An overview of the Inverse Galois Problem

David Harbater, Univ. of Pennsylvania

VaNTAGe seminar, Oct. 3, 2023

Classical Inverse Galois problem (IGP):

Is every finite group a Galois group over $\mathbb{Q}$?

$$\begin{array}{l} L \\ \mid G \quad \text{Galois finite field extension} \\ \mathbb{Q} \end{array}$$

Hilbert: S_n, A_n are Galois groups over $\mathbb{Q}$.

Later: All p-groups are Galois groups over $\mathbb{Q}$.

More generally, all nilpotent groups are Galois groups over $\mathbb{Q}$.

— construct via towers of fields

$$\left.\begin{array}{l} L = K_n \\ \vdots \\ K_i \\ \vdots \\ K_1 \\ \mid \\ \mathbb{Q} = K_0 \end{array}\right] G \qquad \left.\begin{array}{l} K_i \\ \vdots \\ K_1 \\ \mid \\ \mathbb{Q} = K_0 \end{array}\right] G_i$$

Shafarevich (1950's): All solvable groups are Galois groups$/\mathbb{Q}$.

— intricate argument; can rephrase via Galois cohomology [NSW].

$$\begin{array}{ll} L & \\ \vdots & \\ K_{i+1} & \\ \mid & \text{Galois} \\ K_i & \\ \vdots & \text{not Galois} \\ \mathbb{Q} & \end{array}$$

For other groups — use Hilbert's Irreducibility Theorem (HIT):

If $\begin{array}{l} L = K[Y]/f(Y) \\ \mid G \\ K = \mathbb{Q}(x_1, \dots, x_n) \end{array}$ then can specialize x_i's to elements $\alpha_i \in \mathbb{Q}$ to get a Galois extension of $\mathbb{Q}$:

$f(Y)$ in $K[Y]$

$$\begin{array}{l} L_\alpha = \mathbb{Q}[Y]/f_\alpha(Y) \\ \mid G \\ \mathbb{Q} \end{array}$$

replace x_i by α_i in $f(Y)$.

<u>Example</u> $L = K[\sqrt{x}] = K[Y]/(Y^2 - x)$
$\quad | \; C_2$ - Galois
$K = \mathbb{Q}(x)$

If we replace x by a non-square $\alpha \in \mathbb{Q}$, get C_2-Galois field extension $\mathbb{Q}(\sqrt{\alpha})$
$\quad | \; C_2$
$\mathbb{Q}$

So <u>if</u> we can find a G-Galois extension of $\mathbb{Q}(x_1, \dots, x_n)$, then we get a G-Galois extension of $\mathbb{Q}$.

How to carry this out?

<u>Noether problem</u>: Given a finite group $G \hookrightarrow S_n$, let G act on $\{z_1, \dots, z_n\}$ by permutations and take the fixed field: $E = \mathbb{Q}(z_1, \dots, z_n)$

$$\begin{array}{c} E = \mathbb{Q}(z_1, \dots, z_n) \\ | \\ F = \mathbb{Q}(z_1, \dots, z_n)^G \end{array}$$

G-Galois field extension

transcendence degree n over $\mathbb{Q}$.

Is F purely transcendental over $\mathbb{Q}$?
i.e. Is $F \cong \mathbb{Q}(X_1, \dots, X_n)$?

If so, then Hilbert's Irreducibility Theorem
$\Rightarrow$ G is a Galois group over $\mathbb{Q}$.

1st case: $G = S_n$, acting on $\{z_1, \dots, z_n\}$.

The field of invariants $= \mathbb{Q}(\sigma_1, \dots, \sigma_n)$, purely transcendental.

elementary symmetric polynomials

So get S_n as a Galois group over $\mathbb{Q}$ (again)

What about for <u>other</u> groups G?

Is $\mathbb{Q}(z_1,\dots,z_n)^G$ purely transcendental over $\mathbb{Q}$?

E.g. Cyclic groups C_n? Yes for $n=2,3,4,5,6,7$

<u>No</u> for $n=8$ (Lenstra, Saltman; related to the exceptional case of Grunwald–Wang Theorem).

First no with n prime: $n=47$ (Swan)

So can't use this method of invariants to get <u>all</u> finite groups$/\mathbb{Q}$.

But can do more with Hilbert's Irreducibility Theorem.

Say <u>IGP holds for a field K</u> if every finite group is a Galois group over K.

By HIT, $IGP/\mathbb{Q}(x) \Rightarrow IGP/\mathbb{Q}$.

How to understand Galois extensions of $\mathbb{Q}(x)$?

$$\begin{array}{c} E \\ \Big| \, G \\ F = \mathbb{Q}(x) \end{array} \qquad \text{E.g.} \quad \begin{array}{c} E = \mathbb{Q}(\sqrt{x}) = F[Y]/(Y^2-x). \\ \Big| \, C_2 \\ F = \mathbb{Q}(x) \end{array}$$

Suppose $\mathbb{Q}$ is algebraically closed in E. As in example

Then can base change to $\mathbb{C}$: $\cdot \otimes_{\mathbb{Q}} \mathbb{C}$:

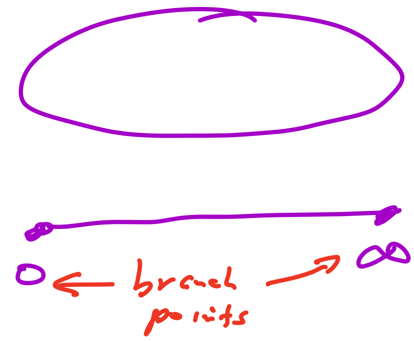
$$\begin{array}{c} E_{\mathbb{C}} = E \otimes_{\mathbb{Q}} \mathbb{C} \\ \Big| \\ F_{\mathbb{C}} = \mathbb{C}(X) \end{array}$$

Still Galois with group G. (E, $\mathbb{C}$ are linearly disjoint$/\mathbb{Q}$)

$$\text{E.g.} \quad \begin{array}{c} \mathbb{C}(x)[Y]/(Y^2-x) \\ \Big| \, C_2 \\ \mathbb{C}(x) \end{array}$$

In this example, have a Galois extension of complex function fields, corresponding to a Galois branched cover of complex curves:

$$\begin{array}{lll} Y & (y\text{-line}) & \\ \downarrow C_2 & & y^2 = x. \\ X = \mathbb{P}^1 & (x\text{-line}) & \end{array}$$



This is unramified (étale) away from finitely many points (branch points).

Over the complex metric topology, it's a covering space over $\mathbb{C} - \{0\}$, with C_2 = group of deck transformations.

More generally, whenever we have

$$\begin{array}{c} E \\ |\, G \\ F = \mathbb{Q}(x) \end{array}$$

s.t. E is <u>regular</u> over $\mathbb{Q}$ (i.e. $\mathbb{Q}$ alg. closed in E), we get a G-Galois branched cover of $\mathbb{P}^1_{\mathbb{C}}$, & a covering space of some $U = S^2 - \{P_0, \ldots, P_n\}$ $(n \geq 0)$ with G = group of deck transformations.

(Field thy) $\longrightarrow$ (Cx. alg. geom.) $\longrightarrow$ (Topology)

Can we reverse this process, to get Galois groups over $\mathbb{Q}(x)$ (& hence $/\mathbb{Q}$) via topology?

To do this, first need to understand Galois topological covers of $U = S^2 - \{P_0, \dots, P_n\}$, $n \geq 0$.

— i.e. group G of deck transformations acts simply transitively on the fibers of a given point.

$$\begin{tikzcd}
\tilde{U} \arrow[dd, "\pi_1(U)"'] \arrow[dr, "N \triangleleft \pi_1(U)"] & \\
& V \arrow[dl, "G"] \\
U &
\end{tikzcd}$$

$\tilde{U}$ = universal cover of U

$N \triangleleft \pi_1(U)$, normal subgroup of finite index

$U = S^2 - \{P_0, \dots, P_n\}$

$$G = \pi_1(U)/N$$

$\pi_1(U) \cong F_n$, free group on n generators

So for a given choice of $U = S^2 - \{P_0, \dots, P_n\}$, the (Galois) groups of deck transformations that arise are the finite groups on n generators.

So <u>every</u> finite group G arises topologically for some U.

Now want to reverse the above process to get Galois groups over $\mathbb{Q}(x)$ and $\mathbb{Q}$:

(Field thy) $\leftarrow$ (Cx. alg. geom.) $\leftarrow$ (Topology)

To go from topology to complex algebraic geometry: need that every finite covering space over $U = S^2 - \{P_0, \ldots, P_n\}$ is induced by an étale cover of $U = \mathbb{P}^1_{\mathbb{C}} - \{P_0, \ldots, P_n\}$, or equivalently by a branched cover of $\mathbb{P}^1_{\mathbb{C}}$ (with branch locus $\{P_0, \ldots, P_n\}$).

This is by Riemann's Existence Theorem (which follows from Serre's GAGA).

Next, want to pass from complex algebraic geometry to field theory.

Taking function fields above, we get:

Every finite group is a Galois group / $\mathbb{C}(x)$.
(IGP / $\mathbb{C}(x)$)

Now want to descend to $\mathbb{Q}(x)$:

$$\begin{tikzcd}
\exists ?\, L_0 \arrow[d, dash, "G"'] \arrow[r, dash] & L \arrow[d, dash, "G"] \\
\mathbb{Q}(x) \arrow[r, dash] & \mathbb{C}(x)
\end{tikzcd}$$

Equivalently, given

$$\begin{tikzcd} Y \arrow[d, "\varphi"', "G"] \\ X = \mathbb{P}^1_{\mathbb{C}} \end{tikzcd}$$

unramified away from $\{P_0, \dots, P_n\}$,

is it induced by a G-Galois cover of $\mathbb{P}^1_{\mathbb{Q}}$?

Here $Y \xrightarrow{\varphi} X$ is given by polynomial equations $/\mathbb{C}$, as are the automorphisms of Y over X ($\leftrightarrow$ elements of G).

Can we choose these polynomials to have coefficients in $\mathbb{Q}$?

For simplicity, assume $P_0, \dots, P_n$ are $\mathbb{Q}$-points of $\mathbb{P}^1$ (e.g. $P_j = j$).

Then by a theorem of Grothendieck,

$Y \xrightarrow{\varphi} X$ and its automorphisms are defined over $\overline{\mathbb{Q}}$.

Since these polynomials have finitely many coefficients,

we get G as a (regular) Galois group of an extension $\begin{array}{c} L \\ | \\ K(x) \end{array}$ for <u>some</u> number field K

a field of definition of $L/\mathbb{C}(x)$

For <u>which</u> choices of K? Does $\mathbb{Q}$ work?

If $\mathbb{Q}$ works, then if $\omega \in \mathrm{Gal}(\mathbb{Q}) := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, & if apply ω to all the coefficients of the defining polynomials of $Y \xrightarrow{\varphi} X$ and its automorphisms, we get back the <u>same</u> cover (and automorphisms).

Can write:

cover transformed by ω

$$\begin{tikzcd} Y^\omega \arrow[rr, phantom, "\cong"] \arrow[dr, "G"'] & & Y \arrow[dl, "G"] \\ & X = \mathbb{P}^1 & \end{tikzcd}$$

To understand the action of $\mathrm{Gal}(\overline{\mathbb{Q}})$ on covers:

Use classification of covers of $U = S^2 - \{P_0, \dots, P_n\}$

by the finite quotients of $\pi_1(U) = \langle a_0, \dots, a_n \mid a_0 \cdots a_n = 1 \rangle$.
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \cong F_n$

— viz. by finite groups G together with generators $g_0, \dots, g_n$ such that $g_0 \cdots g_n = 1$. $(*)$

A technical point: These are for <u>pointed</u> covers (because of the base point of π_1). If we change the base point from $Q \in Y$ to $Q' \in Y$, say $Q' = g(Q)$, $g \in G$, then $(g_0, \dots, g_n)$ is uniformly conjugated by g.

So

$$\begin{tikzcd} Y \arrow[d, "G"'] \\ X = \mathbb{P}^1 \end{tikzcd} \quad \longleftrightarrow \quad (G; g_0, \dots, g_n)/\sim$$

unramified away from $\{P_0, \dots, P_n\}$ $\qquad$ s.t. $(*)$

uniform conjugation

By a local analysis of covers (looking at complete local rings about the branch points), one gets for $\omega \in \mathrm{Gal}(\overline{\mathbb{Q}})$:

If $\begin{array}{c} Y \\ G \circlearrowleft \downarrow \\ X \end{array} \leftrightarrow (G; g_0, \dots, g_n)/\sim$ and $\begin{array}{c} Y^\omega \\ G \circlearrowleft \downarrow \\ X \end{array} \leftrightarrow (G; h_0, \dots, h_n)/\sim$

then $g_j \sim h_j^{\chi(\omega)}$

cyclotomic character

conjugacy in G

I.e. if $\theta(g_j) = r_j$, and $\omega(\zeta_{r_j}) = \zeta_{r_j}^{c_j}$, then $g_j \sim h_j^{c_j}$.

This gives a partial formula for Y^ω in terms of Y.

But only partial, because we know the h_j's only up to individual conjugacy, not up to uniform conjugacy.

So there is a finite amount of ambiguity in determining Y^ω.

But sometimes: it turns out there's no ambiguity — the phenomenon of rigidity:

Say we have $(G; g_0, \dots, g_n)/\sim \leftrightarrow \begin{array}{c} Y \\ \downarrow \\ \mathbb{P}^1 \end{array}$, as above.

Let $C_i \subset G$ be the conjugacy class of $g_i \in G$.

Let $\Sigma = \{(h_0, \dots, h_n) \mid h_0, \dots, h_n \text{ generate } G,\ \prod h_i = 1,\ h_i \in C_i\}$.

includes all possible descriptions of $\begin{array}{c} Y^\omega \\ \downarrow \\ \mathbb{P}^1 \end{array}$

Say $(G; g_0, \dots, g_n)$ (or $(G; C_1, \dots, C_n)$)

is rigid if all the elements of Σ are uniformly conjugate to each other (in particular, to $(g_0, \dots, g_n)$).

Suppose in addition, if we write $N := |G|$, and if $\forall r \in (\mathbb{Z}/N)^\times$ $(g_0^r, \dots, g_n^r) \sim (g_0, \dots, g_n)$, then we say $(G; g_0, \dots, g_n)$ is <u>rationally rigid.</u>

In this case, for $\begin{array}{c} Y \\ \downarrow G \\ \mathbb{P}^1 \end{array} \leftrightarrow (G; g_0, \dots, g_n)$ and $\begin{array}{c} Y^\omega \\ \downarrow G \\ \mathbb{P}^1 \end{array} \leftrightarrow (G; h_0, \dots, h_n)$,

we have $(g_0, \dots, g_n) \sim (h_0, \dots, h_n)$ (uniformly),

so
$$\begin{tikzcd} Y \arrow[rr, "\sim"] \arrow[dr, "G"'] & & Y^\omega \arrow[dl, "G"] \\ & \mathbb{P}^1 & \end{tikzcd}.$$
So $Gal(\overline{\mathbb{Q}})$ leaves $\begin{array}{c} Y \\ \downarrow G \\ \mathbb{P}^1 \end{array}$ fixed.

"$\mathbb{Q}$ is the field of moduli of the cover".

Under some conditions on G (e.g. trivial center, or abelian) this implies $\begin{array}{c} Y \\ \downarrow G \\ \mathbb{P}^1 \end{array}$ is <u>defined</u> over $\mathbb{Q}$.

So then G is a Galois group over $\mathbb{Q}(x)$, and so over $\mathbb{Q}$.

<u>A variant</u>: if the $(G; g_0, \dots, g_n)$ is rigid but not rational, then we still get that $\begin{array}{c} Y \\ \downarrow G \\ \mathbb{P}^1 \end{array}$ is defined over $\mathbb{Q}(\zeta_N)$ above, $N = |G|$

in fact over a computable subfield of $\mathbb{Q}(\zeta_N)$.

In particular, get that it's defined over $\mathbb{Q}^{ab}$.

HIT holds over number fields, and over $\mathbb{Q}^{ab}$ (these fields are "Hilbertian"), so get those groups as Galois groups over those fields.

The notion of rigidity was defined in the early 1980's independently by Belyi, Matzat, Thompson, following related work of Shih and Fried.
This notion was then used to realize many finite simple groups as Galois groups over $\mathbb{Q}$ — in fact, regularly, giving evidence for the Regular Inverse Galois Problem (RIGP) / $\mathbb{Q}$:
every finite group is a regular Galois group / $\mathbb{Q}$:

$$\begin{array}{c} E \\ G \big| \\ \mathbb{Q}(x) \end{array}$$

where $\mathbb{Q}$ is alg. cl. in E.

In particular, among the 26 sporadic finite simple groups, all are Galois groups over $\mathbb{Q}$ except possibly the Mathieu group M_{23}.
So the other simple Mathieu groups (M_{11}, M_{12}, M_{24}) do occur, and so does the Monster group (of order $\approx 8 \cdot 10^{53}$).
Many of the other finite simple groups (in families) have also been shown to be Galois groups over $\mathbb{Q}$, mostly using rigidity (e.g. $PSL_2(\mathbb{F}_p)$ for most p; the rest by another method [Zywina]).

But how to carry out the computations, given the size of the groups?
Answer: by character theory.

Namely, recall that given conjugacy classes $C_1, \dots, C_n \subset G$,

$$\Sigma = \{(h_1, \dots, h_n) \mid h_1, \dots, h_n \text{ generate } G, \prod h_i = 1, h_i \in C_i\}.$$

Rigidity holds if Σ consists of a single uniform conjugacy class.

Say $Z(G) = 1$. (e.g. G non-abelian simple)

Then rigidity $\Leftrightarrow |\Sigma| = |G|$ (since G acts freely on Σ; must have $\geq$)

$$\Sigma \subseteq \bar{\Sigma} = \{(h_1, \dots, h_n) \mid \prod h_i = 1, h_i \in C_i\}.$$

So if $|\bar{\Sigma}| = |G|$ then $\Sigma = \bar{\Sigma}$ and so have rigidity.

Formula:

$$|\bar{\Sigma}| = \frac{|G|^n}{\prod_i |Z(g_i)|} \sum_{\chi \in X(G)} \prod_i \chi(g_i) / \chi(1)^{n-1}$$

Can compute this using the Atlas of Finite Groups.

E.g. for the monster group, get (rational) rigidity for (g_1, g_2, g_3) of orders 2, 3, 29.

Over $\mathbb{Q}^{ab}$, even more groups are known to be Galois groups, since don't need rationality — just rigidity.

In particular, all the sporadic simple groups occur over $\mathbb{Q}^{ab}$.

(For more detail: [MM], [Völ], [Ser] books on inverse Galois theory)

Going further than IGP:

What is the structure of $Gal(\mathbb{Q})$ as a profinite group?

This group is infinitely generated as a topological group, & if IGP holds then every finite group is a quotient. But this does not determine $Gal(\mathbb{Q})$

Note: A (topologically) finitely generated profinite group is determined by the set of its finite quotients.
But false for infinitely generated profinite groups.

In fact, if IGP holds for all number fields K (as expected), then the groups $Gal(K)$ all have the same set of finite quotients. But by a theorem of Neukirch, non-isomorphic number fields K have non-isomorphic absolute Galois groups $Gal(K)$. (Related to Grothendieck's anabelian conjecture.)

There is no (reasonable) conjecture about the structure of $Gal(\mathbb{Q})$ in terms of generators and relations (Though it is conjecturally isomorphic to $\widehat{GT}$).

But for $\mathbb{Q}^{ab}$, there is

<u>Conj.</u> (Shafarevich) $Gal(\mathbb{Q}^{ab}) = Gal(\bar{\mathbb{Q}}/\mathbb{Q}^{ab})$ is isomorphic to the free profinite group on countably many generators.

This is open, but there is

<u>Theorem</u> (Iwasawa'53) $Gal(\mathbb{Q}^{solv}/\mathbb{Q}^{ab})$ is isomorphic to the free prosoluble group on countably many generators.

How to show that a profinite group is free?

<u>Theorem</u> (Iwasawa) A countably generated profinite group Γ is free iff every finite embedding problem is soluble.

Terminology:

A finite embedding problem

$$\begin{tikzcd} & \Gamma \arrow[d] \arrow[dl, dashed, "\exists ?"'] \\ G \arrow[r, two heads] & H \end{tikzcd}$$

a solution

finite groups

Why an "embedding problem"? Because of Galois theory: If $\Gamma = Gal(K)$, it asks if every H-Galois extension of K embeds in a G-Galois extension of K.

Another question:

Which finite groups are Galois groups of an extension $K/\mathbb{Q}$ that is ramified only at a given set of primes?

Conj (Boston–Markin) If $G/[G,G]$ can be generated by d elements, then $G = \mathrm{Gal}(K/\mathbb{Q})$ for some K ramified $/\mathbb{Q}$ at d primes (incl ∞).

Conj (DH) $\exists\, C>0$ s.t. $\forall\, n>0$, if $\begin{matrix} K \\ | \, G \\ \mathbb{Q} \end{matrix}$ is (tamely) ramified just at primes dividing n (and maybe ∞), G can be generated by $\leq \log(n) + C$ elements.

There are also partial results on which finite groups can be Galois groups over $\mathbb{Q}$ ramified only at p (and maybe ∞) for small p. But in general: mysterious.

What about IGP over other fields?

The above suggests:

<u>Conjecture</u> (Regular Inverse Galois Problem — RIGP)

For <u>every</u> field K, and every finite group G, there is a G-Galois extension $L/K(x)$ with K algebraically closed in L.

As noted above: true for $K = \mathbb{C}, \bar{\mathbb{Q}}$; & expect it to hold for K a number field and for $K = \mathbb{Q}^{ab}$.

If RIGP holds for a Hilbertian field K, then have IGP for K.

RIGP for K a finite field $\mathbb{F}_q$?

$\mathbb{F}_q(x)$ is analogous to a number field, so expect this to hold. And should be easier than for number fields. But still open.

Weak form known: $\forall$ finite groups G $\exists n \geq 1$ such that G is a Galois group over $k(x)$ for every finite field k s.t. $|k| \geq n$.
(Pop, Fried, Jarden) (Uses Weil bound on $|X(k)|$.) ← curve

RIGP for other fields? How to generalize RIGP for $\mathbb{C}$?
Hint: $\mathbb{C}$ is algebraically closed and complete.

Theorem (D.H.) If K is algebraically closed, or if K is a complete discretely valued field, then RIGP holds for K.

So true for $\bar{\mathbb{F}}_p$, $\mathbb{Q}_p$, $k((t))$, etc.
(Also true for $K = \operatorname{frac} R$, for R any complete local domain that is not a field; e.g. $k((x,y)) = \operatorname{frac} k[[x,y]]$.)

Idea of proof:

For complete case — e.g. $K = \mathbb{Q}_p$:

Given G, want to build a G-Galois branched cover of $\mathbb{P}^1_{\mathbb{Q}_p}$.

Do so locally in the p-adic topology, s.t. locally cyclic, and s.t. the local covers agree on overlaps

(e.g. trivial on overlaps). Now patch together, p-adic analytically, to get the desired cover.

For this last step, can use Grothendieck's theory of formal schemes (motivated by work of Zariski) or the theory of rigid analytic spaces (begun by Tate).

For the algebraically closed case: Want RIGP / $k = \bar{k}$.

Let $K = k((t))$. By the complete case, get RIGP for K.

So have $\begin{array}{c} L \\ \mid G \\ K(x) \end{array}$. The equations defining L involve only finitely many Laurent series.

So $L/K(x)$ is induced by $\begin{array}{c} B \\ \mid \\ A[x] \end{array}$ $B \leftarrow$ generically G-Galois over $A[x]$; $A[x] \leftarrow$ finitely generated k-subalgebra of K

So have a G-Galois branched cover of $\mathbb{P}^1_A = \mathbb{P}^1_k \times V$ ($V \leftarrow \operatorname{Spec}(A)$).

Picking a suitably general k-point P of V, and taking the fiber of $\mathbb{P}^1_k \times V$ over P, we get a G-Galois branched cover of $\mathbb{P}^1_k$. ✓

The above argument used that k is algebraically closed to get that every smooth k-variety with a k-point has <u>infinitely</u> many k-points.

Pop called a field <u>large</u> if it has that property.
some say "ample"

e.g. alg. closed fields, $\mathbb{R}$, $\mathbb{Q}_p$, $\mathbb{Q}^{tr}$, ...

Get <u>Thm</u> (Pop) RIGP holds for large fields.

(The case of $\mathbb{R}$ was shown much earlier by Krull and Neukirch.)

What about the structure of $\mathrm{Gal}(K(x))$ as a profinite group?

Case $K=\mathbb{C}$: $\mathrm{Gal}(\mathbb{C}(x))$ is a free profinite group of uncountable rank $(=|\mathbb{C}|)$. Due to Douady

Rough idea: Galois extensions of $\mathbb{C}(x)$

$\updownarrow$

Galois branched covers of $\mathbb{P}^1_{\mathbb{C}}$

If branched at $S=\{P_0, \ldots, P_n\}$, $P_0 = \infty$, it has generators $a_1, \ldots, a_n$.

Max'l extension of $\mathbb{C}(x)$ ramified only at S has Galois group <u>free</u> on generators $\leftrightarrow P_1, \ldots, P_n \in \mathbb{C}$.

In limit as S grows, get free profinite group on all the elements of $\mathbb{C}$.

What about $\mathrm{Gal}(K(x))$ for <u>other</u> alg. closed fields K?
In char p, due to wild ramification, the Galois group of the maximal extension ramified just at a finite set S is <u>not</u> free.

So expect $\mathrm{Gal}(K(x))$ to be a limit of non-free groups, in char p.

Nevertheless:

<u>Theorem</u> (D.H., Pop) If $K = \bar{K}$ then $\mathrm{Gal}(K(x))$ is a free profinite group on $|K|$ generators.

The proof involves passing to $K((t))$, and patching in the t-adic topology, to solve embedding problems to obtain freeness.
Here, if $|K|$ is uncountable, Iwasawa's thm doesn't suffice.
Instead, use a more general result:

<u>Theorem</u> (Melnikov, Chatzidakis). Let Γ be a profinite group, and m an infinite cardinal. Then Γ is free of rank m iff every non-trivial finite embedding problem for Γ has exactly m solutions.

For $K = \overline{\mathbb{F}}_p$, the above freeness result says:
$\mathrm{Gal}(\overline{\mathbb{F}}_p(x))$ is free of countable rank.
Since $\overline{\mathbb{F}}_p(x)$ is the maximal cyclotomic extension of $\mathbb{F}_p(x)$,
and since $\mathbb{F}_p(x)$ is analogous to $\mathbb{Q}$, this freeness
is analogous to the freeness of $\mathrm{Gal}(\mathbb{Q}^{ab}) = \mathrm{Gal}(\mathbb{Q}^{cycl})$,
which was conjectured by Shafarevich.

So can view the above freeness result as a geometric
analog of Shafarevich's conjecture.
(Also, $\mathrm{Gal}(\mathbb{F}_p(x)^{ab})$ is free as well; result of D.H.)

What about Galois groups with prescribed ramification?
There are just fragmentary results for $K = \mathbb{Q}$;
somewhat more for $\mathbb{F}_p(x)$ (and other global function fields).
But we know more for $k(x)$ with k alg. closed.

If $k = \mathbb{C}$, & $S = \{P_0, \ldots, P_n\} \subset \mathbb{C}$, $n \geq 0$, then as we saw,
the finite Galois groups over $\mathbb{C}(x)$ ramified just at S
are the groups on $\leq n$ generators.

More generally, if X is a smooth projective curve / $\mathbb{C}$ of genus $g \geq 0$, and $S = \{P_0, \ldots, P_n\} \subset X$, $n \geq 0$, then $\pi_1(X - S)$ is free of rank $2g+n$, and so the finite Galois groups over $\mathbb{C}(X)$ ramified just at S are the groups on $2g+n$ generators.

If $k = \bar{k}$ of characteristic 0, then the same conclusions hold. Shown by Grothendieck in SGA 1, by relating k to $\mathbb{C}$, and using the result for $\mathbb{C}$.

What about $k = \bar{k}$ of characteristic $p > 0$?
Then false.

Ex. $X = \mathbb{P}^1$, $n = 0$, $P_0 = \infty$, $U = X - \{P_0\} = \mathbb{A}^1$.
There is a non-trivial Galois unramified cover of U, given by $y^p - y = x$. (Artin-Schreier cover).
So $\mathbb{A}^1$ is not simply connected in characteristic p.
The above cover has Galois group $= C_p$.
In fact, every finite p-group is a Galois group over U.

alg. closed

So what finite groups should occur over $\mathbb{A}^1_k$ in char p?
And more generally, over $U = X - S$ in char p?

smooth projective curve / $k = \bar{k}$ of genus g

finite set, $\{P_0, \ldots, P_n\}$

In 1957, Abhyankar Conjectured:

Let X be a smooth projective curve of genus g over an algebraically closed field of char p. Let $S = \{P_0, \ldots, P_n\} \subset X$, $n \geq 0$. Then:

The finite groups G that are Galois groups of unramified covers of $U = X - S$ are those such that every prime-to-p quotient of G can be generated by $2g+n$ elements.

In particular, if $X = \mathbb{P}^1$ and $n=0$, it says: for $U = \mathbb{A}^1$, we get the set of quasi-p groups: those with no prime-to-p quotients (Equivalently: those generated by their p-subgroups)

The case of $\mathbb{A}^1$ was proven by Raynaud, using rigid patching. Then the general case by DH, by formal patching.

So we know the finite Galois groups over affine curves $U = X - S$ over $k = \bar{k}$ of char p.

But what is the structure of the (profinite) Galois group $\pi_1(U)$ of the max'l extension ramified only over S?

(Difficulty: $\pi_1(U)$ is infinitely generated, in char p.)

Conjecture: $\pi_1(U)$ determines U (and in particular determines k).

(Related to anabelian conjecture.)

Just a bit is known:

Thm (Tamagawa) Let $U_0 = \mathbb{A}^1_{\overline{\mathbb{F}}_p}$. If $\pi_1(U) \cong \pi_1(U_0)$ then $U \cong U_0$ as schemes.

But otherwise it is open.

References:

[MM] G. Malle, B.H. Matzat. Inverse Galois Theory.

[Ser] J.-P. Serre. Topics in Galois Theory.

[Völ] H. Völklein. Groups as Galois Groups.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg. Cohomology of Number Fields.