Torsors and Topology in Diophantine Problems

MSRI DDC Semester

David Corwin

October 28, 2020

Motivation: Rational and Integral Points on Varieties

Let X be a variety over a number field k. E.g., $k = \mathbb{Q}$.

Question

Is $X(k)$ empty? finite? infinite?
If finite, what is the set of rational points?

This is hard, and there's no known algorithm. But here are some computable questions:

- Is $X(\mathbb{Q}_p)$ empty?
- Is $X(\mathbb{R})$ empty?
- Is $X(\overline{\mathbb{Q}})$ empty?

One can similarly ask about $X(\mathbb{Z})$ (which is also hard), and then ask about $X(\mathbb{Z}_p)$ and $X(\overline{\mathbb{Z}})$ (which are computable).

Simplifying the Problem

Approaches to $X(k)$

Suppose $k = \mathbb{Q}$. One might consider the following approaches:

- Find $X(\mathbb{Q}) \subseteq X(\mathbb{Q}_p)$.
  Maybe using some p-adic methods, even p-adic analysis.
- Find $X(\mathbb{Q}) \subseteq X(\overline{\mathbb{Q}})$.
  Then $X(\mathbb{Q})$ is precisely the subset of $X(\overline{\mathbb{Q}})$ fixed by the absolute Galois group.

For a field k, let $G_k = \mathrm{Gal}(\overline{k}/k)$. Then we have $X(k) = X(\overline{k})^{G_k}$.

For a number field k and a valuation v, we consider its completions k_v (e.g., $\mathbb{Q}_p$ and $\mathbb{R}$ for $k = \mathbb{Q}$).

Note that $G_{k_v} \subseteq G_k$, so we might try to combine the approaches.

Relating Rational Points to Galois Theory

Question

How do we effectively use Galois groups to study rational points?

Answer: torsors (AKA principal homogeneous spaces) and Galois cohomology

Definition

A *group over k* is a group π with an action $G_k \to \operatorname{Aut}\pi$

Examples

- π is any group with trivial action of G_k. This is called *constant*.
- $\pi = \mu_n := \{x \in \overline{k} \mid x^n = 1\}$. (This is constant iff k contains all nth roots of unity.)
- For a fixed elliptic curve E over k, $\pi = E[n] := \{P \in E(\overline{k}) \mid nP = O\}$.

Torsors

Definition

A *torsor* under π over k is a set T with an action of G_k and an action of π such that:

- The action of π on T is simply transitive (i.e., choosing an element of T gives a bijection between π and T)
- The map $\pi \times T \to T$ is equivariant for the action of G_k, i.e., if $\sigma \in G_k$, $a \in \pi$, and $b \in T$, then

$$\sigma(a(b)) = \sigma(a)(\sigma(b))$$

Torsors are classified by group cohomology. The set of torsors under π over k up to isomorphism is $H^1(G_k; \pi)$.

This means that sets of torsors have a lot of nice formal properties and can be computed in many cases.

Examples of Torsors

Examples

- If π is any group over k, we can set $T = \pi$ with the same G_k-action, and let π act by translation. This is called the *trivial* torsor.
- For $z \in k^\times$, then $T_z = z^{1/n} := \{x \in \overline{k} \mid x^n = z\}$ is a torsor under μ_n.
- For $z \in E(k)$, then $T_z = [n]^{-1}(z) := \{x \in E(\overline{k}) \mid nx = z\}$ is a torsor under $E[n]$.

Note that a torsor is trivial iff T has an element fixed by G_k.

We will now see how the latter two examples come naturally from finite coverings of algebraic curve.

Topological Origin of These Torsors

First let's consider nth roots:

- Let $X = \mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$. Then topologically, $X(\mathbb{C})$ is a punctured plane, so its fundamental group is $\mathbb{Z}$.
- For an integer n, there is a topological cover of degree n corresponding to the subgroup $n\mathbb{Z} \subseteq \pi_1(X(\mathbb{C}))$. Algebraically, this cover is given by the map $x \mapsto z = x^n$.
- The group μ_n is naturally the group of automorphisms of the topological cover. A root of unity ζ_n sends x to $x\zeta_n$.
- The torsor T_z is the fiber (preimage) of $z \in X(k)$ by the covering map.

Next, let's consider the elliptic curve example:

Topological Origin (cont.)

- For an elliptic curve E, we have $\pi_1(E(\mathbb{C})) = \mathbb{Z} \times \mathbb{Z}$.
- The multiplication-by-n map $[n]$ on E (using its group law) expresses E as the topological cover of itself corresponding to the index n^2 subgroup $n\mathbb{Z} \times n\mathbb{Z} \subseteq \pi_1(E(\mathbb{C}))$.
- As an example, for the elliptic curve $y^2 = x^3 + x$, the map $[2]$ is given explicitly by

$$[2](x,y) = \left(\frac{(x^2-1)^2}{4(x^3+x)}, \frac{y(x^6+5x^4-5x^2-1)}{8(x^3+2)^2} \right)$$

- The torsor T_z is similarly the fiber of $[n]$ over the point $z \in E(k)$.

Motivation from Topology

- There is an analogy between Galois groups and fundamental groups.
- In this analogy, a field k is really a space $\operatorname{Spec} k$ whose fundamental group is G_k.
- Monodromy action: if $f\colon V \to S$ is a covering or bundle over S, then $\pi_1(S)$ acts on the fibers of f.
- Similarly, $\pi_1(S)$ acts on the various algebro-topological invariants of the fibers.
- A group π or a torsor T is called "over k" precisely because it has a "monodromy" action of G_k
- The theory of schemes and the étale topology can be used to make this analogy more precise and rigorous.

Torsors Under the Fundamental Group

- If X is any smooth variety over k (a subfield of $\mathbb{C}$), a theorem of Riemann says that any finite topological cover of $X(\mathbb{C})$ can be expressed as a map $Y \xrightarrow{f} X$ of algebraic varieties over k.
- If this is a Galois cover of degree d (i.e., its automorphism group has size d), then its automorphism group π is a quotient of $\pi_1(X(\mathbb{C}))$.
- For $z \in X(k)$, the set $f^{-1}(z)$ has d points, but some of them might have irrational (but algebraic) coordinates.
- Given $\sigma \in G_k$ and $x \in f^{-1}(z)$, we can apply σ to the coordinates of x to get another element of $f^{-1}(z)$.
- $f^{-1}(z)$ also has a simply transitive action of π, so it's a torsor under π over k.
- The torsor is trivial iff $f^{-1}(z)$ has a point fixed by G_k; i.e., a rational point.

The Kummer Map

- By considering *all* finite covers, one can associate to any $z \in X(k)$ a torsor over k under $\widehat{\pi_1(X(\mathbb{C}))}$ (the profinite completion of the fundamental group).
- The set of such torsors is $H^1(G_k; \widehat{\pi_1(X(\mathbb{C}))})$ (you can take that as a notation, but it's actually the same as group cohomology!)
- This torsor is denoted $\kappa(z)$. In fact, for any reasonable variety X, we have a map

$$X(k) \xrightarrow{\kappa} H^1(G_k; \widehat{\pi_1(X(\mathbb{C}))})$$

- It is called the Kummer map, after Kummer studied field extensions defined by radicals using what we now call the map $k^\times \to H^1(G_k; \mu_n)$; i.e., the case of $X = \mathbb{G}_m$
- More generally, you could consider that map only for a single cover (as we did on the last slide), or even a certain collection of covers - thus for a (Galois-equivariant) quotient of $\widehat{\pi_1(X(\mathbb{C}))}$.

Comparing p-adics and $\mathbb{Q}$

- We have a similar map

$$X(k_v) \xrightarrow{\kappa_v} H^1(G_{k_v}; \pi_1\widehat{(X(\mathbb{C})})) $$

  for every v.
  We can thus create a diagram:

$$\begin{tikzcd} X(k) \arrow[r] \arrow[d, "\kappa"'] & X(k_v) \arrow[d, "\kappa_v"] \\ H^1(G_k; \pi_1\widehat{(X(\mathbb{C})})) \arrow[r, "\mathrm{loc}"] & H^1(G_{k_v}; \pi_1\widehat{(X(\mathbb{C})})) \end{tikzcd}$$

- One often approaches $X(k)$ by studying $\kappa_p^{-1}(\mathrm{Im}(\mathrm{loc}))$. It is a subset of $X(k_v)$ that contains $X(k)$.
- All of my work has involved variants on this diagram.

Obstructions to the Local-Global Principle

In this variant, we use not one place/prime/valuation v, but rather all v, bundled together in the adele ring $\mathbb{A}_k$:

$$\begin{array}{ccc} X(k) & \longrightarrow & X(\mathbb{A}_k) \\ {\scriptstyle\kappa}\downarrow & & \downarrow{\scriptstyle\kappa_a} \\ H^1(G_k;\pi_1\widehat{(X(\mathbb{C})})) & \xrightarrow{\text{loc}} & \prod_v H^1(G_{k_v};\pi_1\widehat{(X(\mathbb{C})})) \end{array}$$

- $X(\mathbb{A}_k)^{\mathrm{f-cov}} := \kappa_a^{-1}(\mathrm{Im}(\mathrm{loc}))$ is the *finite descent obstruction* set
- Manin defined $X(\mathbb{A}_k)^{\mathrm{Br}}$, another subset of $X(\mathbb{A}_k)$ containing $X(\mathbb{Q})$.
- Originally defined using Brauer groups; Harpaz-Schlank gave it a much more topological interpretation:
- As $X(\mathbb{A}_k)^{\mathrm{f-cov}}$ is defined using $\pi_1\widehat{(X(\mathbb{C})})$, the set $X(\mathbb{A}_k)^{\mathrm{Br}}$ uses $H^*(X(\mathbb{C});\widehat{\mathbb{Z}})$.
- One can combine them into the étale homotopy obstruction $X(\mathbb{A}_k)^h$.

Brauer and Etale Homotopy Obstructions to Rational Points on Open Covers

The obstructions on the previous slide are often used to answer whether $X(k)$ is empty (i.e., if $X(\mathbb{A}_k)^h$ is empty, then so is $X(k)$!)
In arXiv:2006.11699, we (joint w/ Schlank) prove:

1. If k is a totally real field, and $X(k) = \emptyset$, there is a Zariski open covering $\{U_i\}$ of X such that $U_i(\mathbb{A}_k)^{\mathrm{f-cov}} = \emptyset$.
2. If the section conjecture in anabelian geometry holds, then the same is true for any number field k.
3. Using the homotopical nature of $X(\mathbb{A}_k)^h$, we show:

Theorem

If $f\colon X \to S$ is a fibration of varieties (e.g., smooth proper map), $S(\mathbb{A}_k)^h = \emptyset$, and for every $s \in S(k)$, we have $X_s(\mathbb{A}_k)^h = \emptyset$, then under some technical conditions $X(\mathbb{A}_k)^h = \emptyset$.

Brauer and Etale Homotopy Obstruction: Future Directions

- Seems like an algorithm: if $X(k)$ is empty, just show $U_i(\mathbb{A}_k)^{\mathrm{f-cov}} = \emptyset$ for all i.
- If U_i were proper (compact), then this would be computable (with a *finite* set of finite covers).
- Generally: might need infinitely many covers
- Hope: could choose U_i so that only finitely many covers are needed
- Works in specific examples, and there's an intuition that one needs infinitely many only when there are "rational points on the cusp" (does not happen if $X(k) = \emptyset$).
- Future project: étale homotopy obstruction for $k = \mathbb{Q}_p(t)$. For reasons of Galois cohomological dimension, $\pi_3(X(\mathbb{C}))$ is relevant, unlike for k a number field.

Non-Abelian Chabauty's Method

- Uses a diagram with only one place (prime) v, but only certain topological covers.
- More specifically, only covers whose automorphism group is a *nilpotent group*. This corresponds to a quotient of $\pi_1\widehat{(X(\mathbb{C}))}$ denoted $\pi_1^{un}(X)$, giving the following diagram:

$$\begin{tikzcd} X(\mathbb{Q}) \arrow[r] \arrow[d, "\kappa"'] & X(\mathbb{Q}_p) \arrow[d, "\kappa_p"] \\ H^1(G_{\mathbb{Q}}; \pi_1^{un}(X)) \arrow[r, "\mathrm{loc}"] & H^1(G_{\mathbb{Q}_p}; \pi_1^{un}(X)) \end{tikzcd}$$

- $H^1(G_{\mathbb{Q}_p}; \pi_1^{un}(X))$ is related via p-adic Hodge theory to p-adic analytic functions.
- One gets analytic functions on $X(\mathbb{Q}_p)$ whose common zero set contains $X(\mathbb{Q})$.

Work on Non-Abelian Chabauty

- Much has been computed by Balakrishnan et al
- My work: explicit computations for $X = \mathbb{A}^1 \setminus \{0,1\} = \mathbb{P}^1 \setminus \{0,1,\infty\}$ (building on work of Dan-Cohen and Wewers).
- We find $X(\mathbb{Z}[1/N])$ in place of $X(\mathbb{Q})$ (using $X(\mathbb{Z}_p)$ in place of $X(\mathbb{Q}_p)$).
- Equivalent to "S-unit equation": find x, y such that:
  1. $x + y = 1$
  2. the numerator and denominator of x and y contain only primes dividing N
- We have some new ideas and computations in arXiv:1812.05707 and an algorithm in arXiv:1811.07364 (joint w/ Dan-Cohen)
- Working on expanding our methods to integral points on elliptic curves, with a view toward all higher genus curves.

Thank You!

Relevant Links:

- `https://arxiv.org/abs/2006.11699` on Brauer and Etale Homotopy Obstructions
- `https://arxiv.org/abs/1812.05707` and `https://arxiv.org/abs/1811.07364` on non-Abelian Chabauty for a punctured line
- `math.berkeley.edu/~dcorwin` for other versions of and slides about those papers
- `math.berkeley.edu/~dcorwin/files/etale.pdf` for an introduction to the relationship between Galois groups and fundamental groups