Determining the Galois group of a rational polynomial

Alexander Hulpke

Department of Mathematics

Colorado State University

Fort Collins, CO, 80523

hulpke@math.colostate.edu

http://www.math.colostate.edu/~hulpke

The Task

Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree n.

Then $G = \mathrm{Gal}(f) = \mathrm{Gal}(L, \mathbb{Q})$ with L the splitting field of f over $\mathbb{Q}$.

Problem: Given f, determine G.

WLOG: f monic, integer coefficients.

Field Automorphisms

If we want to represent automorphims explicitly, we have to represent the splitting field L

For example as splitting field of a polynomial $g \in \mathbb{Q}[x]$.

The factors of g over L correspond to the elements of G.

Note: If $\deg(f) = n$ then $\deg(g) \leq n!$.

In practice this degree is too big.

Permutation type of the Galois Group

$\mathrm{Gal}(f)$ permutes the roots $\alpha_1, \ldots, \alpha_n$ of f:

- faithfully ($L = \mathrm{Spl}(f) = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$).
- transitively ($\prod_{i \in I} (x - \alpha_i)$ is a factor of f).

This action gives an embedding $G \leq S_n$. The field $\mathbb{Q}(\alpha_1)$ corresponds to the subgroup $\mathrm{Stab}_G(1)$.

Arrangement of roots corresponds to conjugacy in S_n.

We want to determine the S_n-class of G.

Assumption

We can calculate "everything" about S_n.

- n is small ($n \leq 20$)
- Can use table of transitive groups (classified up to degree 30)

We can approximate the roots of f (numerically and p-adically)

Reduction at a prime

Let p be a prime that does not divide the discriminant of f (i.e. f is squarefree modulo p).

Consider f as a polynomial f_p over $\mathbb{F}_p$. Then $\mathrm{Gal}(f_p)$ embeds into G ("Frobenius elements").

> The degrees of the factors of f modulo p correspond to the cycle shapes of an element in the Galois group.

Chebotarev's theorem:

> If $p \to \infty$, the distribution of factor degrees approaches the distribution of cycle shapes in the group.

This is also very useful to describe polynomial factorization modulo p.

Elements of the Galois group

For the purpose if identifying a Galois group, this means that we can get (an approximation of) the cycle stuctures occurring in the group.

We can check, which of the transitive groups contain an element of such a shape.

This gives a probabilistic test for the type of the Galois group.

(However, in degree 8 there are two groups with identical shape frequencies.)

It also gives quickly a "lower bound" for G (often this turns out to be exactly G but we cannot prove it.)

Invariants

S_n acts on the polynomial ring $\mathbb{Q}[x_1, \ldots, x_n]$ by permuting the indeterminates.

A polynomial $h = h(x_1, \ldots, x_n)$ is an *invariant* for a subgroup $U \leq S_n$ if h is fixed by U.

For every subgroups $U \leq S_n$ one can find a polynomial h_U such that $U = \mathrm{Stab}_{S_n}(h_U)$. For example take

$$h_U := \sum_{u \in U} (x_1 \cdot x_2^2 \cdot x_n^n)^u$$

Evaluated Invariants

Let $L = \mathrm{Spl}(f) = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Consider the evaluation homomorphism

$$\varphi\colon \mathbb{Q}[x_1, \ldots, x_n] \to L, \qquad g(x_1, \ldots, x_n) \mapsto g(\alpha_1, \ldots, \alpha_n).$$

Then $G = \mathrm{Gal}(f)$ acts as Galois group on $\varphi(\mathbb{Q}(\alpha_1, \ldots, \alpha_n))$ *in the same way* as it acts as permutation group on $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$.

In particular: If h is invariant under G, then $\varphi(h) \in \mathbb{Q}$.

If f is monic with integer coefficients, the α_i are algebraic integers and $\varphi(h) \in \mathbb{Z}$ (which is easier to test).

Proving Invariance

We want to use invariants h to prove that $G \leq \mathrm{Stab}_{S_n}(h)$. We thus need to show that G-invariance of $\varphi(h)$.

Alas Let $f = x^4 + 3x^2 + 5 = g(x^2)$ with $g = x^2 + 3 + 5$. Then

$$\alpha_i = \pm\sqrt{\pm 2 \cdot \sqrt{-2}}$$

So in particular $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4 = 0 \in \mathbb{Z}$.

But $\mathrm{Gal}(f) = D_8$ does not leave $x_1 + x_2$ invariant.

Proving Invariance, cont.

Lemma Assume that

$$\varphi(h) \neq \varphi(h') \quad \text{for all} \quad h' \in h^G$$

Then h is G-invariant if and only if $\varphi(h) \in \mathbb{Z}$.

Proof If there is $g \in G$ such that $h' = h^g \neq h$ then $\varphi(h) \neq \varphi(h')$ cannot be rational.

Theorem (Girstmair) For each polynomial h, there is a Tschirnhaus-transform of f – a polynomial whose roots are a polynomial in α,

$$\mathrm{Res}_y(p(y) - x, f(x))$$

such that φ becomes injective on h^G.

The Method

We determine for sufficiently many polynomials $h \in \mathbb{Q}[x_1, \ldots, x_n]$ whether (or not) they are invariant under G, until this uniquely determines G.

There are two main variants which differ in the way how these polynomials are obtained:

Soicher/McKay method

Form *resolvent polynomials* for $m \leq n$, whose roots correspond to sets/tuples of roots. For example:

$$\prod_{\{i_1,i_2,\ldots,i_m\} \subset \{1,\ldots,n\}} (x - (\alpha_{i_1} + \alpha_{i_2} + \cdots + \alpha_{i_m}))$$

(One can construct such resolvents using polynomial techniques, such as resultants.)

The coefficients of the irreducible factors of the resolvents are Galois invariants. The factors correspond to transitive actions of G on sets or tuples.

For each n determine a priori how many such actions are needed to distinguish the group.

Example

Let $f = 1 + x - 3x^2 - x^3 + x^4$. A polynomial with roots of the form $\alpha_i + \alpha_j$ is

$$1-4x-2x^2+11x^3-3x^4-3x^5+x^6 = (-1-x+x^2)(-1+5x-4x^2-2x^3+x^4)$$

We thus know that the Galois group has one orbit of length 2 and one orbit of length 4 on pairs of points.

It thus is a dihedral group of size 8.

Stauduhar method

Suppose we know for a given $U \leq S_n$ that $G \leq U$.

For each maximal subgroup $M \leq U$ test (by a suitable invariant) whether $G \leq M$.

If yes, continue with M in place of U.

If G is not contained in any maximal subgroup, we know that $G = U$.

Required Information

For each transitive $U \leq S_n$ compute:

- all maximal subgroups $M < U$.
- For each maximal $M < U$ a distinguishing invariant $h(x_1, \ldots, x_n)$.

(This is required only up to conjugacy)

Evaluation of invariants

We need to approximate $\varphi(h)$ well enough so that it can be proven whether it is an integer.

Due to error propagation numerical approximation is infeasible, if one wants mathematically proven results.

Instead, use p-adic approximation. A rough estimation of the magnitude of the values of $\varphi(h)$ (analytic or numerical) determines the required accuracy.

Since we have to test for every maximal $M \leq U$, we can also test for integral roots of

$$\prod_{h_i} (x - \varphi(h_i))$$

with h_i running over invariants for maximal subgroups in one U-class.

Comparison

Stauduhar

+ Identifies actual Galois action
+ Very fast approximate calculations
+ Each new step uses already previous information
- Large number of maximal pairs
- Potentially large number of steps (1654 gps. of deg. 16)
- Invariants can be messy
- Evaluation of invariants requires high precision

Soicher/McKay

+ Factor coefficients "hide" messy invariants
+ Approximation is hidden in factorization
+ Single resolvent answers more than a single inclusion
+ Resolvents factors define subfields
- Complete distinction can require complicated actions
- Resolvents are worst kind of polynomials for Hensel factorization

Combined approach

Resolvent factors in the Soicher/McKay approach tell more than their degrees:

The roots of one irreducible factor correspond to an orbit of G.(Roots can be approximate, even mod p.)

We thus know that G is a subgroup of the stabilizer of this orbit in S_n.

Such subgroups are called *closures* of G (WIELANDT, 1968):

- $G^{(k)}$: k-closure — same orbits on k-tuples
- $G^{\{k\}}$: k-set-closure — same orbits on k-sets.

Different resolvents give different closures – G is contained in each (and thus the intersection).

Properties:

$$
\begin{aligned}
G^{(k)} &\leq G^{(k+1)} \\
G^{(k)} &\leq G^{\{k\}} \\
G^{\{k+1\}} &\leq G^{\{k\}} \qquad \text{(if } k < \tfrac{n}{2}\text{)} \\
G^{\{2\}} & \quad \text{determines block systems of } G
\end{aligned}
$$

At any point we can switch to the Stauduhar method.

Advantages

Identify first closures of G (might give sufficient group theoretic information). (Question: What properties of G are implied by $G^{\{k\}}$?)

Known closure information can be used to speed up further polynomial factorization.

The Frobenius element for the prime p we use for approximating roots is also known exactly.

Hard Case

In all variants the difficult cases are different groups with very “similar" action.

Often these are maximal subgroups of each other.

In this case one needs complicated invariants (requiring high accuracy) or high degree resolvent polynomials.

The prototypical case for this is the quintuply transitive $M_{12} \leq A_{12}$.