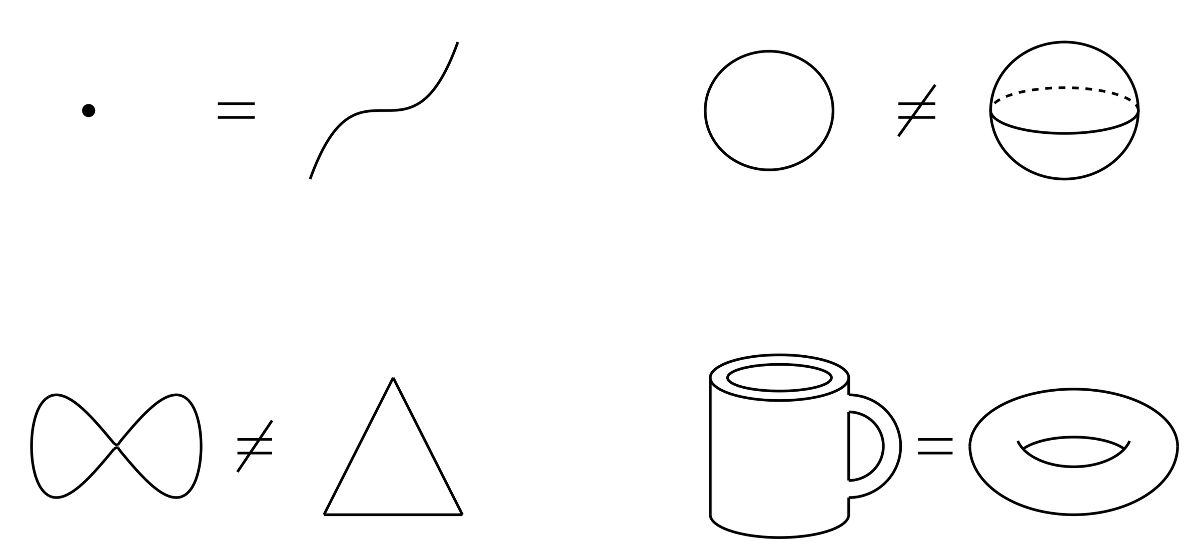
Homotopy Theory and Diophantine Geometry

What is the shape of an equation?

Christopher Lazda, Pure Mathematics

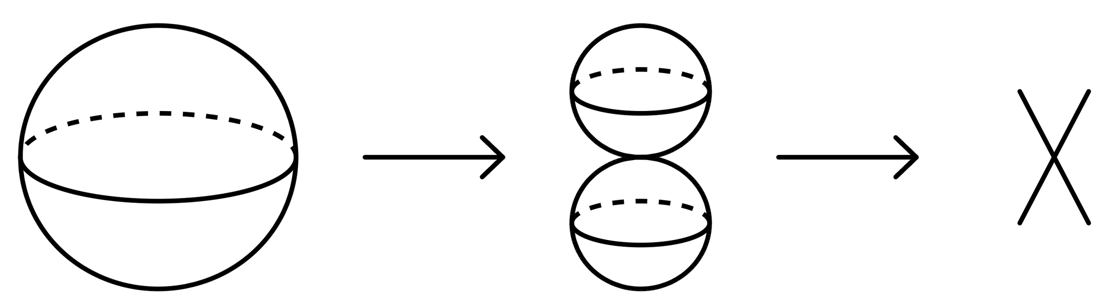
What is Homotopy Theory?

In homotopy theory, we study topological spaces, but only 'up to homotopy'. That is we consider two spaces the same, and we say that they have the same 'homotopy type' if they can be continuously deformed into one another.



Example of homotopy (non-)equivalences

The tools of algebraic topology are very important - invariants like singular/simplicial homology $H_n(X,\mathbb{Z})$, which counts n-dimensional holes in X, and the fundamental group $\pi_1(X)$, which classifies loops in X (i.e. maps $S^1 \to X$), depend only on the underlying 'homotopy type' of the topological space.



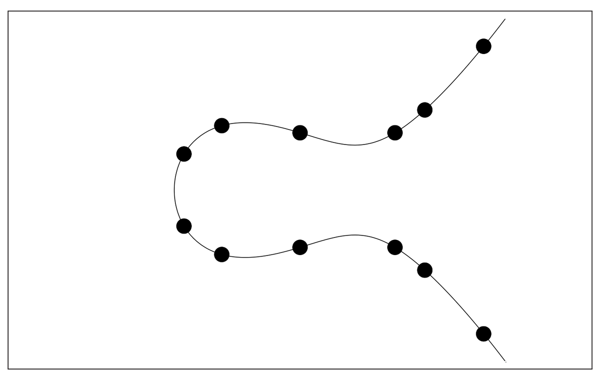
Addition in homotopy groups

We can also define higher 'fundamental' groups $\pi_n(X)$ by looking at maps $S^n \to X$ from higher dimensional spheres. The sequence of groups $\{\pi_n(X)\}_n$ tells us a lot about the homotopy type of X. This is because a lot of the spaces we care about are built up from spheres (such spaces are called CW complexes or cell complexes), and if we know how spheres map into X, then we know how spaces built from spheres map into X.

What is Diophantine Geometry?

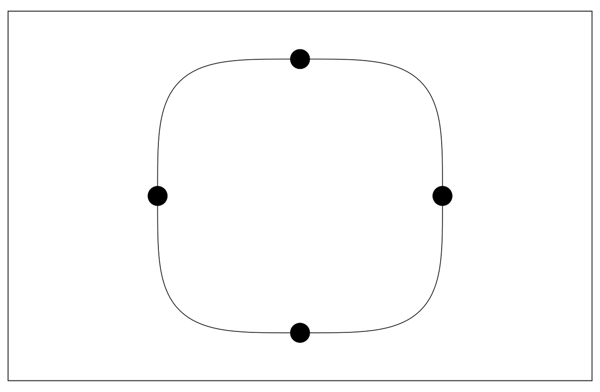
Diophantine geometry is the study of integer and/or rational solutions to polynomial equations. For example we might want to consider solutions (x,y) to equations like $x^4+y^4=1$ where $x,y\in\mathbb{Q}$ - this is a case of Fermat's last theorem. Diophantine problems can be very difficult to solve!

For example, if we look at the curve $y^2=x^3-x+1$ in the plane $\mathbb{R}^2$, then we get lots of rational points (in fact, infinitely many).



An elliptic curve with infinitely many rational points

But Fermat's last theorem (in this special case proved by Euler) tells us that for $x^4+y^4=1$, the only rational points are the four obvious ones.



A Fermat curve with finitely many rational points

In general, we consider 'algebraic' subsets $V\subset\mathbb{C}^n$ - these are subsets cut out by polynomial equations $p_i\in\mathbb{C}[x_1,\ldots,x_n]$.

$$V=\{(x_1,\ldots,x_n)\in\mathbb{C}^n \mid p_1(x_1,\ldots,x_n)=\ldots=p_m(x_1,\ldots,x_n)=0\}$$

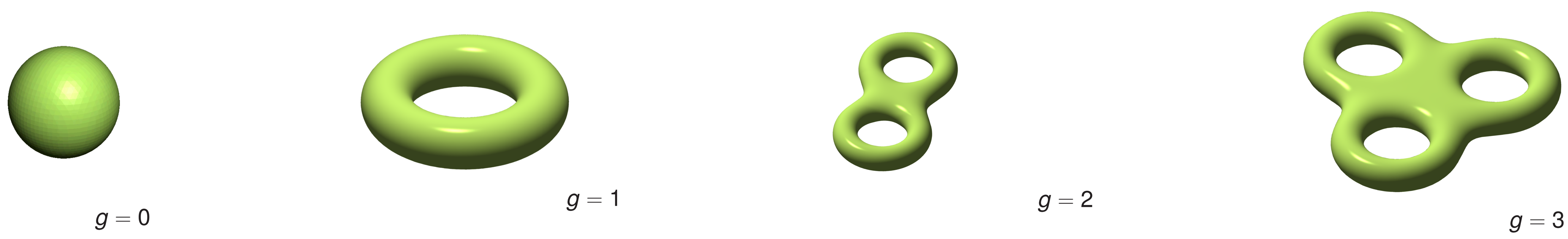
If these polynomial equations p_i have rational coefficients, then we can ask about the set $V(\mathbb{Q})$ of rational points in V - i.e. those elements of V whose co-ordinates are rational numbers .

Typical 'Diophantine' questions are:

- How may rational solutions are there? Zero? Finitely many? Infinitely many?
- Are the rational points 'dense' in V?
- Is there an algorithm that produces rational points?

What can topology tell us about arithmetic?

If we look at a polynomial equation $p(x,y)=0$ in two variables, with rational coefficients, then the set of complex solutions forms a surface inside $\mathbb{C}^2\cong\mathbb{R}^4$. There is a natural way to 'complete' this surface, and we end up with a multi-holed torus.



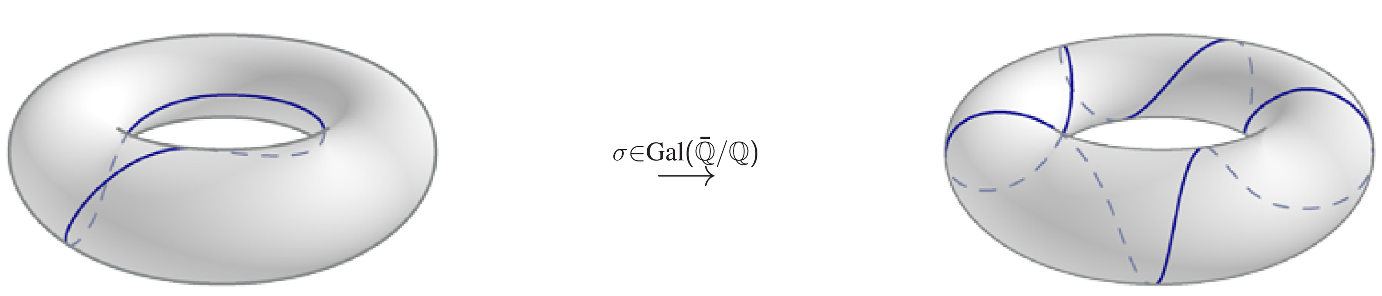
Thus associated to our equation $p(x,y)=0$, we have a 'homotopy type', which is determined by it's number of holes, g, called the genus. This can give us arithmetical information.

Theorem. *(Faltings, 1983) If $g\geq 2$ then there are only finitely many rational solutions to $p(x,y)=0$.*

Idea of Proof: We can perform the above 'completion' operation algebraically, to give a smooth curve C inside $\mathbb{P}^2(\bar{\mathbb{Q}})$. We can then use the theory of abelian varieties to study such curves via their Jacobians - the result follows from the fact that there are only finitely many isomorphism classes of abelian varieties over $\mathbb{Q}$ with certain properties. This is what Faltings proves, and he does so by studying the fundamental groups of abelian varieties. □

Galois actions

In the above situation, the fact that our polynomial $p(x,y)$ has rational coefficients ensures that the associated homotopy type has an extra, very rich structure - it comes with an action of the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ of $\mathbb{Q}$. This structure is far from being just dependent on g, and can give us very deep arithmetical information - it is the study of this Galois action on the fundamental group that is the key ingredient in Faltings' proof. Indeed, assuming certain conjectures about this Galois action, one can produce an algorithm that computes rational points.



Galois action on the fundamental group

More generally, given any collection of polynomial equations with rational coefficients, one can use the set of complex solutions to obtain a homotopy type. This homotopy type will come with a 'rational structure', i.e. an action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and we can use this to study the Diophantine properties of our system of equations.

My research

Instead of looking at polynomial equations over $\mathbb{Q}$, I look at polynomial equations over other fields, like for instance the finite field $\mathbb{F}_p$ or the 'function field' $\mathbb{F}_p(T)$ whose elements are ratios $p(t)/q(t)$ of polynomials over $\mathbb{F}_p$. In this situation, since there is no embedding into $\mathbb{C}$, we can't use complex solutions to define homotopy types. The sort of questions I look at are the following:

- Can we still define homotopy types in this situation?
- What sort of structure do these homotopy types have?
- Can we use this additional structures to study rational points?

For example, in the case of a smooth, complete curve over $\mathbb{F}_p(T)$, the fundamental group has the structure of something called an 'overconvergent F-isocrystal', which is an analogue of a Galois action. I am hoping that a study of this F-isocrystal structure might lead to information about rational points.

$$F\text{-}\mathcal{D}^{\dagger}_{\widehat{\mathbb{P}}^1_{\mathscr{V}}}({}^{\dagger}D)\curvearrowright\pi_1(C)\Rightarrow\#C(\mathbb{F}_p(T))<\infty?$$