# Fundamental groups, principal bundles, and rational points

**Minhyong Kim**

**27 March, 2008**

**Bangalore**

Main goal:

Construct non-abelian analogue of the Jacobian that can be used to study the Diophantine geometry of hyperbolic curves, i.e., curves that are uniformized by the upper half-plane.

I. Jacobians

II. Some non-abelian constructions

III. The non-abelian Albanese map: profinite version

IV. The unipotent Albanese map and Selmer varieties

V. The non-abelian method of Chabauty (and Weil-Lang)

VI. The Coates-Wiles connection

I. **The Jacobian**

$E/\mathbb{Q}$ elliptic curve has group law determined as follows:

Fix one point $b \in E(\mathbb{Q})$ as the origin. For any $P$, $Q$, there exists a rational function with zeros exactly at $P$ and $Q$ and one pole at $b$. $P + Q$ is defined to be the other pole.

$X/\mathbb{Q}$, a hyperbolic curve of genus $g$ and $b \in X$.

Can try to generalize the previous discussion in a formal way by defining

$$Pic_X = \mathbb{Z}[X]/(\text{geometric equivalence relation } R)$$

$R: \quad \Sigma_i[P_i] \sim \Sigma_i[Q_i] \Leftrightarrow$ there exists a rational function whose zeros are exactly the $\{P_i\}$ and whose poles are the $\{Q_i\}$.

This relation is quite complicated in general.

For genus one, reduces to relation between points on the curve: $\Sigma_{i=1}^{n} P_i \sim (n-1)[b] + [Q]$ for unique $Q \in E$.

Group law accounted for by the topology of a torus:

$$X(\mathbb{C}) = \mathbb{C}/\Lambda$$

where $\Lambda \subset \mathbb{C}$ is a lattice.

For higher degree equations, sum of two points will no longer be on the curve. No group law, because of the fact that $X(\mathbb{C})$ is a Riemann surface of higher genus.

But another geometric structure underlies this construction:

For $n \geq g$,

$$\Sigma_{i=1}^{n}[P_i] \sim \Sigma_{i=1}^{g}[Q_i] + (n-g)[b]$$

for $Q_i$ unique most of the time.

Define the Jacobian:

$$J_X = \mathbb{Z}[X]_0/R$$

$$\mathbb{Z}[X]_0 = \{\Sigma n_P[P] \mid \Sigma n_P = 0\}$$

Then we can write

$$Pic_X = J_X \times \mathbb{Z}$$

corresponding to

$$\Sigma_{i=1}^{n}[P_i] = \Sigma_{i=1}^{n}([P_i] - [b]) + n[b]$$

and the assertion is that

$$J_X \sim Sym^g(X)$$

Reflects the status of $J_X$ as a kind of *abelianization* of $X$, a notion figuring prominently in the theory of motives.

What we have described is the *Chow construction* of the Jacobian.

There is an associated *Albanese map*:

$$X \longrightarrow J_X$$

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

that ends up being an embedding.

Hodge-theory construction:

$$J_X(\mathbb{C}) = H_1(X(\mathbb{C}), \mathbb{Z}) \backslash H^0(X(\mathbb{C}), \Omega_{X(\mathbb{C})})^*$$

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

$$= \mathrm{Ext}^1_{MHS,\mathbb{Z}}(\mathbb{Z}, H_1(X(\mathbb{C}), \mathbb{Z}))$$

as extensions in the category of mixed Hodge structures.

[Hodge-realization of the *motivic construction*.]

Albanese map:

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

$$x \mapsto$$

$$[0 \to H_1(X(\mathbb{C}), \mathbb{Z}) \to H_1(X(\mathbb{C}), \{b, x\}; \mathbb{Z}) \to \mathbb{Z} \to 0]$$

Topological construction:

$$J_X = \mathrm{Hom}(\pi_1(X(\mathbb{C}), b), S^1) = \mathrm{Hom}(H_1(X(\mathbb{C}), \mathbb{Z}), S^1)$$

$$= H^1(X(\mathbb{C}), S^1)$$

as unitary characters of the fundamental group of $X(\mathbb{C})$.

Albanese map is not apparent.

Significance of Chow construction: Weil's *algebraic* theory of $J_X$ as a projective algebraic variety.

$$J_X \sim Sym^g(X)$$

In particular,

$X$ defined over $\mathbb{Q} \Rightarrow J_X$ defined over $\mathbb{Q}$.

Importantly, if $b \in X(\mathbb{Q})$, then

$$i_b : X \hookrightarrow J_X$$

is defined over $\mathbb{Q}$.

Thereby,

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

and one might attempt to study the structure of $X(\mathbb{Q})$ *using* $J_X(\mathbb{Q})$. Weil's main motivation for algebraic construction.

In fact, $J_X(\mathbb{Q})$ is a finitely-generated abelian group.

Frequently infinite, because of group structure. But points of $J_X$ are usually not points of $X$. Cannot be used to generate points on $X$.

Mordell's conjecture: $X$ has at most finitely many rational points.

Proved in 80's by Faltings.

From our perspective, an arithmetic manifestation of incompatibility of group law on $J_X$ with complicated topology of $X$. Weil had attempted in his thesis to implement this idea directly to prove Mordell's conjecture (without success).

Made precise in Lang's conjecture:

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

is finite for any finitely generated subgroup of $J_X(\mathbb{C})$.

Of course would imply Mordell's conjecture, but this approach was only implemented under the assumption

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

by Chabauty.

In general, abelian group structure of $J_X$ appears to be an intrinsic obstruction to extracting information about the points of $X$.

More abstractly, problem is the abelian nature of the category of motives reflecting the properties of homology. So, even in the best of possible worlds (i.e., where all conjectures are theorems), the category of motives misses out on fundamental objects of arithmetic, i.e., sets

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

Can attempt to replace $J_X$ (or category of motives) by a more refined object (or category).

## II. Non-abelian constructions and vector bundles

Weil 1938: 'Generalization of abelian functions'.

'A paper about geometry disguised as a paper about analysis whose motivation is arithmetic' (Serre).

Stresses importance of developing 'non-abelian mathematics' with a key role for non-abelian fundamental groups.

Clearly motivated by the Mordell conjecture and the attendant need for a 'non-abelian Jacobian.'

Chow construction has no natural non-abelian analogue.

But there is another algebro-geometric interpretation. The *line bundle construction*:

$J_X$ is the moduli space of line bundles of degree zero on $X(\mathbb{C})$.

This interpretation can also be viewed as a consequence of mildly non-linear Hodge theory.

$$H^1(X(\mathbb{C}),\mathbb{R}) \hookrightarrow H^1(X(\mathbb{C}),\mathbb{C}) \to H^1(X(\mathbb{C}),\mathcal{O}_X)$$

induces isomorphisms

$$H^1(X(\mathbb{C}),\mathbb{R}) \simeq H^1(X(\mathbb{C}),\mathcal{O}_X)$$

and

$$H^1(X(\mathbb{C}),S^1) \simeq H^1(X(\mathbb{C}),\mathcal{O}_X^*)_0$$

Line bundle construction of Jacobian much better than Chow construction for considering non-abelian analogue:

line bundle $\longrightarrow$ vector bundle

Weil's generalized the Hodge-theoretic correspondence to vector bundles, leading eventually to work Narasimhan-Seshadri, Simpson, etc., referred to as *non-abelian Hodge theory*.

For example, the theorem of N-S:

irreducible unitary representations of $\pi_1 \leftrightarrow$ stable vector bundles of degree zero on $X(\mathbb{C})$.

The N-S theorem unifies two desiderata:

-Relevance of $\pi_1$;

-construction of an object defined over $\mathbb{Q}$: moduli space $M(n,0)$ of vector bundles on a curve.

That is, theory of vector bundles *is* a theory of fundamental groups over $\mathbb{Q}$:

*function-theoretic refinement* of the Jacobian.

**However** loss of Albanese map:

$$x \mapsto \mathcal{O}_X((x) - (b))$$

No natural way to associate a vector bundle to a point.

[Challenge for bundle-theorists.]

One needn't algebraize geometrically. *Topological refinement* provides another way to define fundamental groups over $\mathbb{Q}$:

In fact, it is Grothendieck's theory of the *étale fundamental group* that leads to a good theory of *non-abelian Albanese maps*.

## III. The non-abelian Albanese map: profinite version

Elementary idea:

$$i_b^{na}(x) := [\pi_1(X; b, x)]$$

where the image runs over a classifying space.

A classifying space of *principal bundles* for the fundamental group.

That is, $\pi_1(X; b, x)$ is a principal bundle for $\pi_1(X, b)$:

-action by composition

$$\pi_1(X; b, x) \times \pi_1(X; b) \to \pi_1(X; b, x);$$

-choice of an path $p \in \pi_1(X; b, x)$ determines a bijection

$$\pi_1(X; b) \simeq \pi_1(X; b, x)$$

$$l \mapsto p \circ l$$

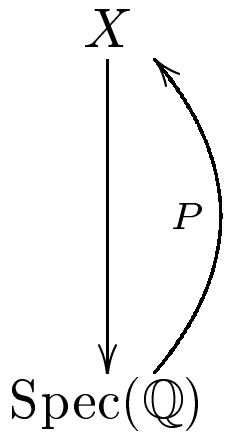
$\pi_1(X; b, x)$ is a principal bundle over a point, and hence, trivial.

Grothendieck's theories allow us to enrich points in various ways:

$$\mathrm{Spec}(\mathbb{Q})$$

Function-theoretic enrichment of a point.

Using this, can distinguish rational points from generic points:



Topological enrichment: The étale topology.

Spaces like $\mathrm{Spec}(\mathbb{Q})$ or $\mathrm{Spec}(\mathbb{Z})$ are endowed now with very non-trivial topologies that go beyond scheme theory.

Open sets are *étale maps* between schemes: proper finite-to-one maps with surjective tangent map.

The connected étale coverings of $\mathrm{Spec}(\mathbb{Q})$ are maps

$$\mathrm{Spec}(F) \to \mathrm{Spec}(\mathbb{Q}),$$

where $F$ is a finite (separable) field extension of $\mathbb{Q}$.

Pro-finite sheaves on $\mathrm{Spec}(\mathbb{Q})$ canonically identified with pro-finite sets carrying continuous action of

$$G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

via

$$\mathcal{L} \mapsto \varinjlim_{F} \mathcal{L}(\mathrm{Spec}(F))$$

Sheaf (co)homology for the étale topology rather well-known, with numerous applications: Weil conjectures, Faltings' theorem, Wiles theorem, etc.

Grothendieck's exotic topologies also lead to interesting *homotopy* groups and principal bundles.

The universal pointed covering space

$$(\tilde{X}(\mathbb{C}), \tilde{b}) \to (X(\mathbb{C}), b)$$

is a principal $\pi_1(X; b)$-bundle over $X(\mathbb{C})$. This specializes to the $\pi_1(X; b, x)$:

$$\tilde{X}_b \simeq \pi_1(X; b)$$

and

$$\tilde{X}_x \simeq \pi_1(X; b, x)$$

via lifting of paths.

Important fact: Homotopy classes of paths are realized as the fibers of the universal covering space.

But

$$\tilde{X}(\mathbb{C}) \to X(\mathbb{C})$$

can be *approximated* by systems of finite covers

$$X_i(\mathbb{C}) \to X(\mathbb{C})$$

consisting of map of algebraic varieties.

Example:

$$\exp(2\pi i(\cdot)) : \mathbb{C} \to \mathbb{C}^*$$

is approximated by

$$(\cdot)^n : \mathbb{C}^* \to \mathbb{C}^*$$

Note that the approximating system is *defined over* $\mathbb{Q}$.

Similarly,

$$\mathcal{P} : \mathbb{C} \to E(\mathbb{C})$$

can be approximated by

$$[n] : E \to E$$

Even in general, there is a system

$$(\tilde{X}^{et}, b^{et}) = \{(X_i, b_i)\}$$

that can be defined over $\mathbb{Q}$, and viewed as an arithmetic universal covering space.

[In this assertion, we are using the rationality of the base-point.]

The fiber $\tilde{X}_b^{et}$ now consists of systems of algebraic ($\bar{\mathbb{Q}}$) points, that are acted on by $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Still has the structure of a *pro-finite* group, the étale fundamental group

$$\pi_1^{et}(\bar{X}, b) := \tilde{X}_b^{et}$$

For any other point $x \in X(\mathbb{Q})$,

$$\pi_1^{et}(\bar{X}; b, x) := \tilde{X}_x^{et}$$

also consists of algebraic points, and is a pro-finite principal bundle for $\pi_1^{et}(\bar{X}, b)$.

The group and principal bundle carry compatible Galois actions reflecting the fact that there are sheaves

$$b^*(\tilde{X}^{et})$$

and

$$x^*(\tilde{X}^{et})$$

on $\mathrm{Spec}(\mathbb{Q})$ underlying these sets.

[Recall:

$$b, x : \mathrm{Spec}(\mathbb{Q}) \to X$$

]

Thus we get an arithmetic Albanese map

$$X(\mathbb{Q}) \to H^1(G, \pi_1^{et}(\bar{X}, b))$$

$$x \mapsto [\pi_1^{et}(\bar{X}; b, x)]$$

where the target is a classifying space for principal $\pi_1^{et}(\bar{X}; b)$-bundles on the étale topology of $\mathrm{Spec}(\mathbb{Q})$.

For curves of genus $\geq 1$, this map is injective!

## IV. The unipotent Albanese map and Selmer varieties

The profinite version of the non-abelian Albanese map is difficult to study, because geometry has been entirely removed. Only profinite topology remains.

Can reinsert geometry at the level of 'coefficients' for the non-abelian cohomology by replacing the fundamental groups by suitable algebraic completions. Of course

Geometry of the base field vs. geometry of coefficients

is an important theme in arithmetic geometry.

$\Gamma$ finitely-generated discrete group. $\mathbb{C}[\Gamma]$ group algebra.

$$\Delta : \mathbb{C}[\Gamma] \to \mathbb{C}[\Gamma] \otimes \mathbb{C}[\Gamma]$$

induced by

$$\gamma \mapsto \gamma \otimes \gamma$$

for $\gamma \in \Gamma$. Then, in fact,

$$\Gamma = \{f \in \mathbb{C}[\Gamma] : \Delta(f) = f \otimes f\}$$

i.e., $\Gamma$ is the set of 'group-like elements' in the Hopf algebra $\mathbb{C}[\Gamma]$.

But can consider the formally completed group algebra

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

where $I \subset \mathbb{C}[\Gamma]$ is the augmentation ideal.

Then we get more group-like elements, e.g.,

$$\exp(\lambda \log(\gamma))$$

for $\gamma \in \Gamma$ and $\lambda \in \mathbb{C}$.

The $\mathbb{C}$-*pro-unipotent completion* $\Gamma^u$ of $\Gamma$ is the set of group-like elements in $\mathbb{C}[[\Gamma]]$.

Thereby arrive at a more structured object:

$\Gamma^u$ is a pro-algebraic group.

$\Gamma^u_n := \Gamma^u/(\Gamma^u)^{(n)}$ is an algebraic group for each $n$.

Can do this to the fundamental group:

$$\pi_1(X(\mathbb{C}), b) \to \pi_1^u(X(\mathbb{C}), b)$$

getting the group generated by the holonomy of all unipotent connections on $X(\mathbb{C})$.

[Vector bundles lie in the background in the Tannakian approach.]

Also have 'unipotent principal bundle of paths'

$$\pi_1^u(X(\mathbb{C}); b, x)$$

obtained by push-out:

$$\pi_1(X(\mathbb{C}); b, x) \times_{\pi_1(X(\mathbb{C}), b)} \pi_1^u(X(\mathbb{C}), b)$$

Can carry out same construction for the étale fundamental group and the completed group ring

$$\mathbb{Q}_p[[\pi_1^{et}(\bar{X}, b)]]$$

to arrive at the $\mathbb{Q}_p$-pro-unipotent étale fundamental group:

$$\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)$$

The previous classifying space gets replaced by

$$H^1(G, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b))$$

Further refinement:

$S$: set of primes of bad reduction for $X$.

$X(\mathbb{Z}_S)$:set of points in the ring $\mathbb{Z}_S$ of $S$-integers. (If $X$ is compact, then the integral points are the same as rational points.)

The map

$$X(\mathbb{Q}) \to H^1(G, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b))$$

$$x \mapsto [\pi_1^{u,\mathbb{Q}_p}(\bar{X}; b, x)],$$

when restricted to the integral points, factors through a natural subspace

$$X(\mathbb{Z}_S) \longrightarrow H^1_f(G, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)) \subset H^1(G, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b))$$

corresponding to local conditions satisfied by the torsors $\pi_1^{u,\mathbb{Q}_p}(\bar{X}; b, x)$, such as being unramified away from the primes of bad reduction and $p$, and being crystalline at $p$.

[The geometry of the situation allows extension of sheaves $x^*\tilde{X}$ to $\mathrm{Spec}(\mathbb{Z}_T)$, $T = S \cup \{p\}$.]

Last condition arises from the *p-adic Hodge theory* of

$$X \times_{\mathrm{Spec}(\mathbb{Q})} \mathrm{Spec}(\mathbb{Q}_p)$$

Such a condition is probably meaningless for $H^1(G, \pi_1^{et}(\bar{X}, b))$.

The advantage of considering them in the unipotent setting is that the subspace

$$H^1_f(G, \pi_1^{u,\mathbb{Q}_p}(\bar{X}, b))$$

becomes canonically equipped with the structure of a pro-algebraic variety:

*The Selmer variety.*

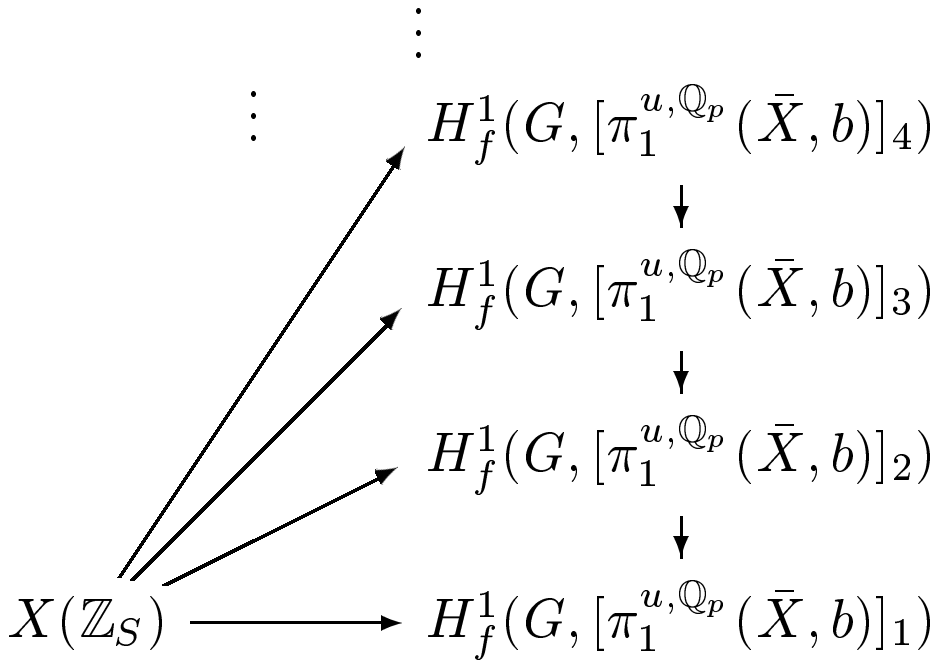
There are finite-dimensional quotients

$$H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

obtained by considering quotients modulo the descending central series.

A moduli space of principal bundles!

In fact, a tower of moduli spaces and maps:




refining the map at the bottom (which has a classical interpretation in Kummer theory).

End up with diagrams:

$$\begin{array}{ccc} X(\mathbb{Z}_S) & \longrightarrow & X(\mathbb{Z}_p) \\ \downarrow & & \downarrow \\ H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) & \longrightarrow & H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) \end{array}$$

involving a local version of the classifying space on the lower right hand corner, with $G_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$.

Vertical maps are all of the form

$$x \mapsto [\pi_1^{u,\mathbb{Q}_p}(\bar{X}; b, x)]$$

obtained from the previous one by pushing out principal bundles. The *unipotent Albanese map.*

The local classifying space

$$H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

has the structure of a $p$-adic symmetric space,

$$H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) \simeq U_n^{DR}/F^0$$

and the map

$$X(\mathbb{Z}_p) \to U_n^{DR}/F^0$$

is obtained by $p$-adic iterated integrals.

## V. The non-abelian method of Chabauty (and Weil-Lang)

Dimension hypothesis:

$$\dim H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) < \dim H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

for $n$ sufficiently large.

**Theorem 0.1** *Let $X$ be a curve and suppose*

$$dim H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n) < dim H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

*for some $n$. Then $X(\mathbb{Z}_S)$ is finite.*

Theorem is intimately related to non-abelian nature of the fundamental groups and the corresponding non-linearity of the classifying spaces.

Idea of proof: (1)

$$X(\mathbb{Z}_p) \to H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

is finite-to-one: a purely analytic fact;

(2)

$$Im(X(\mathbb{Z}_p)) \subset H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

is a dense analytic curve. In fact, this is true of every residue disk in $X(\mathbb{Z}_p)$.

(3)

$$Im(H^1_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)) \subset H^1_f(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

lies inside a proper closed subvariety.

(2) and (3) imply that

$$Im(X(\mathbb{Z}_p)) \cap Im(H_f(G, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)) \subset H_f^1(G_p, [\pi_1^{u,\mathbb{Q}_p}(\bar{X}, b)]_n)$$

is finite.

Together with (1), get finiteness of $X(\mathbb{Z}_S)$.

Remark: this strategy is a non-abelian version of Chabauty's method, but could be also be interpreted as a non-Archimedean, non-abelian realization of Weil's and Lang's intuition.

Can use the theorem to prove finiteness of $S-$integral points for

-hyperbolic curves of genus zero;

-elliptic curves with complex multiplication minus the origin (with a modified fundamental group).

The dimension hypothesis for general curves follows from 'structure theory of mixed motives'.

For example,

Fontaine-Mazur conjecture on representations of geometric origin $\Rightarrow$ dimension hypothesis $\Rightarrow$ Faltings' theorem.

**VI. The Coates-Wiles connection**

The constructions are also *non-abelian extensions* of the method of Coates and Wiles.

That is, proofs are an extension of:

Non-vanishing of $L$-function $\Rightarrow$ finitness of Selmer group $\Rightarrow$ finiteness of rational points

that was first carried out by Coates and Wiles.

In fact,

Finiteness of zeros of $p$-adic $L$-function $\Rightarrow$ control of Selmer varieties $\Rightarrow$ finiteness of integral points

in the case of CM elliptic curves.

Precise non-vanishing related to *effectivity*.