebra $\mathcal{H}$
  on an algebraic variety over a field K
  generates a family of pairs of irreducible representations

$$(\sigma, \pi) \quad \text{of } \mathrm{Aut}(\overline{K}/K) \text{ and } \mathcal{H}\,.$$

Natural questions:

- Are there algebraic varieties X
  endowed with actions of an algebra $\mathcal{H}$
  which generate meaningful intertwinings
  of irreducible representations of $\mathrm{Aut}(\overline{K}/K)$ and $\mathcal{H}$?
- If yes,
  how to express and study these intertwinings?
- Can such intertwinings
  give information on Galois groups
  of some fields, in particular $\mathbb{Q}$?

The Grothendieck-Lefschetz point formula:

Theorem. –

Let X be a projective algebraic variety over a finite field $k = \mathbb{F}_q$.

Let ℓ be a prime such that $\ell \neq 0$ in $\mathbb{F}_q$.

Then:

(i) *For any $n \geq 1$,*

$$\begin{aligned} \# X(\mathbb{F}_{q^n}) &= \# \{\text{fixed points of } \mathrm{Fr}_q^n \text{ acting on } \overline{X} = X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q\} \\ &= \sum_{i \geq 0} (-1)^i \cdot \mathrm{Tr}(\mathrm{Fr}_q^n, H^i(\overline{X}, \mathbb{Q}_\ell)) \,. \end{aligned}$$

(ii) *For any correspondence $\Gamma \to X \times X$ and any $n \geq 1$,*

$$\begin{aligned} &\# \{\text{fixed points of } \Gamma \circ \mathrm{Fr}_q^n \text{ acting on } \overline{X} = X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q\} \\ = &\sum_{i \geq 0} (-1)^i \cdot \mathrm{Tr}(\Gamma \circ \mathrm{Fr}_q^n, H^i(\overline{X}, \mathbb{Q}_\ell)) \,. \end{aligned}$$

Application to the determination of irreducible components:

Corollary. – *Let K be the field of (rational) functions on some integral base scheme of finite presentation*

$$S \longrightarrow \mathrm{Spec}(\mathbb{Z}[\tfrac{1}{\ell}]) \longrightarrow \mathrm{Spec}(\mathbb{Z}) .$$

Consider a smooth projective scheme over S

$$X \xrightarrow{p} S$$

(extending its "generic fiber" $X_K = X \times_S \mathrm{Spec}(K)$).
Suppose an algebra $\mathcal{H}$ acts by correspondences

$$\Gamma \longrightarrow X \times_S X \quad \text{(such that } \mathrm{pr}_1 : \Gamma \to X \text{ is finite étale).}$$

Then, for

$$\begin{cases} \text{any element } h \in \mathcal{H}, \\ \text{any closed point } s = \mathrm{Spec}(\mathbb{F}_{q_s}) \text{ of } S, \\ \text{any } n \geq 1 , \end{cases}$$

we have

$$\begin{aligned} & \# \{\text{fixed points of } h \circ \mathrm{Fr}_s^n \text{ acting on } \overline{X}_s = X_s \otimes_{\mathbb{F}_{q_s}} \overline{\mathbb{F}}_{q_s}\} \\ = \; & \sum_{i \geq 0} (-1)^i \cdot \mathrm{Tr}(h \circ \mathrm{Fr}_s, H^i(\overline{X}_K, \mathbb{Q}_\ell)) . \end{aligned}$$

Remark. – The Fr_s define conjugacy classes in $\pi_1(S, \mathrm{Spec}(\overline{K}))$.
They are dense.

Getting knowledge on Galois representations through geometry:

- In the previous situation of a smooth projective scheme

$$X \longrightarrow S$$

over a finitely presentable base scheme

$$S \longrightarrow \mathrm{Spec}(\mathbb{Z}[\tfrac{1}{\ell}]) \longrightarrow \mathrm{Spec}(\mathbb{Z})$$

with function field K,
and an action of an algebra $\mathcal{H}$ by correspondences

$$\Gamma \longrightarrow X \times_S X\,,$$

the irreducible components of the

$$H^i(\overline{X}_K, \mathbb{Q}_\ell)$$

as representations of $\mathrm{Aut}(\overline{K}/K) \times \mathcal{H}$
are entirely determined by the geometric information

$$\#\,\{\text{fixed points of } \; h \circ \mathrm{Fr}_s^n \text{ acting on } \overline{X}_s = X_s \otimes_{\mathbb{F}_{q_s}} \overline{\mathbb{F}}_{q_s}\}$$

for

$$\begin{cases} h = \text{element of } \mathcal{H}, \\ s = \mathrm{Spec}(\mathbb{F}_{q_s}) = \text{closed point of } S. \end{cases}$$

III. From arithmetic algebraic geometry to harmonic analysis

The central question of algebraic number theory and arithmetic algebraic geometry:

- What can be known about
$$\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q}) \ ?$$
- More generally, what can be known about
$$\mathrm{Aut}(\overline{K}/K)$$
for fields K of "arithmetic nature"?

Fields of “arithmetic nature”:

- A field can be called “of arithmetic nature” if

(1) it can be written as a fraction field

$$K = \mathrm{Frac}(A)$$

of some “integral domains”
(= commutative rings without zero divisors)
which are finitely presentable

$$A \cong \mathbb{Z}[T_1, \cdots, T_k]/(P_1, \cdots, P_r),$$

(2) equivalently, it can be written as the
“function field”
= “field of rational functions”
= residue field at the “generic point”
(= topological point whose closure is everything)
of an integral finitely presentable scheme S.

Definition. – *The dimension of such an “arithmetic field”*

$$K = \mathrm{Frac}(A) = \text{function field of } S$$

is defined as $\dim(\mathrm{Spec}(A)) = \dim(S)$.

Arithmetic fields of dimension 0:

Proposition. –
The only arithmetic fields of dimension 0
are finite fields

$$\mathbb{F}_q .$$

Their Galois groups are fully known:

Theorem. –
For any finite field $\mathbb{F}_q$,
there is a canonical isomorphism

$$\begin{array}{rcl} \varprojlim\limits_{n\geq 1} \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}} & \xrightarrow{\sim} & \mathrm{Aut}(\overline{\mathbb{F}}_q/\mathbb{F}_q)\,, \\ 1 & \longleftrightarrow & \mathrm{Fr}_q\,. \end{array}$$

Arithmetic fields of dimension 1:

Proposition. –
The only "arithmetic fields" of dimension 1 are "global fields" consisting in the two families:

(1) *"Number fields"*

- $\mathbb{Q}$,
- *"finite extensions" of* $\mathbb{Q}$
  $=$ *finite-dimensional algebraic extensions of* $\mathbb{Q}$.

(2) *"Functions fields"*
$=$ *finite extensions of some* $\mathbb{F}_q(\top)$
$=$ *fields of rational functions* K
on some "curve" X *over a finite field* $\mathbb{F}_q$.

Remark. –
For any "function field" K,
there are a unique finite field $\mathbb{F}_q$ and a unique curve S over $\mathbb{F}_q$ such that

- K is the field of rational functions on S,
- S is projective and smooth over $\mathbb{F}_q$,
- $\overline{S} = S \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$ is connected.

The “class field” isomorphisms:

- Recall that any (topological) group G has a biggest abelian quotient:

$$G^{\mathrm{ab}} = G/[G, G]$$
$$\|$$
invariant subgroup generated by commutators $g\,k\,g^{-1}k^{-1}$

- Most of algebraic number theory from Euler to the early 1930’s can be summarized by the “class field isomorphism” theorem:

Theorem. –
Let K be a “global field” (= arithmetic field of dimension 1).
Then one can construct a canonical isomorphism

$$\mathrm{Aut}(\overline{K}/K)^{\mathrm{ab}} \xrightarrow{\sim} \textit{profinite completion of } \mathbb{A}_K^\times/K^\times$$

where

$$\begin{cases} \mathbb{A}_K = \textit{topological ring of “adèles” of } K, \\ \mathbb{A}_K^\times = \textit{topological group of invertible elements of } \mathbb{A}_K. \end{cases}$$

Remark. – The proof constructs an explicit equivalence

$$\left\{ \begin{array}{c} \text{finite sets endowed} \\ \text{with a transitive} \\ \text{continuous action of } \mathbb{A}_K^\times/K^\times \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{finite Galois extensions} \\ K \subseteq L \\ \text{whose Galois group } \mathrm{Aut}(L/K) \\ \text{is abelian} \end{array} \right\}.$$

Adèle rings:

Definition. –

(i) *If K is a "number field" canonically written as*

$K = \mathrm{Frac}(A_K)$

for A_K = finite normal extension of $\mathbb{Z}$,

its adèle ring is the topological ring

$\mathbb{A}_K = \mathbb{A}_K^f \times \mathbb{A}_K^\infty$ *with*

$$\begin{cases} \mathbb{A}_K^\infty = K \otimes_{\mathbb{Q}} \mathbb{R}\,, \\ \mathbb{A}_K^f = \left(\varprojlim_{I = \text{non zero ideal}} A_K/I \right) \otimes_{A_K} K\,. \end{cases}$$

(ii) *If K is a "function field" canonically written as*

K = *function field of* S_K

for S_K = smooth projective curve over some $\mathbb{F}_q$,

its adèle ring is the topological ring

$$\varinjlim_{\substack{U_K = \mathrm{Spec}(A_K) \\ = \text{ open affine subscheme of } S_K}} \left(\varprojlim_{I \,=\, \text{non zero ideal}} A_K/I \right) \otimes_{A_K} K$$

Basic properties of adèle rings:

Proposition. –
Let K be a global field.

(i) *The canonical morphism*

$$K \longrightarrow \mathbb{A}_K$$

is an embedding. Furthermore,

$$\begin{cases} \bullet & K \text{ is a discrete subring of the topological ring } \mathbb{A}_K, \\ \bullet & \text{the quotient } \mathbb{A}_K/K \text{ is compact.} \end{cases}$$

(ii) *The induced embedding*

$$K^\times \hookrightarrow \mathbb{A}_K^\times$$

makes $K^\times$ a discrete subgroup of the topological group $\mathbb{A}_K^\times$. The quotient is naturally endowed with a surjective morphism

$$\begin{cases} \mathbb{A}_K^\times/K^\times \xrightarrow{\deg} \mathbb{R} & \text{if } K \text{ is a number field,} \\ \mathbb{A}_K^\times/K^\times \xrightarrow{\deg} \mathbb{Z} & \text{if } K \text{ is a function field} \end{cases}$$

whose kernel

$$\mathbb{A}_K^{\times 0}/K^\times$$

is compact.

Back to the central question:

If K is a global field,
how to get knowledge on the Galois group

$$\mathrm{Aut}(\overline{K}/K)$$

besides its abelian part?

Grothendieck's direct geometric approach:

In the case $K = \mathbb{Q}$,
Grothendieck proposed to get information on
(and possibly determine?) $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$
by studying its actions on categories of finite étale covers

Cov_X ($\xrightarrow{\sim}$ category of finite topological covers of $X(\mathbb{C})$)

of "natural" algebraic varieties

X over $\mathbb{Q}$,

and exploiting the fact that they have to respect the pull-back functors

$$u^* : \mathrm{Cov}_Y \longrightarrow \mathrm{Cov}_X$$

defined by morphisms $X \xrightarrow{u} Y$ of algebraic varieties over $\mathbb{Q}$.

The indirect approach through linear representations:

- Introduce "natural" algebraic varieties over global fields K
$$X_K \longrightarrow \mathrm{Spec}(K)$$
or more generally "natural" schemes over a base scheme S
$$X \xrightarrow{p} S\,,$$
endowed with natural actions by algebras of correspondences
$$\mathcal{H}\,,$$
so that their ℓ-adic cohomology spaces or sheaves
$$H^i(\overline{X}_K, \mathbb{Q}_\ell) \qquad \text{or} \qquad R^i p_* \mathbb{Q}_\ell$$
can be seen as linear representations of
$$\mathrm{Aut}(\overline{K}/K) \qquad \text{or} \qquad \pi_1(S, \overline{s})$$
endowed with an action of $\mathcal{H}$.
- Study, using in particular the Grothendieck fixed points theorem, the pairs (σ, π) consisting in
$$\begin{cases} \sigma = \text{irreducible representation of } \mathrm{Aut}(\overline{K}/K) \text{ or } \pi_1(S, \overline{s}), \\ \pi = \text{irreducible representation of } \mathcal{H}, \end{cases}$$
such that $\sigma \otimes \pi$ appears as an irreducible component of some
$$H^i(\overline{X}_K, \mathbb{Q}_\ell) \qquad \text{or} \qquad R^i p_* \mathbb{Q}_\ell\,.$$

How to define "natural" algebraic varieties or schemes?

Grothendieck's general principle: start from "moduli" problems.

- Consider a base scheme S (in general, a finitely presentable integral scheme whose function field may be for instance a global field) and the category Sch/S of finitely presentable schemes over S

$$(S' \longrightarrow S)\,.$$

- Define a presheaf $M : (\mathrm{Sch}/S)^{\mathrm{op}} \longrightarrow \mathrm{Set}$ by a"moduli" problem, i.e. a classification problem of some type of geometric structures over objects of Sch/S

$$(S' \to S) \quad \longmapsto \quad M(S' \to S) = \left\{ \begin{array}{l} \text{set of isomorphism classes} \\ \text{of geometric structures over } S' \\ \qquad C' \to S' \\ \text{of some prescribed type} \end{array} \right\},$$

$$\begin{pmatrix} S_2' & \longrightarrow & S_1' \\ & \searrow \quad \swarrow & \\ & S & \end{pmatrix} \quad \longmapsto \quad \text{map } [M(S_1' \to S) \to M(S_2' \to S)]$$

defined by pull-back $(C' \to S_1') \mapsto (C' \times_{S_1'} S_2' \to S_2')$.

Moduli problems and "meaningful" schemes:

Definition. – *A moduli problem incarnated as a presheaf*

$$\begin{array}{rccl} M \; : & (\mathrm{Sch}/S)^{\mathrm{op}} & \longrightarrow & \mathrm{Set}\,, \\ & (S' \to S) & \longmapsto & \text{set } M(S' \to S)\,, \\ & \left(\begin{array}{ccc} S_2' & \longrightarrow & S_1' \\ & \searrow \quad \swarrow & \\ & S & \end{array}\right) & \longmapsto & \text{map } [M(S_1' \to S) \to M(S_2' \to S)] \end{array}$$

has a "geometric solution", if it is representable by a scheme $\mathcal{M} \longrightarrow S\,.$

Remarks : –

- If a moduli problem M has a geometric solution $\mathcal{M}$, it is unique up to unique isomorphism.
- In that case, for any $(S' \to S)$, the set of morphisms
$$\left(\begin{array}{ccc} S' & \longrightarrow & \mathcal{M} \\ & \searrow \quad \swarrow & \\ & S & \end{array}\right)$$
identifies with the set $M(S' \to S)$ of isomorphism classes of geometric structures $C' \to S'$ of the prescribed type.
- Schemes that are solutions to moduli problems can be considered "meaningful".

A key example: the modular schemes classifying curves

Theorem (stated in a simplified almost correct way). –
For any integer $g \geq 0$,
there is a finitely presentable scheme

$$\mathcal{M}_g \longrightarrow \mathrm{Spec}(\mathbb{Z})$$

such that, for any scheme S,

$$\mathcal{M}_g(S)$$

identifies with the set of isomorphism classes
of "relative curves" of genus g

$$C \longrightarrow S\,,$$

meaning

- *the structure morphism $C \to S$ is projective and smooth,*
- *for any geometric point $\overline{s}$ of S, the associated fiber*

$$C_{\overline{s}} = C \times_S \overline{s} \quad \text{is a connected curve of genus } g.$$

The derived family of schemes classifying curves with chosen points:

Corollary. –
For any integers $g \geq 0$ and $n \geq 0$, there is a finitely presentable scheme

$$\mathcal{M}_{g,n} \longrightarrow \mathrm{Spec}(\mathbb{Z})$$

such that, for any scheme S,

$$\mathcal{M}_{g,n}(S)$$

identifies with the set of isomorphism classes
of "relative curves" of genus g

$$C \xrightarrow{p} S$$

endowed with n sections x_i

$$C \underset{x_i}{\overset{p}{\rightleftarrows}} S$$

whose images do not meet.

Remarks. –

- For any geometric point $\overline{s}$ of such S,

$$C_{\overline{s}} = C \times_S \overline{s}$$

  is just a (smooth projective) curve of genus g with n chosen points.
- $\mathcal{M}_{0,4}$ identifies with $\mathbb{P}^1 - \{0, 1, \infty\}$.

The geometric diagram of modular schemes of curves:

- The modular schemes $\mathcal{M}_{g,n}$ (including $\mathcal{M}_{g,0} = \mathcal{M}_g$) are related by morphisms

$$\mathcal{M}_{g,n} \longrightarrow \mathcal{M}_{g,m} \qquad \text{(for } m < n\text{)}$$

  defined by forgetting $n - m$ of the chosen points.
- On the other hand, one can prove that they have natural compactifications

$$\mathcal{M}_{g,n} \hookrightarrow \overline{\mathcal{M}_{g,n}}$$

  which are also defined as solutions of moduli problems.
- As a consequence of the moduli interpretations, the boundaries

$$\overline{\mathcal{M}_{g,n}} - \mathcal{M}_{g,n}$$

  split into boundary strata

$$\partial\,\overline{\mathcal{M}_{g,n}}$$

  which are endowed with natural projections

$$\partial\,\overline{\mathcal{M}_{g,n}} \longrightarrow \mathcal{M}_{g',n'}\,.$$

A question of Grothendieck about the Galois group:

- Consider the algebraic varieties over $\mathbb{Q}$

$$\mathcal{M}_{g,n}^{\mathbb{Q}}, \quad \overline{\mathcal{M}_{g,n}^{\mathbb{Q}}}, \quad \partial\, \overline{\mathcal{M}_{g,n}^{\mathbb{Q}}}$$

deduced from the schemes $\mathcal{M}_{g,n}$, $\overline{\mathcal{M}_{g,n}}$, $\partial\overline{\mathcal{M}_{g,n}}$ as the fibers over $\mathrm{Spec}(\mathbb{Q}) \to \mathrm{Spec}(\mathbb{Z})$.

- The Galois group

$$\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$$

embeds (thanks to Belyi's theorem and $\mathcal{M}_{0,4} \cong \mathbb{P}^1 - \{0, 1, \infty\}$) into the group of families of self-equivalences of categories

Cov_X ($\xrightarrow{\sim}$ category of finite topological covers of $X(\mathbb{C})$)

for $X \in \{\mathcal{M}_{g,n}^{\mathbb{Q}}, \quad \overline{\mathcal{M}_{g,n}^{\mathbb{Q}}}, \quad \partial\, \overline{\mathcal{M}_{g,n}^{\mathbb{Q}}}\}$,
which respect the pull-back functors induced by the natural morphisms

$$\left\{ \begin{array}{ccc} \mathcal{M}_{g,n}^{\mathbb{Q}} & \longrightarrow & \mathcal{M}_{g,m}^{\mathbb{Q}}, \\ \overline{\mathcal{M}_{g,n}^{\mathbb{Q}}} & \hookrightarrow & \overline{\mathcal{M}_{g,n}^{\mathbb{Q}}}, \\ \partial\overline{\mathcal{M}_{g,n}^{\mathbb{Q}}} & \longrightarrow & \mathcal{M}_{g',n'}^{\mathbb{Q}}. \end{array} \right. \quad \partial\overline{\mathcal{M}_{g,n}^{\mathbb{Q}}} \hookrightarrow \overline{\mathcal{M}_{g,n}^{\mathbb{Q}}},$$

Grothendieck's question. – Is this embedding an isomorphism?

Picard and Jacobian schemes

This is another natural family of moduli schemes.

Theorem. – *Let $C \to S$ be a smooth projective morphism of schemes such that, for any geometric point $\overline{s}$ of S,*

$C_{\overline{s}} = C \times_S \overline{s}$ *is a connected curve of genus g. Then:*

(i) *The presheaf*

$$\begin{aligned} (\mathrm{Sch}/S)^{\mathrm{op}} &\longrightarrow \mathrm{Set} \\ (S' \to S) &\longmapsto \left\{ \begin{array}{c} \text{set of isomorphism classes} \\ \text{of rank 1 vector bundles on } C \times_S S' \end{array} \right\} \end{aligned}$$

is representable by a scheme over S

$$\mathrm{Pic}_{C/S} = \coprod_{d \in \mathbb{Z}} \mathrm{Pic}^d_{C/S}$$

whose components $\mathrm{Pic}^d_{C/S}$ are projective and smooth of relative dimension g over S.

(ii) *The tensor product of rank 1 vector bundles defines a commutative group structure on $\mathrm{Pic}_{C/S}$ which is compatible with the "degree" morphism*

$$\mathrm{Pic}_{C/S} = \coprod_{d \in \mathbb{Z}} \mathrm{Pic}^d_{C/S} \longrightarrow \mathbb{Z}\,.$$

In particular, $\mathrm{Pic}^0_{C/S} = \mathrm{Jac}_{C/S}$ is an "abelian scheme" over S.

Drinfeld's moduli of rank 1 "shtukas":

- Consider a smooth projective curve C over a finite field $\mathbb{F}_q$ such that $\overline{C} = C \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q}$ is connected.
- For any scheme S over $\mathbb{F}_q$, consider the canonical Frobenius morphism

$$\mathrm{Fr}_S : S \longrightarrow S$$

which is defined on any affine scheme $\mathrm{Spec}(A) \to S$ by

$$\begin{array}{ccc} A & \longrightarrow & A\,, \\ a & \longmapsto & a^q\,. \end{array}$$

Definition. – *Consider a scheme S over $\mathbb{F}_q$ and two morphisms $0, \infty : S \rightrightarrows C$ whose graphs are denoted $\Gamma_0 \hookrightarrow S \times C$ and $\Gamma_\infty \hookrightarrow S \times C$.*

(i) *A rank 1 "shtuka" over S of zero 0 and pole ∞ is a rank 1 vector bundle $\mathcal{E}$ on $S \times C$ endowed with an isomorphism well-defined on $S \times C - (\Gamma_0 \cup \Gamma_\infty)$*

$$(\mathrm{Fr}_S \times \mathrm{id}_C)^* \mathcal{E} \xrightarrow{\sim} \mathcal{E}$$

which has a simple "zero" on Γ_0 and a simple "pole" on Γ_∞.

(ii) *If $I \hookrightarrow C$ is a finite closed subscheme and $\infty, 0$ take values in $C - I$, a "level I structure" on such a rank 1 shtuka is an isomorphism*

$$\mathcal{E}_{|S\times I} \xrightarrow{\sim} \textit{trivial rank 1 vector bundle on } S \times I$$

which is compatible with $(\mathrm{Fr}_S \times \mathrm{id}_I)^* \mathcal{E}_{|S\times I} \xrightarrow{\sim} \mathcal{E}_{|S\times I}$.

Moduli schemes of rank 1 "shtukas":

We still consider a smooth projective curve C over $\mathbb{F}_q$.

Theorem. –

(i) *The presheaf*

$$\begin{array}{ccc} (\mathrm{Sch}/C \times C)^{\mathrm{op}} & \longrightarrow & \mathrm{Set} \\ (S \xrightarrow{(0,\infty)} C \times C) & \longmapsto & \left\{ \begin{array}{c} \textit{set of isomorphism classes} \\ \textit{of rank } 1 \textit{ shtukas over } S \\ \textit{of zero } 0 \textit{ and pole } \infty \end{array} \right\} \end{array}$$

is representable by a scheme over $C \times C$

$$\mathrm{Sht}_C^1 = \coprod_{d \in \mathbb{Z}} \mathrm{Sht}_C^{1,d} \longrightarrow C \times C$$

whose components $\mathrm{Sht}_C^{1,d} \longrightarrow C \times C$ are finite étale covers.

(ii) *Similarly, for any finite closed subscheme $I \hookrightarrow C$, the presheaf of rank 1 shtukas endowed with a level I structure is representable by a scheme over $(C - I) \times (C - I)$*

$$\mathrm{Sht}_{C,I}^1 = \coprod_{d \in \mathbb{Z}} \mathrm{Sht}_{C,I}^{1,d} \longrightarrow (C - I) \times (C - I)$$

whose components $\mathrm{Sht}_{C,I}^{1,d} \longrightarrow (C - I) \times (C - I)$ are finite étale covers.

Actions of groups of invertible bundles:

Lemma. –

(i) *The tensor product defines an action on* $\mathrm{Sht}_C^1 \to C \times C$ *of the group*

$$\mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)$$

of rank 1 *vector bundles on* C.

(ii) *Similarly, for any finite closed subscheme* $I \hookrightarrow C$, *the tensor product defines an action on* $\mathrm{Sht}_{C,I}^1 \longrightarrow (C - I) \times (C - I)$ *of the group*

$$\mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)_I$$

of rank 1 *vector bundles* $\mathcal{E}$ *on* C *endowed with an isomorphism*

$$\mathcal{E}_{|I} \xrightarrow{\sim} \text{trivial rank 1 bundle on } I.$$

Remarks. –

- The group $\mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)$ acts simply transitively on the geometric fibers of
$$\mathrm{Sht}_C^1 \longrightarrow C \times C\,.$$
- Similarly, the group $\mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)_I$ acts simply transitively on the geometric fibers of
$$\mathrm{Sht}_{C,I}^1 \longrightarrow (C - I) \times (C - I)\,.$$

Drinfeld's geometric "meaningful realization" of abelian fundamental groups of curves:

Let K be the field of rational functions of C
and $\overline{c} = \mathrm{Spec}(\overline{K})$ be a geometric point of C defined by $K \subset \overline{K}$.

Proposition. –

(i) *The morphism defined by the cover* $\mathrm{Sht}^1_C \longrightarrow C \times C$

$$\pi_1(C \times C, \overline{c} \times \overline{c}) \longrightarrow \mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)$$

canonically factorises through a morphism

$$\pi_1(C, \overline{c})^{\mathrm{ab}} \times \pi_1(C, \overline{c})^{\mathrm{ab}} \longrightarrow \widehat{\mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)} \quad (= \textit{profinite completion})$$

whose two components are related by the isomorphism $g \longmapsto g^{-1}$.

(ii) *Similarly, for any finite closed subscheme* $I \hookrightarrow C$
the morphism defined by the cover $\mathrm{Sht}^1_{C,I} \longrightarrow (C - I) \times (C - I)$

$$\pi_1((C - I) \times (C - I), \overline{c} \times \overline{c}) \longrightarrow \mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)_I$$

canonically factorises through a morphism

$$\pi_1(C - I, \overline{c})^{\mathrm{ab}} \times \pi_1(C - I, \overline{c})^{\mathrm{ab}} \longrightarrow \widehat{\mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)_I}$$

whose two components are related by $g \mapsto g^{-1}$.

The class field isomorphism revisited by Drinfeld:

We still denote K the function field of C,
and $\overline{c}$ is the geometric point defined by an algebraic closure $K \subseteq \overline{K}$.

Lemma. – *There is a canonical isomorphism*

$$\mathrm{Aut}(\overline{K}/K) \xrightarrow{\sim} \varprojlim_{I} \pi_1(C - I, \overline{c})$$

and a fortiori

$$\mathrm{Aut}(\overline{K}/K)^{\mathrm{ab}} \xrightarrow{\sim} \varprojlim_{I} \pi_1(C - I, \overline{c})^{\mathrm{ab}} .$$

Lemma (which comes back to André Weil). –
There is canonical isomorphism

$$\mathbb{A}_K^{\times}/K^{\times} \xrightarrow{\sim} \varprojlim_{I} \mathrm{Pic}_{C/\mathbb{F}_q}(\mathbb{F}_q)_I .$$

Theorem. – *The induced morphism*

$$\mathrm{Aut}(\overline{K}/K)^{\mathrm{ab}} \longrightarrow (\widehat{\mathbb{A}_K^{\times}/K^{\times}})$$

is an isomorphism.
It is none other than the "class field isomorphism".

Drinfeld's moduli of rank r "shtukas":

We keep on considering a smooth projective curve C over $\mathbb{F}_q$.

Definition. – *Consider a scheme S over $\mathbb{F}_q$ and two morphisms $0, \infty : S \to C$ whose graphs are denoted $\Gamma_0 \hookrightarrow S \times C$ and $\Gamma_\infty \hookrightarrow S \times C$.*

(i) *A rank r "shtuka" over S of zero 0 and pole ∞ is a rank r vector bundle $\mathcal{E}$ on $S \times C$ endowed with an isomorphism well-defined on $S \times C - (\Gamma_0 \cup \Gamma_\infty)$*

$$(\mathrm{Fr}_S \times \mathrm{id}_C)^* \mathcal{E} \xrightarrow{\sim} \mathcal{E}$$

which has a simple "zero" on Γ_0 and a simple "pole" on Γ_∞.

(ii) *If $I \hookrightarrow C$ is a finite closed subscheme and $\infty, 0$ take values in $C - I$, a "level I structure" on such a rank r shtuka is an isomorphism*

$$\mathcal{E}_{|S \times I} \xrightarrow{\sim} \text{trivial rank } r \text{ vector bundle on } S \times I$$

which is compatible with $(\mathrm{Fr}_S \times \mathrm{id}_I)^* \mathcal{E}_{|S \times I} \xrightarrow{\sim} \mathcal{E}_{|S \times I}$.

Moduli schemes of rank r "shtukas":

Theorem (stated in a simplified essentially correct form). –

(i) *The presheaf*

$$\begin{array}{ccc} (\mathrm{Sch}/C \times C)^{\mathrm{op}} & \longrightarrow & \mathrm{Set}, \\ (S \xrightarrow{(0,\infty)} C \times C) & \longmapsto & \left\{ \begin{array}{c} \textit{set of isomorphism classes} \\ \textit{of } \underline{\textit{rank } r \textit{ shtukas}} \textit{ over } S \\ \textit{of zero } 0 \textit{ and pole } \infty \end{array} \right\} \end{array}$$

is *representable* *by a (locally finitely presentable) scheme over* $C \times C$

$$\mathrm{Sht}_C^r \longrightarrow C \times C$$

which is *smooth of relative dimension* $2r$.

(ii) *Similarly, for any* *finite closed subscheme* $I \hookrightarrow C$,
the presheaf of *rank r shtukas endowed with a level I structure*
is *representable* *by a (locally finitely presentable) scheme*

$$\mathrm{Sht}_{C,I}^r \longrightarrow (C - I) \times (C - I)$$

which is *smooth of relative dimension* $2r$.

Actions of Hecke correspondences:

Proposition. –
For any finite closed subscheme $I \hookrightarrow C$, the moduli scheme

$$\mathrm{Sht}^r_{C,I} \longrightarrow (C - I) \times (C - I)$$

is endowed with a natural action by correspondences
of the Hecke algebra

$$\mathcal{H}^r_I$$

of compactly supported functions

$$\mathrm{GL}_r(\mathbb{A}_K) \longrightarrow \mathbb{Q}$$

which are invariant on both sides
by some compact open subgroup

$$H_I \hookrightarrow \mathrm{GL}_r(\mathbb{A}_K)$$

defined by $I \hookrightarrow C$.

Remark. –
The multiplication law on $\mathcal{H}^r_I$ is defined
by convolution relatively to an invariant measure on $\mathrm{GL}_r(\mathbb{A}_K)$.

Induced actions on ℓ-adic cohomology spaces:

We still consider a geometric point $\overline{c}$ of C defined by an algebraic closure $\overline{K} \supset K$ of the function field K of C.

Proposition. –
For any finite closed subscheme $I \hookrightarrow C$, the ℓ-adic cohomology spaces

$$H^i(\mathrm{Sht}^r_{C,I} \times_{(C-I)\times(C-I)} (\overline{c},\overline{c}), \mathbb{Q}_\ell)$$

are canonically endowed with commuting actions of

- *the square profinite group*

$$\pi_1(C-I,\overline{c}) \times \pi_1(C-I,\overline{c}),$$

- *the Hecke algebra*

$$\mathcal{H}^r_I = \{\textit{compactly supported functions} \quad H_I\backslash \mathrm{GL}_r(\mathbb{A}_K)/H_I \to \mathbb{Q}\}$$

A cohomological realization of Langland's correspondence:

Theorem. –

(i) *The colimits of cohomology spaces*

$$\varinjlim_{I \hookrightarrow C} H^i(\mathrm{Sht}^r_{C,I} \times_{(C-I)\times(C-I)} (\overline{c},\overline{c}), \mathbb{Q}_\ell)$$

are canonically endowed with commuting actions of

- *the square profinite group*
$$\mathrm{Aut}(\overline{K}/K) \times \mathrm{Aut}(\overline{K}/K)\,,$$
- *the Hecke algebra*
$$\varinjlim_{I \hookrightarrow C} \mathcal{H}^r_I = \mathcal{H}^r = \left\{ \begin{array}{c} \textit{convolution algebra of} \\ \textit{compactly supported locally constant} \\ \textit{functions} \quad \mathrm{GL}_r(\mathbb{A}_K) \to \mathbb{Q} \end{array} \right\}.$$

(ii) *In middle degree $i = 2r$,*
there appear irreducible components of the form $\sigma \otimes \check{\sigma} \otimes \pi$ *where*

- $\sigma =$ *irreducible ℓ-adic representation of* $\mathrm{Aut}(\overline{K}/K)$ *of dimension r,*
- $\check{\sigma} =$ *dual representation,*
- $\pi =$ *irreducible representation of $\mathcal{H}^r$*
which is "automorphic" in the sense that
it can be realized in a space of functions on $\mathrm{GL}_r(\mathbb{A}_K)/\mathrm{GL}_r(K)$,
- σ *and* π *are related by a precise rule predicted by Langlands.*

Concluding remarks:

- In the case of the function field K of a curve C over $\mathbb{F}_q$, the whole geometric and cohomological construction can be generalized from linear groups GL_r to arbitrary (quasi-split) reductive groups G over K, realizing Langland's correspondence

$$\left\{ \begin{array}{c} \text{“irreducible” morphisms} \\ \mathrm{Aut}(\overline{K}/K) \to \check{G}(\overline{\mathbb{Q}}_\ell) \\ \text{for } \check{G} = \text{“dual” group of } G \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{irreducible representations} \\ \text{of the convolution algebra of} \\ G(\mathbb{A}_K) \\ \text{which are “automorphic”,} \\ \text{i.e. can be realized in spaces of} \\ \text{functions on } G(\mathbb{A}_K)/G(K) \end{array} \right\}.$$

- In the case $K \supseteq \mathbb{Q}$ is a number field, an analoguous geometric and cohomological construction is possible only for some number fields K and some reductive groups closely related to $S_{p_{2r}}$. The moduli schemes of Drinfeld shtukas are replaced by
  "Shimura varieties"
  which classify "abelian varieties"
  endowed with different types of extra structures.