Galois Theory and Diophantine geometry

Minhyong Kim

Leicester, October, 2009

1. Some Examples

1.1

A typical Diophantine equation in two variables:

$$y^2 = x^3 - 2.$$

A solution:

$$(\frac{113259286337279}{449455096000})^2 = (\frac{2340922881}{58675600})^3 - 2$$

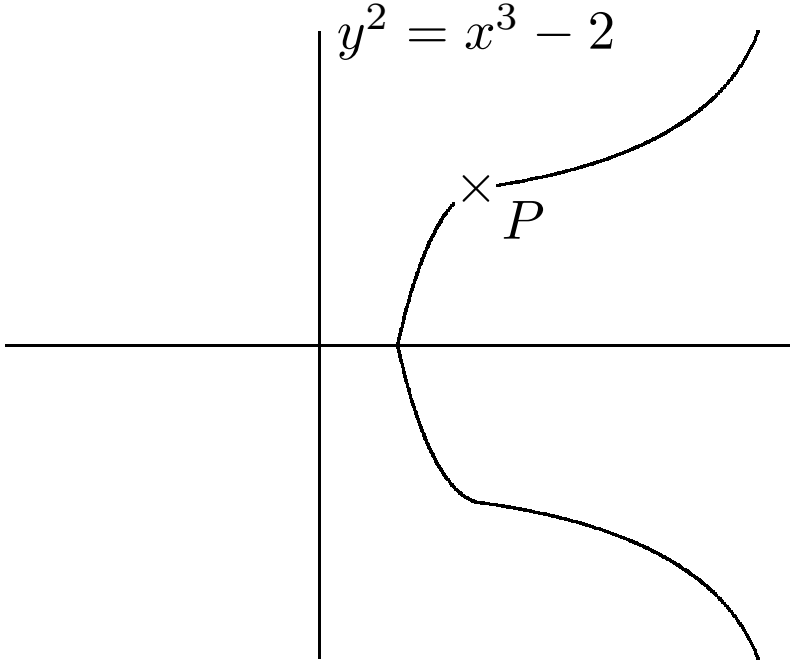
We also refer to the solution as a *point*

$$P = (x, y) = (\frac{2340922881}{58675600}, \frac{1132592863372 79}{449455096000})$$

on the algebraic curve

$$y^2 = x^3 - 2.$$

Picture:



1.2

A typical finiteness theorem in Diophantine geometry:

Let $a, b, c, n \in \mathbb{Z}$ and $n \geq 4$. Then the equation

$$ax^n + by^n = c$$

has at most finitely many rational solutions in (x, y).

General proof due to Faltings.

2. Discussion: The Rising Sea

2.1

A famous theorem of Yuri Matiyasevich indicates that almost any problem of mathematics can be 'encoded' in the theory of Diophantine equations. For example, there is a polynomial

$$h \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$$

with the property that the Riemann hypothesis is true if and only if

$$h(x_1, x_2, \ldots, x_n) = 0$$

has integral solutions. Similar equations can be found for the four-color problem or the Poincare conjecture.

So far, such strange reductions have had no direct impact on the actual resolution of difficult problems outside of arithmetic.

However, it may account in part for

-the astounding diversity of mathematics that intertwines with Diophantine problems: The theorem of Faltings involves Hodge theory and Galois theory, moduli spaces of curves and abelian varieties, metrized line bundles and their curvature.

-the stubborn resistance of Diophantine problems to direct attack. There are indeed few general theorems that can be proved by methods as elementary as their statements.

2.2

Grothendieck: strategy of the rising sea

> Identifying the *relevant structures* in sufficient generality and identifying their *theory* $\longrightarrow$ resolution of Diophantine problems

The suggestion is that 'a sea of structures' will gradually engulf the problem.

3. Some key ideas of Grothendieck

3.1 Scheme Theory (1950's)

Given a polynomial

$$f(x_1, x_2, \ldots, x_n)$$

with coefficients in any ring A, can associate to it the ring

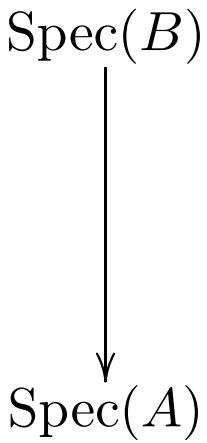
$$B = A[x_1, x_2, \ldots, x_n]/(f)$$

and the space

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

within the framework of a *duality* between rings and spaces.

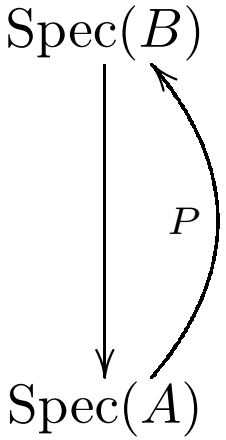
$\mathrm{Spec}(B)$ is fibered over $\mathrm{Spec}(A)$:



in such a way that A-solutions to the equation

$$f(x_1, x_2, \ldots, x_n) = 0$$

correspond to cross sections



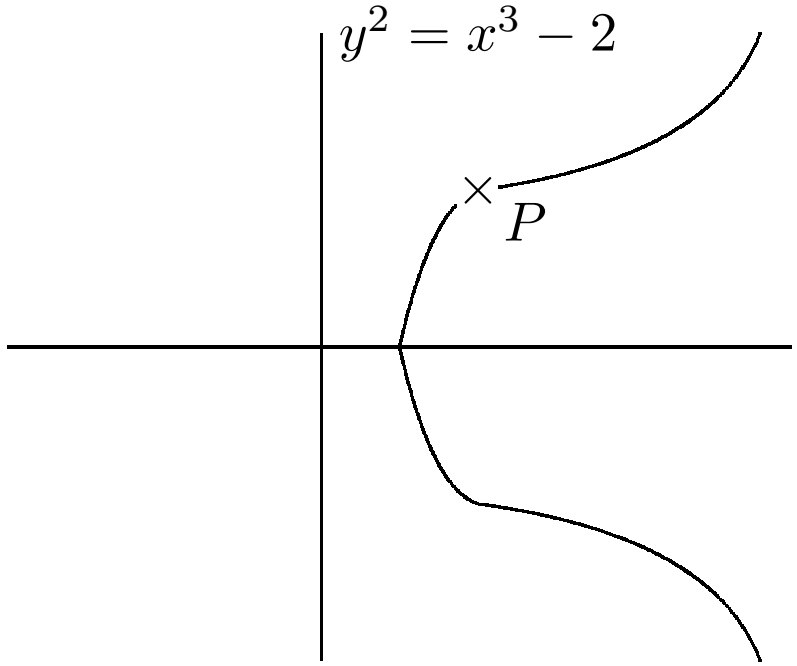
Such an arrow is referred to as a 'point' in scheme theory.

3.1.1 Remark

It is important that even for an equation like

$$y^2 = x^3 - 2,$$

the associated space (=scheme) is not the space



This picture depicts the *real* solutions to the equation and happens to correspond conveniently to everyday visual experience.

The geometry of the scheme is instead determined by *all* potential solutions in *all* rings, like $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}_p, \mathbb{F}_p, \mathbb{Q}[t_1, t_2], \ldots$.

3.2 Generalized topologies (1960's)

Open subset

$$U \subset X$$

is replaced by a map

$$Y \to X$$

Most notions pertinent to subsets can be generalized to maps.
Intersections

$$U_1 \cap U_2 \subset X$$

gets replaced by fiber products

$$Y_1 \times_X Y_2.$$

Coverings

$$\cup_i U_i = X$$

by a surjective collection of maps

$$\coprod_i Y_i \to X.$$

Can formulate a small collection of conditions on such maps, similar to the axioms for subsets, that give rise to a reasonable notion of topology.

Best known, and most successful, is the *étale topology*, where the 'open sets' are algebraic analogues of local homeomorphisms. These algebraic analogues exist because the property of being a local homeomorphism has a function-theoretic formulation (in terms of differentials), which can then be transplanted to scheme theory.

3.2.1 Example

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

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

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

-For $\mathrm{Spec}(\mathbb{Z})$, one can construct an open covering using the two maps

$$\mathrm{Spec}(\mathbb{Z}[i][1/2]) \to \mathrm{Spec}(\mathbb{Z})$$

and

$$\mathrm{Spec}(\mathbb{Z}[(1+\sqrt{-7})/2][1/7]) \to \mathrm{Spec}(\mathbb{Z}).$$

This formulation of point-set topology contains the ingredients for algebraic topology:

Combinatorics of coverings $\longrightarrow$ (co)homology

which, amazingly, connects to refined information about equations.

3.2.2 Equations over finite fields

$$f \in \mathbb{Z}[x, y]$$

$N_d(p)$: number of solutions to equation

$$f(x, y) = 0$$

in the finite field $\mathbb{F}_{p^d}$.

There is a remarkable pattern in the way this number varies with d.

3.2.2.1 Example

Consider

$$y^2 = x^3 - 2$$

in the fields $\mathbb{F}_{3^d}$. For $d = 1$, we get

$$N_1(3) = 3$$

and for general d,

$$N_d(3) = 3^d + (\sqrt{3})^d + (-\sqrt{3})^d.$$

For general f and prime p, can find algebraic numbers

$$\alpha_1, \alpha_2, \ldots, \alpha_m$$

with the property that

$$N_d(p) = p^d + \alpha_1^d + \alpha_2^d + \cdots + \alpha_m^d.$$

Such phenomena are ultimately explained by *étale cohomology.*

In the formula for $N_d(p)$, the term p^d is the contribution of H_c^2 and the term $\alpha_1^d + \alpha_2^d + \cdots + \alpha_m^d$ comes from H_c^1.

3.2.2.2 Example

For projective n-space $\mathbf{P}^n$, we have the formula

$$N_d(p) = 1 + p^d + p^{2d} + \cdots + p^{nd},$$

where p^{id} is accounted for by H^{2i}.

3.2.3 Remark:

Starting with $f(x, y) \in \mathbb{Z}[x, y]$, one can ask about the variation of say, $N_1(p)$ with p. This is at present a much more difficult and tantalizing problem, cases of which are included in the recent proof of the Sato-Tate conjecture. The patterns there are never precise, and touch upon the deepest questions in number theory.

The variation in p is often referred to as the *horizontal variation*, as opposed to the vertical variation in d for a fixed p.

3.3 Anabelian geometry (1980's)

Emphasis on *higher-dimensional algebra* and *non-abelian* structures, in particular, *fundamental groupoids*.

Fundamental groupoids make up the most elementary, but perhaps most difficult layer of *étale homotopy*.

Given an equation

$$f(x, y) = 0$$

with $f \in \mathbb{Q}[x, y]$, start out with a compactification $X(\mathbb{C})$ of the set of complex solutions. Typically, a compact two-manifold.

The fundamental groupoid is made up of the path spaces

$$\pi_1(X(\mathbb{C}); a, b)$$

as the two points a and b vary over $X(\mathbb{C})$, together with the composition

$$\pi_1(X(\mathbb{C}); b, c) \times \pi_1(X(\mathbb{C}); a, b) \rightarrow \pi_1(X(\mathbb{C}); a, c)$$

obtained by concatenating paths.

The portion that originates at a fixed base-point b is comprised of the fundamental group

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

and the homotopy classes of paths

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

for any other point $x \in X(\mathbb{C})$.

We will focus mostly on the category of *torsors* for the group $\pi_1(X(\mathbb{C}), b)$ made up by the path spaces $\pi_1(X(\mathbb{C}); b, x)$.

This means that there is a group action

$$\pi_1(X(\mathbb{C}); b, x) \times \pi_1(X(\mathbb{C}), b) \longrightarrow \pi_1(X(\mathbb{C}); b, x)$$

that is simply transitive.

Alternatively, any choice of a path $p \in \pi_1(X(\mathbb{C}); b, x)$ determines a bijection

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

$$\gamma \mapsto p \circ \gamma.$$

3.3.1 Relevance to Diophantine geometry

The proposal of anabelian geometry is to encode solutions to the equation, i.e., points on X, into the structures $\pi_1(X(\mathbb{C}); b, x)$.

The idea of encoding points into 'larger' geometric objects is a common one in Diophantine geometry, as when solutions

$$a^n + b^n = c^n$$

to the Fermat equation are encoded into the elliptic curves

$$y^2 = x(x - a^n)(x + b^n).$$

The geometry of the path torsor $\pi_1(X(\mathbb{C}); b, x)$ is an extremely canonical version of this idea.

4. Implementation: Non-archimedean completions

To distinguish rational solutions $X(\mathbb{Q})$ from arbitrary complex ones, one needs to pass to a non-archimedean *linearization*.

Standard linearization: the group ring

$$\mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)].$$

Obtain thereby, a number of additional structures.

The group ring is a Hopf algebra with comultiplication

$$\Delta : \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)] \to \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)] \otimes \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]$$

determined by the formula

$$\Delta(g) = g \otimes g$$

for $g \in \pi_1(X(\mathbb{C}), b)$.

Inside the group ring there is the augmentation ideal

$$J \subset \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]$$

generated by elements of the form $g - 1$.

Completion:

$$A = \mathbb{Q}_p[[\pi_1(X(\mathbb{C}), b)]] := \varprojlim_n \mathbb{Q}_p[\pi_1(X(\mathbb{C}), b)]/J^n,$$

whose elements can be thought of as non-commuative formal power series in elements $g - 1$, $g \in \pi_1$.

The previous co-product carries over to an algebra homomorphism

$$\Delta : A \longrightarrow A\hat{\otimes}A := \varprojlim A/J^n \otimes A/J^m,$$

turning A into a *complete Hopf algebra*.

Study of such structures originates in *rational homotopy theory*, with which we are actually concerned from a motivic point of view.

One defines the group-like elements

$$U = \{g \mid \Delta(g) = g \otimes g,\ V \in L\}.$$

The elements of the discrete fundamental group give rise to elements of U, but there are many more. For example, given $g \in \pi_1$, one can obtain elements of U using $\mathbb{Q}_p$-powers of g:

$$g^\lambda := \exp(\lambda \log(g)).$$

The group U is in fact very large, with the structure of a pro-algebraic group over $\mathbb{Q}_p$.

The path torsors can be completed as well, to give

$$P(x) := [\pi_1(X(\mathbb{C}); b, c) \times U]/\pi_1(X(\mathbb{C}), b),$$

which are torsors for U.

The most important extra structure arises when b and x are both rational points. Then U and $P(x)$ admit a very large group of hidden symmetries, a continuous action of

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

The symmetry arises from a reinterpretation of these constructions in terms of the étale topology of the scheme X.

Two important facts:

-If p is chosen large enough and the fundamental group is non-abelian, then the structure $P(x)$ completely determines the point x. That is, if

$$P(x) \simeq P(x')$$

as U-torsors with G-action, then $x = x'$.

-Can classify such structures, using a pro-algebraic moduli space

$$H^1_f(G, U),$$

describing non-abelian continuous group cohomology.

Each $P(x)$ determines an element of this space.

$$X(\mathbb{Q}) \longrightarrow H^1_f(G, U);$$

$$x \mapsto [P(x)].$$

4.1 Construction

The cohomology here is defined as a quotient space

$$H^1(G,U) = Z^1(G,U)/U,$$

where $Z^1(G,U)$ consists of the continuous functions

$$c : G \to U$$

satisfying the 'cocycle condition'

$$c(\sigma_1\sigma_2) = c(\sigma_1)\sigma_1(c(\sigma_2)),$$

and $u \in U$ acts on such functions by

$$(u \cdot c)(\sigma) = u^{-1}c(s)s(u).$$

A torsor T gives rise to such a function when we choose an element $t \in T$. Then for any $\sigma \in G$, we have

$$\sigma(t) = tu_\sigma$$

for some unique $u_\sigma \in U$. It is easily checked that the function

$$\sigma \mapsto u_\sigma$$

satisfies the cocycle condition, and that the corresponding class in $H^1(G, U)$ is independent of the choice of t.

$$H^1_f(G, U) \subset H^1(G, U)$$

is a subspace defined by a collection of 'local conditions' reflecting the natural geometry of the scheme.

4.2 The nature of Diophantine finiteness

Can also consider the p-adic points $X(\mathbb{Q}_p)$, which has a non-archimedean analytic structure.

Thereby, the $\mathbb{Q}$-points $X(\mathbb{Q})$ become embedded in two *entirely canonical families* having, however, very different natures:

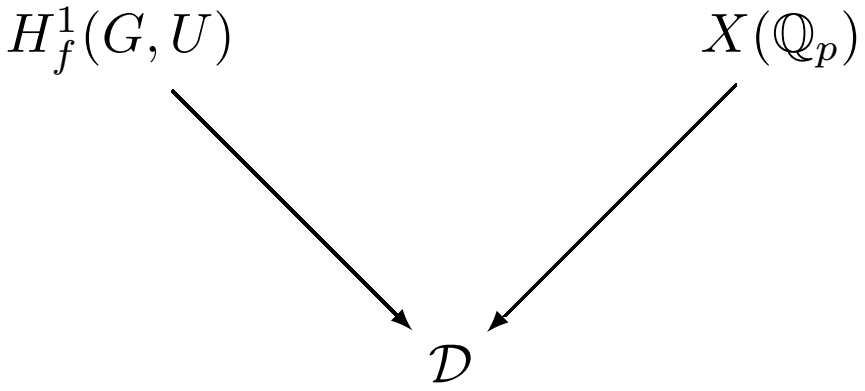
$$H^1_f(G, U)$$

and

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

There is severe tension between the two families when X itself is sufficiently complex, more precisely, when $\pi_1(X(\mathbb{C}), b)$ is *non-abelian*.

This tension is brought out by mapping both families into a large p-adic symmetric space



constructed using *p-adic Hodge theory*.

It emerges that the key difference between the two maps is that $H^1_f(G,U)$ maps to an algebraic subspace, while $X(\mathbb{Q}_p)$ maps to a *space-filling curve*.

4.2.1 Remark

The ambient symmetric space $\mathcal{D}$ is in fact a homogeneous space

$$U^{DR}/F^0$$

for the *De Rham fundamental group* of $X_{\mathbb{Q}_p}$.

4.2.2 Example

For the equation

$$ax^n + by^n = c$$

the fundamental group is non-abelian exactly when $n \geq 4$.

In this case, one can show that

$$Im(H^1_f(G, U)) \cap Im(X(\mathbb{Q}_p))$$

is finite, and deduce from this the finiteness of points.

An important technical ingredient is *multi-variable Iwasawa theory* (joint work with John Coates).

5. Discussion: Diophantine geometry and Galois theory

The arrow

> Identifying the relevant structures and developing their theory $\longrightarrow$ resolution of Diophantine problems

discussed in the context of Grothendieck's philosophy of the rising sea is exemplified by classical Galois theory.

There, *group theory* is shown to underlie a Diophantine classification of polynomials in one variable.

The task at hand is to develop a Galois theory of polynomials in two variables.