Hilbert's Tenth Problem for Generic Algebraic Fields

Russell Miller

Queens College & CUNY Graduate Center

Special Session on Computability Theory

AMS Sectional Meeting

21 April 2024

University of Wisconsin-Milwaukee

(Joint work with Kirsten Eisenträger, Caleb Springer, and Linda Westrick.)

HTP: Hilbert's Tenth Problem

Definition

For a countable field (or ring) F, *Hilbert's Tenth Problem for F* is the set

$$HTP(F) = \{f \in F[X_0, X_1, \ldots] : (\exists \vec{a} \in F^{<\omega})\ f(a_0, \ldots, a_n) = 0\}$$

of all polynomials (in several variables) with solutions in F.

$HTP(F)$ is always c.e. relative to the atomic diagram $D(F)$. Famously, $HTP(\mathbb{Z})$ is exactly as hard as $\emptyset'$, the Halting Problem. Indeed every computably enumerable set is *diophantine*, i.e., definable in $\mathbb{Z}$ by an existential formula. (Matiyasevich-Davis-Putnam-Robinson, 1970.)

Decidability of $HTP(\mathbb{Q})$ is open, but $HTP(\overline{\mathbb{Q}})$ is decidable. Our goal is to examine the general tendency for fields between these two – i.e., for algebraic field extensions of $\mathbb{Q}$.

Intuition for "general tendency"

The equation $X^5 + Y^5 = 1$ has no nonzero solutions in $\mathbb{Q}$. However, it has plenty of solutions in $\overline{\mathbb{Q}}$, and if we choose a subfield F of $\overline{\mathbb{Q}}$ "at random," it seems near-certain that F will contain such a solution.

More rigorously: no matter which (finitely many) elements have already been included in F or excluded from F, there will still remain infinitely many solutions in $\overline{\mathbb{Q}}$ that could yet appear in F.

(Indeed, for infinitely many $x \in \mathbb{Q}$, $\sqrt[5]{1 - x^5}$ could yet appear, and each of these has degree 5 over $\mathbb{Q}$.)

Therefore $X^5 + Y^5 - 1 = 0 \neq XY$ should have a solution in an "arbitrarily chosen" (or *generic*) F: sooner or later some x and y realizing this formula should appear in F.

Another example: beware of your intuition!

The equation $X^2 - 2Y^2 = 0$ has no nonzero solutions in $\mathbb{Q}$. However, it has plenty of solutions in $\overline{\mathbb{Q}}$....

... but this situation is different! Suppose that, in dividing up the elements of $\overline{\mathbb{Q}}$, we decide that $\sqrt{2} \notin F$. Then F cannot contain any nonzero solution, because if $x^2 - 2y^2 = 0 \neq xy$ and $x, y \in F$, then $\frac{x}{y} \in F$, yet $(\frac{x}{y})^2 = 2$.

Thus the choice of excluding $\sqrt{2}$ from F ruled out all nonzero solutions (whereas including $\sqrt{2}$ in F would immediately yield a solution). In this example, both the existential sentence and its negation

$$(\exists x, y)\ x^2 - 2y^2 = 0 \neq xy \qquad (\forall x, y)\ \neg(x^2 - 2y^2 = 0 \neq xy)$$

seem reasonably (equally?) likely to hold.

Topology on the subfields of $\overline{\mathbb{Q}}$

Fix one computable presentation $\overline{\mathbb{Q}}$ of the algebraic closure of $\mathbb{Q}$. Each choice of finitely many elements constitutes a *condition* on subfields. We write $(\vec{a}; \vec{b})$ to denote the condition saying that all of $\vec{a}$ is included and all of $\vec{b}$ is excluded. Then the set

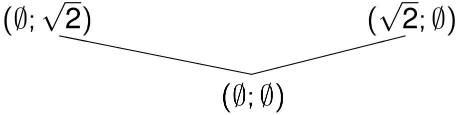
$$\mathcal{U}_{\vec{a};\vec{b}} = \{F \subseteq \overline{\mathbb{Q}} : \mathbb{Q}(\vec{a}) \subseteq F \ \&\ F \cap \{\vec{b}\} = \emptyset\}$$

is a basic open set in our topology on the space $\mathbf{Sub}(\overline{\mathbb{Q}})$ of all subfields of $\overline{\mathbb{Q}}$, and the topology is generated by these basic open sets, as $\vec{a}$ and $\vec{b}$ range over all finite tuples from $\overline{\mathbb{Q}}$.

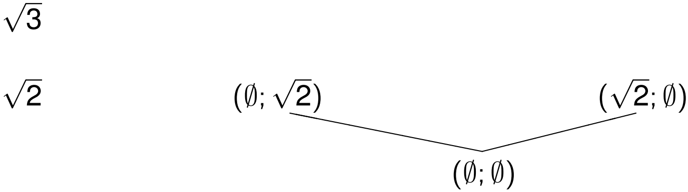
The relations $\mathcal{U}_{\vec{a};\vec{b}} \subseteq \mathcal{U}_{\vec{c};\vec{d}}$, $\mathcal{U}_{\vec{a};\vec{b}} = \mathbf{Sub}(\overline{\mathbb{Q}})$, and $\mathcal{U}_{\vec{a};\vec{b}} = \emptyset$ are decidable, by theorems of Kronecker.

Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$

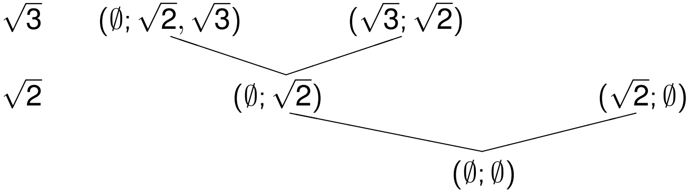
$\sqrt{2}$



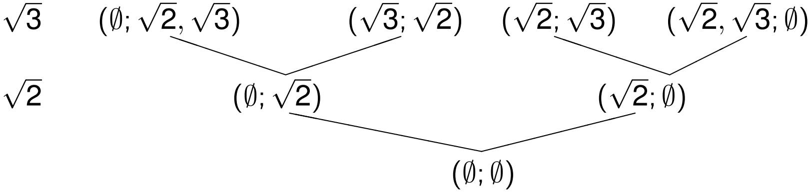
Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$



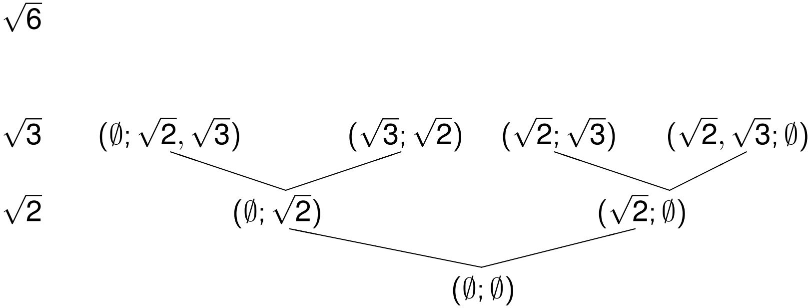
Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$



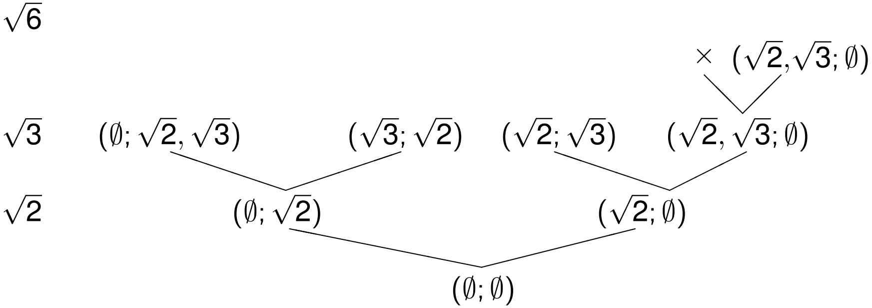
Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$



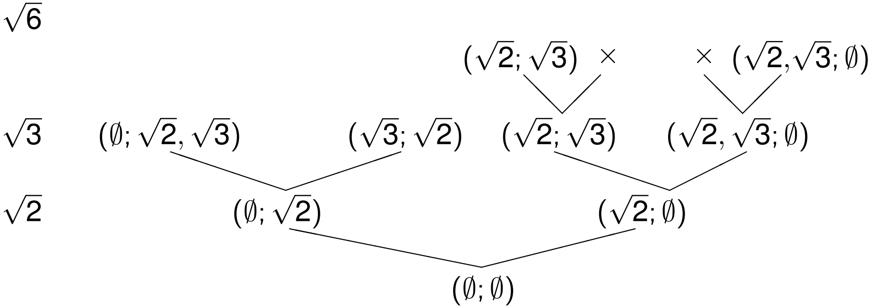
Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$



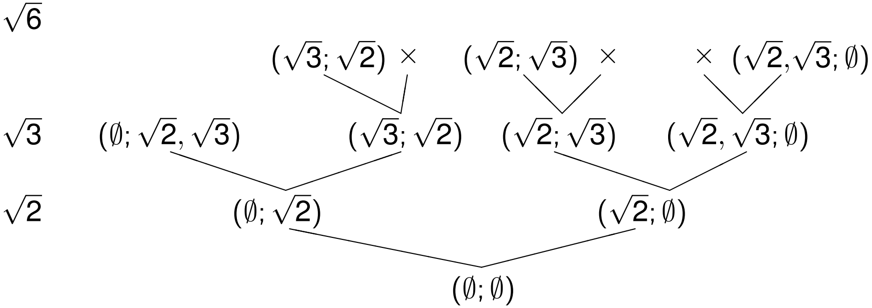
Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$



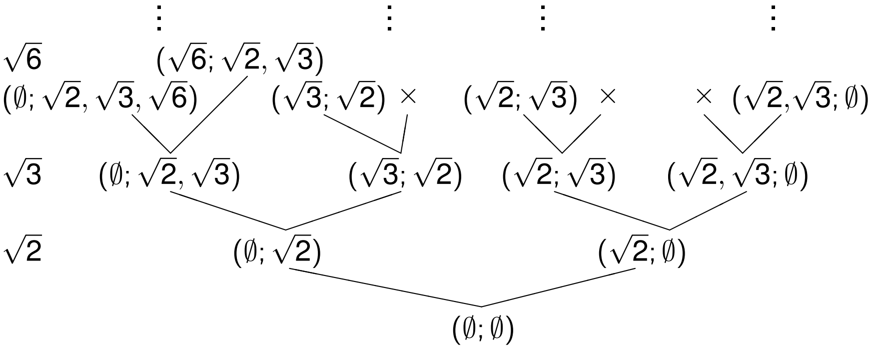
Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$



Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$



Picture: the space Sub($\overline{\mathbb{Q}}$) of all subfields of $\overline{\mathbb{Q}}$



The nodes $\times$ are unsatisfiable conditions: if we have ruled out $\sqrt{2}$, then F cannot contain both $\sqrt{3}$ and $\sqrt{6}$. But we still get a decidable subtree of $2^{<\omega}$, with no terminal nodes and no isolated paths. So the set of paths through it is homeomorphic to Cantor space 2^{ω}. This is the space **Sub**($\overline{\mathbb{Q}}$), with each path naming a subfield.

Conditions and forcing

Definition

A condition $(\vec{a}; \vec{b})$ *forces* a sentence φ, written $(\vec{a}; \vec{b}) \Vdash \varphi$, if

$$\{F \in \mathcal{U}_{\vec{a};\vec{b}} : \varphi \text{ is true in } F\}$$

is dense within $\mathcal{U}_{\vec{a};\vec{b}}$ in our topology.

In our examples earlier:

- $(\emptyset; \sqrt{2}) \Vdash (\forall x \forall y) \neg [x^2 - 2y^2 = 0 \neq xy]$.
- $(\sqrt{2}; \emptyset) \Vdash (\exists x \exists y)\ x^2 - 2y^2 = 0 \neq xy$.
- $(\emptyset; \emptyset) \Vdash (\exists x \exists y)\ x^5 + y^5 - 1 = 0 \neq xy$.

Notice that in the third item, not all fields in $\mathcal{U}_{\emptyset;\emptyset}$ satisfy the sentence given – e.g., $\mathbb{Q}$ does not – but densely many of them satisfy it. Ours is an unusual definition: forcing an existential sentence does not quite guarantee the truth of the sentence being forced!

Specifics of forcing $\exists$ and $\forall$ sentences

If $(\vec{a}; \vec{b}) \Vdash \forall \vec{x} \neg \psi(\vec{x})$, then in fact every field in $\mathcal{U}_{\vec{a};\vec{b}}$ satisfies $\forall \vec{x} \neg \psi(\vec{x})$. If any $F \in \mathcal{U}_{\vec{a};\vec{b}}$ contained a tuple $\vec{c}$ with $\psi(\vec{c})$, then $(\vec{a}, \vec{c};\ \vec{b})$ would be consistent (since F exists!) and every field in $\mathcal{U}_{\vec{a},\vec{c};\ \vec{b}}$ would contain this witness $\vec{c}$. Since $\mathcal{U}_{\vec{a},\vec{c};\ \vec{b}} \subseteq \mathcal{U}_{\vec{a};\vec{b}}$, this would contradict the density in $\mathcal{U}_{\vec{a};\vec{b}}$ of the fields satisfying $\forall \vec{x} \neg \psi(\vec{x})$.

However, as seen with $X^5 + Y^5 = 1$ above, a condition can force an existential sentence without the sentence being true in all fields realizing the condition.

Indeed, if we defined forcing the usual way, then the question of whether $(\vec{a}; \vec{b})$ forces $\exists \vec{x}\ p(\vec{x}) = 0$ would be exactly the question of whether $p = 0$ has a solution in $\mathbb{Q}(\vec{a})$. But this is $HTP(\mathbb{Q}(\vec{a}))$, whose decidability is an open question!

Key theorem

Theorem (Eisenträger, M., Springer, and Westrick)

It is decidable whether a condition $(\vec{a}; \vec{b})$ forces an existential or universal sentence φ (with parameters from $\mathbb{Q}(\vec{a})$). The decision procedure is uniform in $\vec{a}$, $\vec{b}$, and φ.

The proof is not simple. For $(\emptyset; \sqrt{2}) \Vdash \forall X \forall Y \neg (X^2 - 2Y^2 = 0 \neq XY)$, there was a "reason" for the forcing: the rational function $\frac{X}{Y}$. Whenever $X^2 - 2Y^2 = 0 \neq XY$, we get $(\frac{X}{Y})^2 = \frac{2Y^2}{Y^2} = 2$ so $\frac{X}{Y}$ is a square root of 2. The key to the proof is to show that this holds in general: whenever $(\overline{a}; \overline{b})$ forces a universal sentence, there is a "reason" stemming from the excluded tuple $\overline{b}$.

$\exists$-theory of a generic algebraic field

We now focus on the class of *generic* (specifically, 1-generic) fields. These fields form a comeager class in **Sub**($\overline{\mathbb{Q}}$). So, in the sense of Baire category, a property that holds of all generic fields may be considered to hold “almost everywhere.”

Proposition

Let φ be an existential or universal sentence, and let $F \in$ **Sub**($\overline{\mathbb{Q}}$) be a 1-generic field. Then

$$F \models \varphi \iff F \text{ realizes some } (\vec{a}; \vec{b}) \text{ with } (\vec{a}; \vec{b}) \Vdash \varphi.$$

In turn, the conditions realized by F can be determined if we know F as a subfield of $\overline{\mathbb{Q}}$, or equivalently (using Rabni’s Theorem!), if we know the atomic diagram of F and the *root set* of F:

$$HTP_1(F) = R_F = \{g \in F[X] : (\exists x \in F)\ g(x) = 0\}.$$

R_F is the one-variable version of Hilbert’s Tenth Problem $HTP(F)$ for F.

Root sets of generic fields

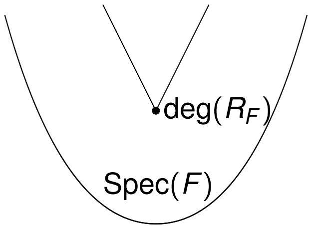
Theorem

Every generic algebraic field has a (standard) presentation F such that

$$R_F \not\leq_T D(F).$$

However, R_F is always *low relative to* $D(F)$: all presentations satisfy

$$(R_F \oplus D(F))' \leq_T (D(F))'.$$



General tendency of $HTP(F)$ for $F \subseteq \overline{\mathbb{Q}}$

Theorem (EMSW)

For all generic algebraic extensions F of $\mathbb{Q}$, the following sets are Turing-equivalent relative to $D(F)$:

- The root set $R_F = HTP_1(F)$.
- $HTP(F)$.
- The image of F in $\overline{\mathbb{Q}}$ under a ($D(F)$-computable) field embedding.

Moreover, all of these are of low Turing degree relative to $D(F)$, and in general they are not computable relative to $D(F)$ (although exceptional copies of F do exist).
Notice that therefore many sets that are $D(F)$-computably enumerable (including the Halting Problem itself) fail to be diophantine in F.

Since the generic extensions of $\mathbb{Q}$ form a comeager class in the space of all algebraic extensions, each of these properties may be considered to hold of "almost all" algebraic extensions of $\mathbb{Q}$, in the sense of Baire category.

$HTP^\infty(F)$

Let $HTP^\infty(F) = \{f \in F[\vec{X}] : f = 0$ has infinitely many solutions in $F\}$.

Theorem (EMSW)

It is decidable, uniformly in $\vec{a}$, $\vec{b}$, and f, whether $(\vec{a}, \vec{b}) \Vdash f \in HTP^\infty(F)$.

Corollary

For all 2-generic extensions F of $\mathbb{Q}$, $HTP^\infty(F) \equiv_T HTP_1(F) = R_F$ is again low (but in general noncomputable) relative to $D(F)$.

Corollary (of the proof)

For every condition $(\vec{a}; \vec{b})$, there exists a computable field $F \in \mathcal{U}_{\vec{a};\vec{b}}$ such that $HTP(F)$ and $HTP^\infty(F)$ are decidable.

Deciding if $(\overline{a}; \overline{b}) \Vdash \exists^\infty (X, Y, Z)\ (X^2 + Y^2)^2 - 2Z^2 = 0$

First check: this f has >1 variable, and $(\overline{a}; \overline{b}) \nVdash \forall X, Y, Z\ f \neq 0$. This f has absolutely irreducible factors f_0, f_1 in $\mathbb{Q}(\sqrt{2})[X, Y, Z]$, so consider two extensions, putting $\sqrt{2}$ in either $\overline{a}$ or $\overline{b}$. Let $F = \mathbb{Q}(\overline{a})$, $K = F(\overline{b})$.

- If $\sqrt{2} \in F$, then $(\overline{a}; \overline{b}) \Vdash \exists^\infty (X, Y, Z)\ f = 0$.
- Else $\sqrt{2} \in K - F$. The same reduction as before finds the formula $\frac{X^2+Y^2}{Z} = \sqrt{2}$, so $f = 0$ only works if $Z = 0$. (If the denominator had ∞-many solutions, we would know $(\overline{a}; \overline{b}) \Vdash \exists^\infty (X, Y, Z)\ f = 0$.)
- Now we know the finitely many Z that can work – here, only $Z = 0$. Specializing, we get $0 = f(X, Y, 0) = (X^2 + Y^2)^2$.
  1. If $i \in F = \mathbb{Q}(\overline{a})$, then $(\overline{a}; \overline{b}) \Vdash \exists^\infty (X, Y, Z)\ f = 0$. Every $(q, iq, 0)$ with $q \in \mathbb{Q}$ is a solution.
  2. If $i \in K - F$, then the only solution is $(0, 0, 0)$, as $\frac{X}{Y} = i$. So $(\overline{a}; \overline{b}) \Vdash \neg\exists^\infty (X, Y, Z)\ f = 0$
  3. If $i \notin K$, then $(\overline{a}; \overline{b})$ forces neither, since it has extensions $(\overline{a}, i; \overline{b})$ and $(\overline{a}; \overline{b}, i)$ that force both results.

Thank you!

Selected Bibliography

- P. Dittmann & A. Fehm, Non-definability of rings of integers in most algebraic fields. *Notre Dame Journal of Formal Logic* **62** (2021) 3, 589–592.
- K. Eisenträger, R. Miller, C. Springer, & L. Westrick, A topological approach to undefinability in algebraic fields. *Bulletin of Symbolic Logic* **29** (2023) 4, 626–655.
- J. Koenigsmann, Defining $\mathbb{Z}$ in $\mathbb{Q}$. *Annals of Mathematics* (2) **183** (2016) 1, 73–93.
- J. Park, A universal first-order formula defining the ring of integers in a number field. *Mathematical Research Letters* **20** (2013) 5, 961–980.