Inverse Galois Problem

Homepage: https://people.maths.bris.ac.uk/~matyd/InvGal/
Magma package, Exercises, Research Problems, Lecture notes, Links to videos.
TA Shiva Chidambaram

LECTURE 1

Suggested exercises Q1, Q2, Q3

§1 Galois theory

k field ← think $\mathbb{Q}$

$\bar{k}$ algebraic closure

$f \in k[x]$ of degree d, roots $\alpha_1, \dots, \alpha_d$ in $\bar{k}$

Always assumed separable: α_i distinct ($\iff \gcd(f, f') = 1$).

$K = k(\alpha_1, \dots, \alpha_d)$ finite Galois extension.

$G = \mathrm{Gal}(K/k) := \mathrm{Aut}(K/k)$ Galois group.

k

Rmk
- $G \curvearrowright \{\alpha_1, \dots, \alpha_d\} \rightsquigarrow G \hookrightarrow S_d$
- Reordering roots α_i gives a conjugate subgroup in S_d.
- G transitive (one orbit on $\alpha_1, \dots, \alpha_d$) $\iff$ f irreducible (Exc.)

Transitive subgroups of S_d have been classified for $d \leq 48$

2t1 C_2	3t1 C_3	4t1 C_4		48t1	
	3t2 S_3	4t2 C_2^2	...	$\vdots$	...
		4t3 D_4		48t195826352	
		4t4 A_4			
		4t5 S_4			

Magma:
```
G:=TransitiveGroup(d,j);
j,d:=TransitiveGroupIdentification(G);
```

- Every finite G is a transitive subgroup of S_d for some d. (take $d = |G|$ and let G act on itself by left mult. – regular action).
- Most groups G have several transitive actions

transitive actions of G $\overset{1:1}{\longleftrightarrow}$ conj. classes of sgps $H < G$

$G/H \longmapsfrom H$

degree $\longleftrightarrow$ index $(G:H)$

$\mathrm{core}(H) := \bigcap_{g \in G} gHg^{-1}$

largest normal sgp of G contained in H.

Ex $\quad G = S_3$ has two trivial core sgps up to conjugation

$C_2 < S_3$ $\qquad S_3/C_2$ = usual action of S_3 on 3 points $\quad [3t2]$

$C_1 < S_3$ $\qquad S_3/C_1$ = regular action of S_3 on 6 points $\quad [6t2]$

From the point of view of Galois theory, these correspond to different fields with the same Galois closure:

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_3, \sqrt[3]{3}) \arrow[dl, dash, "C_2"'] \arrow[dd, dash, "C_3"'] \arrow[ddd, dash, bend left=60, "S_3"'] & \\
\mathbb{Q}(\sqrt[3]{3}) \arrow[ddr, dash, "f_1 = x^3-3"'] & & \\
 & \mathbb{Q}(\zeta_3) \arrow[d, dash] & \\
 & \mathbb{Q} & f_2 = x^6+3
\end{tikzcd}$$

$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \curvearrowright$ roots of x^3-3 as $3t2$

$\curvearrowright$ roots of x^6+3 as $6t2$

Rmk Some groups, e.g. G = abelian (exc.) or $G = Q_{2^m}$ (generalised quaternion) have only regular transitive action, and so can only come from irr. polys of degree $|G|$ as Galois groups.

Sometimes convenient to order groups

- by their order $\quad \leftarrow$ takes 10623531 gps to get to S_6

sometimes

- by transitive group id $\quad \leftarrow$ takes 30 gps to get to S_6, but never get to C_{49}

§2 Inverse Galois Problem

One of the biggest unsolved problems in number theory!

G finite group. I.G.P. :

Conj $\mathcal{I}_{G/\mathbb{Q}}$ There is $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) = G$.

Conj $\mathcal{I}_{G/\mathbb{Q}(t)}$ There is regular $K/\mathbb{Q}(t)$ with $\mathrm{Gal}(K/\mathbb{Q}(t)) = G$.

$K \cap \overline{\mathbb{Q}} = \mathbb{Q}$ also called geometric

equivalently K has no subfields constant over $\mathbb{Q}$, except $\mathbb{Q}$.

We will be interested in regular families over $\mathbb{Q}(t_1, \dots, t_n)$ as well, and usually denote variables $a, b, \dots$ in place of $t_1, t_2, \dots$

Ex $G = S_3$

$x^3 - 3$ $\Rightarrow \mathcal{I}_{S_3/\mathbb{Q}}$ is true.

$x^3 - a$ not regular, $K \supseteq \mathbb{Q}(\zeta_3)$

$x^3 + x + a$ regular, $K \supseteq \mathbb{Q}(\sqrt{-27a^2 - 4})$ $\Rightarrow \mathcal{I}_{S_3/\mathbb{Q}(a)}$ is true.

Inverse Galois Problem over other base fields in place of $\mathbb{Q}$, $\mathbb{Q}(t)$:

- $k = \mathbb{R}, \mathbb{C}$ Every ext. of k has degree ≤ 2 $\rightsquigarrow$ I.G.P. trivially false.
- $k = \mathbb{F}_q$ Every ext. of k is cyclic $\rightsquigarrow$ — " —
- $k = \mathbb{Q}_p$ Every ext. of k is soluble $\rightsquigarrow$ — " —
- $k = \mathbb{C}(t)$ I.G.P. true for every finite G ← essentially Riemann's existence theorem
- $k = \mathbb{Q}_p(t)$ I.G.P. true for every finite G (Harbater)

$k = \mathbb{Q}$ or any number field $\mathcal{I}_{G/k}$, $\mathcal{I}_{G/k(t)}$ expected to hold,

but not known — many methods (reviewed briefly in this course)

but none seem to be strong enough to work for all G.

We will also focus on the explicit version of $\mathcal{I}_{G/\mathbb{Q}(t)}$ — how to construct K?

~~even~~ harder!!

§3 Brief history

- $\mathcal{I}_{G/\mathbb{Q}(t)} \Rightarrow \mathcal{I}_{G/\mathbb{Q}}$, $S_n/\mathbb{Q}(t)$, $A_n/\mathbb{Q}(t)$ Hilbert 1892
- G soluble / $\mathbb{Q}$ Scholz-Reichardt (1937, odd nilpotent), Shafarevich 1989, Neukirch-Schmidt-Winberg 2000 $\Big\}$ non-constructive

G soluble / $\mathbb{Q}(t)$ unknown. $\leftarrow$ even for ℓ-groups, e.g. 3 gps of order 64

- Many simple groups via rigidity: Shih, Malle, Matzat, Belyi, Thompson, ...
  e.g. all sporadic groups but M_{23} are known $/\mathbb{Q}(t)$; see Problem P2
- All transitive groups of degree ≤ 15 $/\mathbb{Q}(t)$ Klüners-Malle 2000
  TD 2021 (constructive).

Databases $/\mathbb{Q}, \mathbb{Q}(t)$: Jones-Roberts, Smith, Klüners-Malle, LMFDB.

§4 Hilbert's Irreducibility Theorem

<u>Thm</u> (Hilbert 1892) $f(t,x) \in \mathbb{Q}(t)[x]$ irreducible polynomial. Then for infinitely many $r \in \mathbb{Q}$, the specialisation $f(r,x) \in \mathbb{Q}[x]$ is irreducible.
[in fact, for "most" r]

<u>Rmk</u> Implies more general version for N polynomials $f_i(t_1, \ldots, t_m, x_1, \ldots, x_n)$.

Fields over which Hilbert's Thm is true are called <u>Hilbertian</u>

e.g. $\mathbb{Q}$, number fields, $\mathbb{Q}^{ab}$, $\mathbb{Q}(t_1, \ldots, t_n)$, are Hilbertian

but $\mathbb{F}_q$ is not : $x^4 + t x^2 + 1 \in \mathbb{F}_q(t)[x]$ irreducible $(2 \nmid q)$

$C_2 \times C_2$-family Family(4,2)

but every specialisation $t = r \in \mathbb{F}_q$ gives a reducible polynomial in $\mathbb{F}_q[x]$.

<u>Cor</u> If G is a Galois group over $\mathbb{Q}(t_1, \ldots, t_n)$ then G is a Galois group over $\mathbb{Q}$, and

⚠ $\mathcal{I}_{G/\mathbb{Q}(t)} \Rightarrow \mathcal{I}_{G/\mathbb{Q}}, \mathcal{I}_{G/k}$ for every number field k.

uses regular.

In other words, <u>one</u> regular family over $\mathbb{Q}(t)$ gives infinitely many G-extensions over any number field!

Thm (Hilbert) S_n is a Galois group over $\mathbb{Q}$ for every $n \geq 1$. $(\mathcal{I}_{S_n/\mathbb{Q}})$

Pf First, realise S_n over $\mathbb{Q}(a_1, \dots, a_n)$

$\alpha_1, \dots, \alpha_n$ interterminants $\rightsquigarrow$ $S_n \circlearrowright K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$

$\circlearrowleft$
S_n

Field of invariants $k = K^{S_n} = \mathbb{Q}(\alpha_1, \dots, \alpha_n)^{S_n} = \mathbb{Q}(a_1, \dots, a_n)$

a_i = i^{th} elementary symmetric function in $\alpha_1, \dots, \alpha_n$

$(a_1 = \alpha_1 + \dots + \alpha_n, \dots, a_n = \alpha_1 \alpha_2 \cdots \alpha_n)$

K

$|\, S_n$

$k = \mathbb{Q}(a_1, \dots, a_n)$ $\leftarrow$ purely transcendental $/\mathbb{Q}$ $\Rightarrow$ done.

Now Hilbert Irreducibility $\Rightarrow$ S_n is a Galois group $/\mathbb{Q}$ ∎

Thm (Hilbert) A_n is a Galois group over $\mathbb{Q}$ for every $n \geq 1$.

Proof Exercise Q7. see also Problem P3