The Inverse Galois Problem

David P. Roberts
University of Minnesota, Morris

1. Polynomials, fields, and their invariants: A degree n number field K has a discriminant $D \in \mathbb{Z}$ and a Galois group $G \subseteq S_n$.

2. The inverse Galois problem: given (D, G), find all corresponding K.

3. Two relevant databases

4. Various major themes

5. Some more fields with interesting (D, G)

Goal: A broad survey, with at most tiny indications of proofs

1. Polynomials, fields, and their invariants. Factoring a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ modulo primes p gives intriguing data:

p	$x^7 - 7x - 3$ factored in $\mathbb{F}_p[x]$	λ_p
2	$x^7 + x + 1$	7
3	$(x+1)^3(x+2)^3x$	$\boxed{1^3 1^3 1}$
5	$x^7 + 3x + 2$	7
7	$(x+4)^7$	$\boxed{1^7}$
11	$x^7 + 4x + 8$	7
13	$\left(x^4 + 12x^3 + x^2 + 8x + 9\right)$ $\left(x^2 + 12x + 2\right)(x+2)$	421
17	$\left(x^3 + 14x^2 + 8x + 16\right)$ $\left(x^3 + 13x^2 + 12x + 15\right)$ $(x+7)$	331
$\vdots$		
79	$\left(x^2 + 28x + 70\right)$ $\left(x^2 + 21x + 52\right)$ $(x+6)(x+28)(x+75)$	22111
$\vdots$		
1879	$(x+1581)(x+1797)$ $(x+996)(x+1472)$ $(x+194)(x+508)(x+968)$	1111111

Let $\alpha_1, \ldots, \alpha_n$ be the complex roots of $f(x)$. Define the *polynomial discriminant*

$$\Delta = \prod (\alpha_i - \alpha_j)^2 \in \mathbb{Z}.$$

Define the *Galois group*

$$G = \mathrm{Aut}(\mathbb{Q}(\alpha_1, \ldots, \alpha_n)) \subseteq S_n.$$

For $x^7 - 7x - 3$,

$$\begin{aligned} \Delta &= 3^8 7^8, \\ G &= GL_3(2). \end{aligned}$$

(Δ, G) governs factorization patterns.

Let $K = \mathbb{Q}[x]/f(x)$. Then G depends only on K. Δ depends on f, but the *field discriminant* $D = \Delta/c^2$ depends only on K. For $x^7 - 7x - 3$,

$$D = 3^6 7^8.$$

2. The inverse Galois problem. Consider the problem of listing out all number fields with Galois group a given $G \subseteq S_n$.

• $G = S_1$. $\mathbb{Q}$ is the unique number field with Galois group S_1.

• $G = S_2$. Fields with $G = S_2$ are exactly $\mathbb{Q}(\sqrt{d})$ as d runs over square-free integers different from 1:

$\ldots -10, -7, -6, -5, -3, -2, -1, 2, 3, 5, 6, 7, 10, \ldots$

The discriminant of $\mathbb{Q}(\sqrt{d})$ is

$$D = \begin{cases} d & \text{if } d \equiv 1\ (4), \\ 4d & \text{if } d \equiv 2, 3\ (4). \end{cases}$$

• G abelian. The Kronecker-Weber theorem says that K embeds in some cyclotomic field $\mathbb{Q}(e^{2\pi i/m})$ and this yields a classification like that of the case S_2.

• A theorem of Hermite says that for any (D, G) there are only finitely many number fields with discriminant D and Galois group G.

• $G = S_3$. Calculation shows that the list of absolute discriminants $|D|$ is irregular:

23, 31, 44, 59, 76, 83, 87, ..., 972, 972, ...

The Davenport-Heilbronn theorem says that a positive integer is the absolute discriminant for on average $1/3\zeta(3) \approx 0.28$ fields.

A framework for pursuing classification questions is the **inverse Galois problem**:

Given an integer D and a transitive permutation group $G \subseteq S_n$, exhibit a defining polynomial for each number field with discriminant D and Galois group G.

The general expectation is that for each $G \neq S_1$ the list of occurring D is infinite.

3. Relevant databases.

Hermite's theorem can be made effective so that all fields with invariants (D, G) can be found by doing an exhaustive search over possible defining polynomials. The *Jones-Roberts database* specializes in lists that have been proved to be complete. Sample results, from very old to newer:

-

G			Smallest $\|D\|$		
$5T1$	$=$	C_5	11^4	$=$	$14,641$
$5T2$	$=$	D_5	47^2	$=$	$2,209$
$5T3$	$=$	F_5	$2^4 13^3$	$=$	$35,152$
$5T4$	$=$	A_5	$2^6 17^2$	$=$	$18,496$
$5T5$	$=$	S_5	1609	$=$	$1,609$

- There are exactly 11814 quintic fields with discriminant $\pm 2^a 3^b 5^c 7^d$.

- There are exactly 18 septic fields with discriminant $\pm 3^b 5^c$.

The *Klueners-Malle database* comes close to presenting at least one field for every group and signature up through degree 19. They aim to include the smallest $|D|$ in each case. Some particularly interesting (G, D) exhibited:

	G		D	
$11T6$	$=$	M_{11}	$2^{18}3^{8}5^{11}$	From M_{12} family
$11T6$	$=$	M_{11}	661^{8}	
$17T6$	$=$	$SL_2(16)$	$2^{30}137^{8}$	Bosman, from modular forms
$17T7$	$=$	$SL_2(16).2$		None so far!

4. Various major themes

• *Lower bounds on field discriminants* (. . . , Odlyzko, . . .)

• *Nilpotent groups* (. . . , Markshaitis, Koch, . . .) Completely explicit results for some arbitrarily large G

• *Solvable groups* (. . . , Shafarevich, . . .) Each solvable G has infinitely many occurring D.

• *Relation to modular forms* (. . . , Khare, Wintenberger, . . .) If G is embeddable in some $GL_2(\mathbb{F}_q)$ then all fields come from modular forms.

- *Relation to algebraic geometry* (. . . , Grothendieck, . . .) $H^w(X, \mathbb{F}_\ell)$ gives rise to Lie-type G with controlled D.

- *Relation to dessins d'enfants* (. . . , Matzat, . . .) Each sporadic G except for perhaps M_{23} has infinitely many occurring D.

- *Asymptotic mass formulas* (. . . , Bhargava, Malle, . . .) Local-global heuristics give expected numbers of fields with given (D, G), sometimes proved correct asymptotically, e.g. $G = S_5$.

5A. A nonsolvable field ramified at five only. In the 1990s, Gross observed no field was known with G nonsolvable and $|D|$ a power of a single prime $p \in \{2, 3, 5, 7\}$. Such fields were proved to exist around 2010 by Dembélé, Greenberg, Voight, and Dieulefait. A polynomial for one of these fields and its invariants:

$$x^{25} - 25x^{22} + 25x^{21} + 110x^{20} - 625x^{19} + 1250x^{18}$$
$$-3625x^{17} + 21750x^{16} - 57200x^{15} + 112500x^{14}$$
$$-240625x^{13} + 448125x^{12} - 1126250x^{11}$$
$$+1744825x^{10} - 1006875x^{9} - 705000x^{8}$$
$$+4269125x^{7} - 3551000x^{6} + 949625x^{5}$$
$$-792500x^{4} + 1303750x^{3} - 899750x^{2} + 291625x$$
$$-36535$$

$$\Delta = 5^{69}(\text{87-digit integer})^2 \qquad G = A_5^5.10$$
$$D = 5^{69}$$

It is obtained from the five torsion points of the elliptic curve with j-invariant

$$j = \frac{-1}{2^6 3^3 5^1 7^{11}} (16863524372777476\pi^4$$
$$+88540369937983588\pi^3 - 112479146605532\,15\pi^2$$
$$-46439936051548357\,2\pi - 35350586673838368\,0)$$

in the cyclic field $F = \mathbb{Q}[\pi]/(\pi^5 + 5\pi^4 - 25\pi^2 - 25\pi - 5)$.

5B. A field with G involving a sporadic group ramified at one prime only. There are now several ways to construct fields with G involving M_{11}, M_{12}, M_{22}, and M_{24}. For M_{11} and M_{24} it is hard to keep D small at all, but for M_{12} and M_{22} there are some fields with quite light ramification. Specializing a Belyi map again at carefully chosen large height point gives

$$\begin{aligned} f(x) = \\ & x^{48} + 2e^3x^{42} + 69e^5x^{36} + 868e^7x^{30} - 4174e^7x^{26} \\ & +11287e^9x^{24} - 4174e^{10}x^{20} + 5340e^{12}x^{18} \\ & +131481e^{12}x^{14} + 17599e^{14}x^{12} + 530098e^{14}x^8 \\ & +3910e^{16}x^6 + 4355569e^{14}x^4 + 20870e^{16}x^2 + 729e^{18}. \end{aligned}$$

Its invariants are

$$\begin{aligned} \Delta &= 11^{842}(\text{159-digit integer})^2 \\ D &= 11^{88} \\ G &= 2.M_{12}.2 \end{aligned}$$

An interesting problem is to find a corresponding unramified automorphic form for which this is a mod 11 representation.

5C. A polynomial with $\Delta = -2^{130729}5^{63437}$ and Galois group S_{15875}.

Let $T_w(x), U_w(x) \in \mathbb{Z}[x, \sqrt{x+2}, \sqrt{x-2}]$ be the classical Chebyshev "polynomials" indexed by $w \in \{1/2, 1, 3/2, 2, \ldots\}$. Form

$$\begin{aligned} T_{m,n}(s,x) &= T_{m/2}(x)^n - tT_{n/2}(x)^m \\ U_{m,n}(s,x) &= U_{m/2}(x)^n - sU_{n/2}(x)^m \end{aligned}$$

Then, like $T_w(x)$, the $T_{m,n}(s,x)$ and $U_{m,n}(s,x)$ have highly factoring discriminants. Unlike the $T_w(x)$, Galois groups now tend to be the full symmetric group on the degree.

Example: The mass heuristic suggests there should be no fields with $D = \pm 2^a 5^c$ past degree $n = 40$. However

$$U_{125,128}(5,x) = \\ (x-2)^3 u_{62.5}(x)^{256} - 5(x+2)^{125} u_{64}(x)^{250}$$

has $\Delta = -2^{130729}5^{63437}$ and $G = S_{15875}$.