

# Non-linearity, fundamental groups, and Diophantine geometry

June 12, 2006

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



From 50's to 80's applications of topology to arithmetic came primarily from *homology*:

- Basic language of homological algebra;
- Arithmetic cohomology theories.

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.

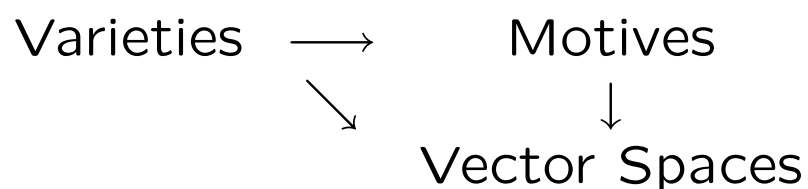
- $H_{DR}^i(X) = H^i(X, \Omega_X^\bullet)$ : The algebraic De Rham cohomology of  $X$ .

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

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’:



A focal point of this lecture: In the homological approach, main ideas and techniques are *linear*.

Important contrast:

Linear  $\leftrightarrow$  Non-linear

In topology,

Homology  $\leftrightarrow$  Homotopy

But also, the linear theory provides input into the non-linear theory via linearization.

Topological version,

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

However, one expects a fully non-linear theory, when fully understood, to be more powerful than a linearized version.

The techniques of homotopy as applied to arithmetic should yield information not accessible to homology.

Homology  $\longrightarrow$  study of L-functions.

Homotopy  $\longrightarrow$  study of Diophantine sets.

Note: L-functions also yield information about Diophantine sets. But actually, linearized Diophantine sets. For example, might be interested in

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

the set of rational points. But L-functions give information on something like  $\mathbb{Z}[X(\mathbb{Q})]$ .

Cannot yield, in any obvious way, Faltings' theorem (Mordell conjecture), for example.

Classically, a basic ‘homological’ construction used in Diophantine geometry of a hyperbolic curve  $X$  is the *Jacobian*  $J_X$ . A very linear-object:

$$J_X :=$$

(Free abelian group generated by  $X$ )/(eq. rel.)

Itself an abelian group variety. Parametrizes line-bundles on  $X$ .

Homological nature: Over  $\mathbb{C}$

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

If we fix a base-point  $x \in X$ , can map the curve into the Jacobian

$$X \rightarrow J_X$$
$$y \mapsto [x - y]$$

Thereby, we can view  $X$  as parametrizing line bundles on itself.

Ends up being a key idea: parametrizing other geometric objects using points of  $X$ .

Note: Can also express this map using abelian integrals.

Weil tried to use this parametrization to prove the Mordell conjecture. Doesn't quite work because  $J$  has too many points: also related to linearity.

The eventual proof of Mordell conjecture involves a non-linear parametrization. A family of curves (Kodaira-Parshin construction):

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

Somewhat ad hoc. Desirable to have a non-linear version of Weil's construction.

The idea of using homotopy in this regard stems in part from Grothendieck's 'anabelian' philosophy. Specifically, the *section conjecture*.

Main point: Relates  $X(\mathbb{Q})$  to the pro-finite fundamental group.

In fact, it turns out there is a non-linear Albanese map

$X \rightarrow$ classifying space

$$y \mapsto [\pi_1(X; x, y)]$$

Actual object involved is the De Rham fundamental group (Chen, Hain, Morgan, . . .).

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

Unipotent completion of usual fundamental group.

Obtained by taking complex linear combinations  $\sum c_l[l]$  of paths and regarding two such as equivalent if they have the same ‘parallel transport’ action on vector bundles with unipotent connection.

Actually a pro-algebraic group. Each quotient

$$Z^{n+1} \backslash \pi_1^{DR}(X, x)$$

by a subgroup in the descending central series is a finite-dimensional unipotent algebraic group.

Can also construct De Rham path spaces

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

which are *torsors* for  $\pi_1^{DR}(X, x)$ .

These groups and path spaces have a Hodge filtration

$$\pi_1^{DR}(X; x, y) \cdots \supset F^{-2} \supset F^{-1} \supset F^0$$

and an integral lattice  $L_y \subset \pi_1^{DR}(X; x, y)$  coming from the image of the topological paths. The torsor structure is compatible with the extra structures. These torsors end up being classified by

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

Non-linear Albanese map (Hain)

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

is given by

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

Note: The ‘abelianization’ gives us the usual Albanese map:

$$y \mapsto [Z^2 \backslash \pi_1^{DR}(X; x, y)]$$

The most important point for Diophantine applications is that one can use this map to pull natural functions back from the classifying space to  $X$ .

For example, when  $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ , the algebraic functions on  $\pi_1^{DR}(X, x)/F^0$  form a vector space

$$\mathbb{C}[\alpha_w]$$

spanned by functions  $\alpha_w$ , indexed by words  $w$  in a two letter alphabet  $\{A, B\}$ . The function  $\alpha_w$  corresponding to the word

$$w = A^{k_1-1} B A^{k_2-1} B \dots A^{k_m-1} B$$

gives rise to the function

$$L_w(z) = \sum_{n_1 > n_2 > \dots > n_m} \frac{z^{n_1}}{n_1^{k_1} \dots n_m^{k_m}},$$

a *multiple polylogarithm*. Ubiquitous in arithmetic, geometry, and physics.

More generally, the non-linear Albanese map can be expressed using iterated integrals.

For arithmetic applications, need a  $p$ -adic version of the construction above: Theory of the crystalline fundamental group and  $p$ -adic Hodge theory. Leads to  $p$ -adic multiple polylogarithms and  $p$ -adic iterated integrals. Important distinction from the archimedean theory is that the functions we end up with are single-valued.

In the case of  $X = \mathbf{P}^1 \setminus \{0, 1, \infty\}$ , applies to the finiteness of  $X(\mathbb{Z}[1/S])$  the set of  $S$ -integers. (Theorem of Siegel.)

Theorem: On  $X(\mathbb{Z}_p)$  there exists a non-trivial linear combination

$$\sum_w c_w P_w$$

of  $p$ -adic multiple polylogarithms that vanishes on

$$X(\mathbb{Z}[1/S]) \subset X(\mathbb{Z}_p).$$

For compact curves of higher genus, reduces Faltings theorem to conjectures of Beilinson.

These results come from the theory of the motivic fundamental group (Deligne) and 'linearization'.

Linearization:

$$0 \rightarrow Z^n / Z^{n+1} \rightarrow \pi_1^M / Z^{n+1} \rightarrow \pi_1^M / Z^n \rightarrow 0$$

Use of the motivic fundamental group:

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

Perhaps can view as a partial vindication of Grothendieck's 'anabelian' vision. Especially mysterious in that the anabelian philosophy gets connected in the process to the theory of (mixed) motives.