Computability and the Absolute Galois Group of $\mathbb{Q}$

Russell Miller

Queens College & CUNY Graduate Center

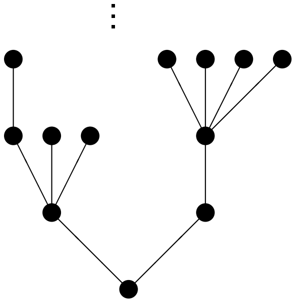
Special Session on Computability Theory
North American Annual Meeting of the ASL
Iowa State University
14 May 2024

(Partially joint work with Debanjana Kundu.)

Paths Through Finite-Branching Trees

König's Lemma

Every infinite finite-branching tree has an infinite path.



Some fail to have any computable path! However,....

Jockusch-Soare *Low Basis Theorem* (1972)

Every infinite decidable subtree of $2^{<\omega}$ has a path of *low* degree.

Galois theory

Definition

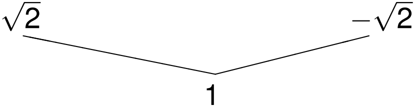
The *absolute Galois group of* $\mathbb{Q}$ is the automorphism group of the field $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$. (Formally it is $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, but every automorphism of $\overline{\mathbb{Q}}$ fixes $\mathbb{Q}$ pointwise.)

The goal here is to study the absolute Galois group $\text{Gal}(\mathbb{Q})$ from an effective standpoint. We will fix one computable presentation $\overline{\mathbb{Q}}$ of this algebraic closure. Indeed, as $\overline{\mathbb{Q}}$ is computably categorical, it is irrelevant which computable presentation $\overline{\mathbb{Q}}$ one chooses.

Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

$\sqrt{2} \mapsto$

$1 \mapsto$

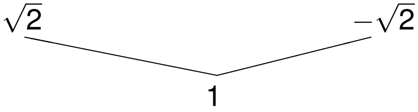


Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

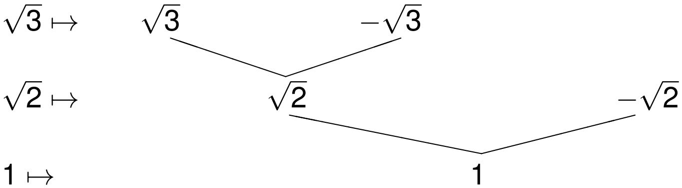
$\sqrt{3} \mapsto$

$\sqrt{2} \mapsto$

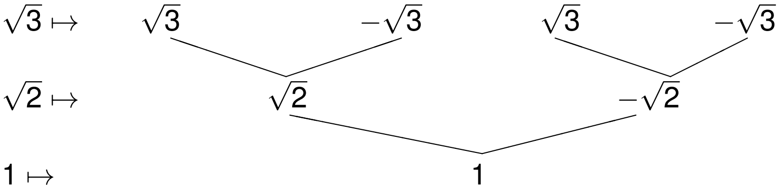
$1 \mapsto$



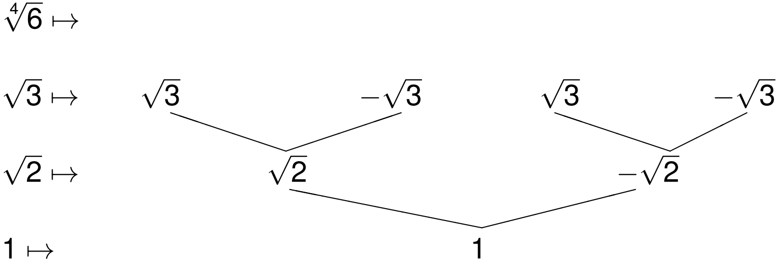
Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$



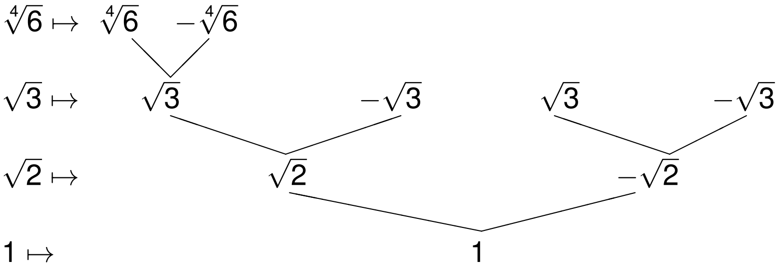
Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$



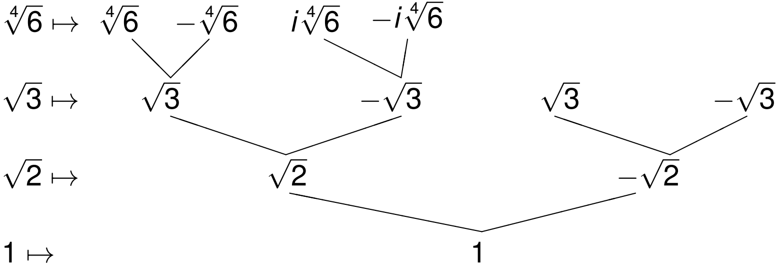
Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$



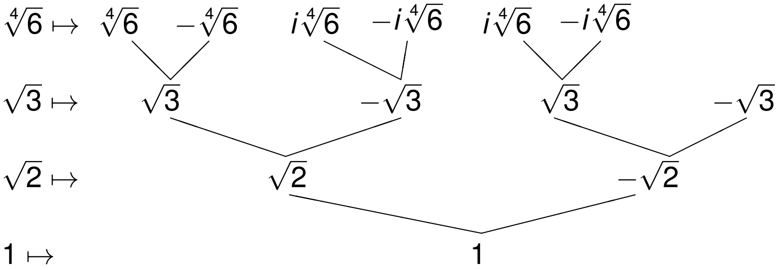
Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$



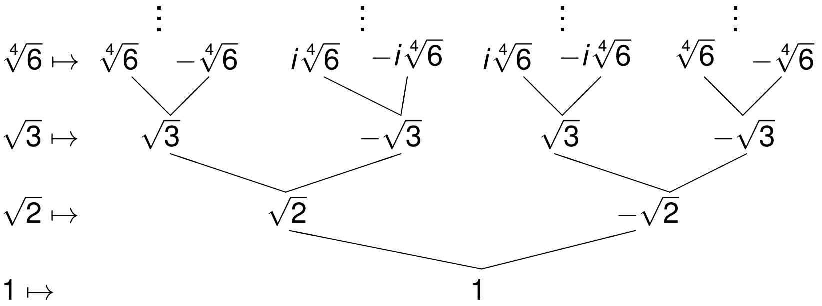
Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$



Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$



Intuitive picture of $\mathrm{Aut}(\overline{\mathbb{Q}}) = \mathrm{Gal}(\mathbb{Q}) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$



Points to bear in mind:

- At level 1, we simply have the two elements of $\overline{\mathbb{Q}}$ that square to 2. Calling them "positive" and "negative" is arbitrary.
- It is cleaner to replace $\sqrt[4]{6}$ by a primitive generator of the Galois extension generated by $\sqrt{2}$, $\sqrt{3}$, and $\sqrt[4]{6}$. Then that level lists each automorphism of that Galois extension exactly once.

Presentation of $\mathrm{Aut}(\overline{\mathbb{Q}})$

We view $\overline{\mathbb{Q}}$ as the union of a tower of finite Galois extensions $\mathbb{Q} = K_0 \subseteq \mathbb{Q}(z_1) = K_1 \subseteq \mathbb{Q}(z_2) = K_2 \subseteq \cdots\cdots \subseteq \cup_n K_n = \overline{\mathbb{Q}}$.
So we now have a computable (highly symmetric) tree $T_{\overline{\mathbb{Q}}}$, where each node σ at level n is an automorphism of K_n, with $\tau \sqsubseteq \sigma$ iff $\sigma \upharpoonright K_{|\tau|} = \tau$.

$\mathrm{Aut}(\overline{\mathbb{Q}})$ consists of the paths through $T_{\overline{\mathbb{Q}}}$: we will say that $f \in \mathrm{Aut}(\overline{\mathbb{Q}})$ is *computable* iff the corresponding path is computable. Each node at level n in $T_{\overline{\mathbb{Q}}}$ corresponds to a unique automorphism of K_n, and extends to countably many computable automorphisms of $\overline{\mathbb{Q}}$, as well as to continuum-many other automorphisms of $\overline{\mathbb{Q}}$.

There are Turing functionals Θ and Υ such that, for all paths $f, g \in \mathrm{Aut}(\overline{\mathbb{Q}})$, $\Theta^{f \oplus g}$ is the product $f \circ g$ and Υ^f is the inverse automorphism f^{-1}. So this is as effective a presentation as one could wish for the continuum-size structure $(\mathrm{Aut}(\overline{\mathbb{Q}}), \circ)$.

Computable automorphisms

Definition

For a Turing degree $\boldsymbol{d}$, define

$$\mathrm{Aut}_{\boldsymbol{d}}(\overline{\mathbb{Q}}) = \{f \in \mathrm{Aut}(\overline{\mathbb{Q}}) : \deg(f) \leq_T \boldsymbol{d}\}.$$

So $\mathrm{Aut}_{\mathbf{0}}(\overline{\mathbb{Q}})$ is the subgroup of all computable automorphisms of $\overline{\mathbb{Q}}$.

Question

Is $\mathrm{Aut}_{\mathbf{0}}(\overline{\mathbb{Q}})$ an elementary subgroup of $\mathrm{Aut}(\overline{\mathbb{Q}})$?

For example, let $f \in \mathrm{Aut}_{\mathbf{0}}(\overline{\mathbb{Q}})$ have the property that

$$(\exists g \in \mathrm{Aut}(\overline{\mathbb{Q}}))\ g \circ g = f.$$

Must there be a computable realization g? That is, when $f \in \mathrm{Aut}_{\mathbf{0}}(\overline{\mathbb{Q}})$ and $\mathrm{Aut}(\overline{\mathbb{Q}}) \models (\exists G)\ G \circ G = f$, does the same hold in $\mathrm{Aut}_{\mathbf{0}}(\overline{\mathbb{Q}})$?

In terms of trees....

Trying to compute some g with $f = g \circ g$, we define a decidable subtree T of $T_{\overline{\mathbb{Q}}}$:

$$T = \{\gamma \in \text{Aut}(K_n) : n \in \mathbb{N} \ \& \ \gamma \circ \gamma = f\restriction K_n\},$$

containing all "square roots of $f\restriction K_n$" in every $\text{Aut}(K_n)$.

Now the elements $g \in \text{Aut}(\overline{\mathbb{Q}})$ with $g \circ g = f$ are precisely the paths through T. So the problem of computing some such g is precisely the problem of computing a path through this T.

Open question

But does this T have a computable path or not? Some computable finite-branching trees have no computable path – but is this T really that complicated?

Examining $g \circ g = f$

Sometimes we can see how to define g. Example: say $K_m = \mathbb{Q}(\sqrt{5})$. Now $f(\sqrt{5}) = \sqrt{5}$, as f is a square. This seems to allow both $g(\sqrt{5}) = \pm\sqrt{5}$ as possibilities. But be patient....

We reach $K_n = \mathbb{Q}(\zeta_5)$, where ζ_5 is a primitive fifth root of 1, so $2(\zeta_5 + \zeta_5^4) + 1 = \sqrt{5}$. Now f has either $f(\zeta_5) = \zeta_5$ or $f(\zeta_5) = \zeta_5^4$.

- If $f(\zeta_5) = \zeta_5$, then either $g(\zeta_5) = \zeta_5$ or $g(\zeta_5) = \zeta_5^4$. In both cases,

$$g(\sqrt{5}) = g(2(\zeta_5 + \zeta_5^4) + 1) = 2(g(\zeta_5) + g(\zeta_5^4)) + 1 = \sqrt{5}.$$

- But if $f(\zeta_5) = \zeta_5^4$, then either $g(\zeta_5) = \zeta_5^2$ or $g(\zeta_5) = \zeta_5^3$. Now

$$g(\sqrt{5}) = g(2(\zeta_5+\zeta_5^4)+1) = 2(g(\zeta_5)+g(\zeta_5^4))+1 = 2(\zeta_5^2+\zeta_5^3)+1 = -\sqrt{5}.$$

So the value $f(\zeta_5)$ tells us how to define $g(\sqrt{5})$. (It does not tell us how to define $g(\zeta_5)$, but maybe some later information about f will help....)

Does this always work?

Now we try the same with $\sqrt{2}$. Again $f(\sqrt{2}) = \sqrt{2}$. But if ζ_8 is a primitive 8-th root of 1, then $\zeta_8 + \zeta_8^7 = \sqrt{2}$. So we check...

ζ_8 has conjugates ζ_8^3, ζ_8^5, and ζ_8^7. However, all four maps $\zeta_8 \mapsto \zeta_8^k$ square to the identity. (Here the Galois group is $\mathbb{Z}_2 \times \mathbb{Z}_2$, not $\mathbb{Z}/(4)$.) Therefore the only possibility for f is $f(\zeta_8) = \zeta_8$, and this tells us nothing about $g(\zeta_8)$, nor about $g(\sqrt{2})$.

So the question is: given an input z_n for g, can we always determine, from some finite portion of f, how to define $g(z_n)$?
(For $g(\sqrt{2})$, this can be determined. For $g(\sqrt{7})$, we don't know.)

If we know that no finite portion of f determines $g(z_n)$, then any choice for $g(z_n)$ will be correct. The difficulty is knowing whether to wait, or just to choose $g(z_n)$ arbitrarily right now.

Skolem functions for $\text{Aut}(\overline{\mathbb{Q}})$

A (generalized) Skolem function for $\text{Aut}(\overline{\mathbb{Q}})$, for the formula $(\exists G)\ G \circ G = F$, is a function S such that, whenever $f \in \text{Aut}(\overline{\mathbb{Q}})$ satisfies this formula, $S(f) \in \text{Aut}(\overline{\mathbb{Q}})$ with $S(f) \circ S(f) = f$.

Theorem (Kundu-M.)

There is no computable Skolem function for $\text{Aut}(\overline{\mathbb{Q}})$ for the formula $(\exists G)\ G \circ G = F$.

Proof: Given any Turing functional Φ, run Φ^{id}. If $\Phi^{\text{id}\upharpoonright K_n}(i)\downarrow = \pm i$ for some n, Kundu-M. have a mechanism yielding $f_0, f_1 \in \text{Aut}(\overline{\mathbb{Q}})$ with

- $f_0, f_1 \in (\text{Aut}(\overline{\mathbb{Q}}))^2$ with $f_0 \upharpoonright K_n = f_1 \upharpoonright K_n = \text{id} \upharpoonright K_n$.
- Every $g_0 \in \text{Aut}(\overline{\mathbb{Q}})$ with $g_0 \circ g_0 = f_0$ has $g_0(i) = i$.
- Every $g_1 \in \text{Aut}(\overline{\mathbb{Q}})$ with $g_1 \circ g_1 = f_1$ has $g_1(i) = -i$.

So either $\Phi^{f_0}(i)$ or $\Phi^{f_1}(i)$ will be incorrect!

The Mechanism

Choose a prime p so large that $\sqrt{p} \notin K_n$. Now $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{p}, i)/\mathbb{Q}) \cong D_4$, and the permutation (13)(24) of the four conjugates of $\sqrt[4]{p}$ is the square of (1234) and (1432) (and nothing else). Both (1234) and (1432) map i to i. So (13)(24) gives our f_0, whose square roots all fix i.

For f_1, which forces $g_1(i) = -i$, we use a similar trick involving extensions F containing i that have Galois group S_4 over $\mathbb{Q}$, hence have $\mathrm{Gal}(F/\mathbb{Q}(i)) \cong A_4$. Here (13)(24) is again the square of (1234) and (1432) and nothing else, and these two 4-cycles are both odd permutations, hence $\notin A_4$, and so both map i to $-i$. S_4 and A_4 are the "generic" Galois groups for degree-4 polynomials over $\mathbb{Q}$, so it is always possible to find such an extension F with $F \cap K_n = \mathbb{Q}(i)$.

Which leaves us wondering....

It remains open whether we can repeat this mechanism with other Galois extensions than $\mathbb{Q}(i)$. If we can, then it should be possible to use finite-injury to diagonalize against all computable square roots, and to build a (computable?) $f \in \text{Aut}(\overline{\mathbb{Q}})$ that is a square there, but is not a square in $\text{Aut}_{\deg(f)}(\overline{\mathbb{Q}})$. This would show that $\text{Aut}_{\deg(f)}(\overline{\mathbb{Q}})$ is not an elementary subgroup of $\text{Aut}(\overline{\mathbb{Q}})$.

The principal question is whether there are other elements of $\text{Aut}(\overline{\mathbb{Q}})$ (besides the identity) that can be expressed as squares in $\text{Aut}(\overline{\mathbb{Q}})$ in two distinct ways. But the identity and complex conjugation are very special automorphisms.

Artin-Schreier Theorem

The only elements of finite order in $\text{Aut}(\overline{\mathbb{Q}})$ are the identity, complex conjugation c, and its conjugates hch^{-1}.

Perhaps no other $f \in \text{Aut}(\overline{\mathbb{Q}})$ has more than one square root?