A Diophantine definition of $\mathbb{Q}$ in $\mathbb{Q}(z)$

Héctor Pastén

Pontificia Universidad Católica de Chile

Joint work with Natalia Garcia-Fritz

Definability, Decidability and Computability over Arithmetically Significant Fields

(Semi-popular opinion: **every** field is arithmetically significant)

A result of Raphael Robinson

Theorem (R. Robinson 1964)

The field $\mathbb{Q}$ is first order definable in the field $\mathbb{Q}(z)$.

Proof.

Using an elliptic curve, one defines an infinite set $S \subseteq \mathbb{Q}$ which is dense in the $\mathbb{R}$-topology (take y-coordinates of rational points).
Then $f \in \mathbb{Q}(z)$ is constant if and only if:

$$\forall g, [g \in S \to (f \leq_4 g \vee g \leq_4 f)]$$

where $\leq_4$ is the partial order defined by sums of 4 squares. □

A folklore question

Motivated by the previous result, the following question has been around for quite some time:

Problem

Is $\mathbb{Q}$ Diophantine in $\mathbb{Q}(z)$?

Natalia and I learned about this question from Thanases Pheidas's talk at the MSRI DDC meeting in 2022.

The problem remains open, but I'll explain a partial answer.

Diophantine definition of k in $k(z)$

More generally, if k is a field we can ask whether k is Diophantine in $k(z)$.

A positive answer is known in the following cases (cf. work by Koenigsmann 2002 and Fehm-Geyer 2009):

- k is large (in the sense of Pop)
- For some $n \geq 2$ the quotient group $k^\times/(k^\times)^n$ is finite.

Unfortunately this says nothing about $k = \mathbb{Q}$.

Elliptic surfaces: the basics

Before stating our main result we need some background on elliptic surfaces. We'll only consider the base $\mathbb{P}^1$.

Let k be a field. An **elliptic surface** over k is a smooth projective surface X/k along with:

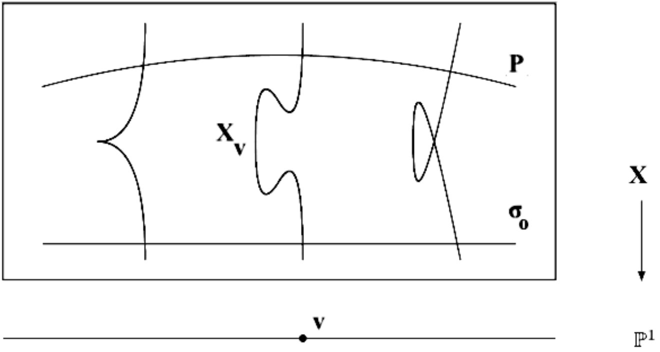
- A surjective morphism $\pi : X \to \mathbb{P}^1$ whose fibres are smooth curves of genus 1, up to finitely many; and
- a distinguished section $\sigma_0 : \mathbb{P}^1 \to X$ of π, that is, $\pi \circ \sigma_0 = Id_{\mathbb{P}^1}$.

Technical conditions: there are bad fibres, and the fibres of π contain no (-1)-curves.

Elliptic surfaces: the basics

Slogan:

An elliptic surface is a 1-parameter family of elliptic curves (with singular fibres.)



Elliptic surfaces: the basics

Important facts:

- For each $v \in \mathbb{P}^1(k)$ with X_v smooth, the fibre X_v is an elliptic curve with neutral element $\sigma_0(v)$.
- The sections $MW(X/k, \pi)$ form a f.g. abelian group (Lang-Neron).

Elliptic surfaces can be given (birationally) by a Weierstrass equation

$$E_t : \quad y^2 = x^3 + a(t)x^2 + b(t)x + c(t)$$

with $a, b, c \in k(t)$. The group of sections can be seen very concretely:

$$MW(X/k, \pi) \simeq E_t(k(t)).$$

Example: $E_t : \quad y^2 = x^3 + tx + t^2$ has the section $P_t = (0, t) \in E_t(k(t))$. This is like giving a point in each X_v which varies algebraically.

Elliptic surfaces: geometry

Conjecture (Ulmer)

Let $X/\mathbb{C}$ be a smooth projective surface with canonical sheaf K_X. There is a constant M such that for every (possibly singular) rational curve $C \subseteq X$ we have $C.K_X \leq M$.

Natalia and I proved:

Theorem (GF-P)

If Ulmer's conjecture holds, then there is an elliptic surface $X/\mathbb{Q}$ with a bad fibre of multiplicative type, such that X contains only finitely many rational curves over $\mathbb{C}$.

This consequence of Ulmer's conjecture is what we need.

Elliptic surfaces: arithmetic

Assume $k = \mathbb{Q}$. The rational points of an elliptic curve over $\mathbb{Q}$ form a finitely generated abelian group (Mordell).

Theorem (Silverman)

Let $\pi : X \to \mathbb{P}^1$ be an elliptic surface over $\mathbb{Q}$. For all but finitely many $v \in \mathbb{P}^1(\mathbb{Q})$ we have

$$\mathrm{rk}\, MW(X/\mathbb{Q}, \pi) \leq \mathrm{rk}\, E_v(\mathbb{Q}).$$

How often do we have equality? How often do we have strict inequality? There are conjectures on this. Under mild assumptions both cases are expected to occur quite often.

Elliptic surfaces: arithmetic

We need the next conjecture which follows from conjectures by Helfgott and Silverman

Conjecture (Positive rank conjecture)

Let $\pi : X \to \mathbb{P}^1$ *be an elliptic surface over* $\mathbb{Q}$ *given in Weierstrass form with polynomial coefficients, having some bad fibre of multiplicative type in the affine part. For* $x > 1$ *define*

$$N(x) = \#\{n \in \mathbb{N}_{\le x} \subseteq \mathbb{P}^1(\mathbb{Q}) : \mathrm{rk}\, X_n(\mathbb{Q}) > 0\}.$$

Then $N(x)$ *grows linearly: there is* $c > 0$ *with* $N(x) > cx$ *for* $x \gg 1$.

Main result

Theorem (GF-P 2022)

If Ulmer's conjecture and the Helfgott–Silverman conjecture hold, then $\mathbb{Q}$ is Diophantine in $\mathbb{Q}(z)$.

We'll sketch a proof. First we need some notions from additive number theory.

Density

Let $S \subseteq \mathbb{N}$. We have the following notions of density:

$$\delta^*(S) = \limsup_{x\to\infty} \frac{1}{x} \cdot \#\{n \in S : n \leq x\} \quad \text{upper density}$$

$$\delta_*(S) = \liminf_{x\to\infty} \frac{1}{x} \cdot \#\{n \in S : n \leq x\} \quad \text{lower density}$$

$$\sigma(S) = \inf_{k\geq 1} \frac{1}{k} \cdot \{n \in S : 1 \leq n \leq k\} \quad \text{Schnirelmann density}$$

Example. $S = 2\mathbb{N}$. Then $\delta^*(S) = \delta_*(S) = 1/2$ while $\sigma(S) = 0$.

It might seem artificial to call σ a density. Nevertheless, it is quite useful.

Density

Lemma

If $\delta_*(S) > 0$ *and* $1 \in S$ *then* $\sigma(S) > 0$.

A set $S \subseteq \mathbb{N}$ is called **additive basis of finite order** if there is a uniform M such that every $n \in \mathbb{N}$ is the sum of $\leq M$ elements of S.

Theorem (Schnirelmann)

If $\sigma(S) > 0$ *and* $0 \in S$ *then* S *is an additive basis of finite order.*

Density

Corollary (Criterion for checking that $\mathbb{Q}$ is Diophantine)

Let A be a commutative $\mathbb{Q}$-algebra. Suppose that there is a set $T \subseteq \mathbb{Q}$ which is Diophantine in A and satisfies $\delta_*(T \cap \mathbb{N}) > 0$. Then $\mathbb{Q}$ is Diophantine in A.

Proof.

- We can add $0, 1$ to T, so that now $T \cap \mathbb{N}$ is an additive basis of finite order.
- We can give a Diophantine definition of a set $T' \subseteq \mathbb{Q}$ that contains $\mathbb{N}$.
- Taking fractions, now we get $\mathbb{Q}$.

□

So we need to produce such a T for $A = \mathbb{Q}(z)$.

Sketch of the Diophantine definition of $\mathbb{Q}$ in $\mathbb{Q}(z)$

- By Ulmer's conjecture there is $X/\mathbb{Q}$ elliptic surface with finitely many rational curves and with a bad multiplicative fibre, say

$$E_t : \quad y^2 = x^3 + A(t)x + B(t).$$

- For any **non-constant** $f \in \mathbb{Q}(z)$ the new elliptic surface

$$E_f : \quad y^2 = x^3 + A(f)x + B(f)$$

has torsion group of sections: each section gives a rational curve in the surface X. Thus, $\mathrm{rk}\, E_f(\mathbb{Q}(z)) = 0$.

- For all but finitely many **constant** $c \in \mathbb{Q} \subseteq \mathbb{Q}(z)$ the substitution $t = c$ gives an elliptic curve $E_c/\mathbb{Q}$ which has $E_c(\mathbb{Q}(z)) = E_c(\mathbb{Q})$. These **might** have positive rank: that would be

$$\mathrm{rk}\, E_c(\mathbb{Q}(z)) = \mathrm{rk}\, E_c(\mathbb{Q}) > 0. \qquad (?)$$

Sketch of the Diophantine definition of $\mathbb{Q}$ in $\mathbb{Q}(z)$

- By Mazur's torsion theorem, "to have positive rank over $\mathbb{Q}$ or $\mathbb{Q}(z)$" is a Diophantine condition over $\mathbb{Q}(z)$.
- Therefore, the set

$$\begin{aligned} T &= \{f \in \mathbb{Q}(z) : \mathrm{rk}\, E_f(\mathbb{Q}(z)) > 0\} \\ &= \{c \in \mathbb{Q} : \mathrm{rk}\, E_c(\mathbb{Q}) > 0\} \subseteq \mathbb{Q} \end{aligned}$$

  is Diophantine over $\mathbb{Q}(z)$.
- Under the Helfgott–Silverman conjecture, $\delta_*(T \cap \mathbb{N}) > 0$.
- We conclude by the "criterion for checking that $\mathbb{Q}$ is Diophantine". □

Some possible directions

- Construct the required elliptic surface unconditionally. Recall: we need
  - $X \to \mathbb{P}^1$ defined over $\mathbb{Q}$
  - with a bad multiplicative fibre
  - with only finitely many rational curves on it.
- What about number fields?
- What about $\mathbb{Q}$ in $\mathbb{Q}(z_1, z_2)$?
- Let $C/\mathbb{Q}$ be a smooth projective curve of genus g. Is $\mathbb{Q}$ Diophantine in $\mathbb{Q}(C)$? We studied the case of $C = \mathbb{P}^1$.
- Find interesting subfields $F \subseteq \mathbb{Q}((z))$ where $\mathbb{Q}$ is Diophantine.

Thanks for your attention.