Computing Galois groups I

David P. Roberts
University of Minnesota, Morris

General background, with some subtleties emphasized

1. Definition of Galois groups
2. The Trinks polynomial and $C = \mathbb{C}$
3. The Trinks polynomial and $C = \mathbb{Q}_{1849}$
4. Comparing two choices of auxiliary fields
5. Decomposition groups
6. T-numbers

Basic computational methods

7. Use Magma!
8. Frobenius partitions
9. Ramification partitions
10. Resolvents

1. Definition of Galois groups. Let Q be a field and let F be a degree n separable algebra over Q.

For concreteness, we work with a presentation $F = Q[x]/f(x)$ for $f(x) \in Q[x]$ a monic separable polynomial (such a presentation may not exist for Q finite and F a non-field; if one is interested in this case, one can translate back to the more abstract language).

Let C be a field extension of Q in which $f(x)$ has n distinct roots. Let $X \subset C$ be this set of roots. F^{gal} be the subalgebra of C generated by X. Then $G =$ *Gal*(F^{gal}/Q) *is the group of automorphisms of* F^{gal} *which fix* Q*.*

One normally views G as inside the symmetric group $\text{Sym}(X)$ of permutations of X.

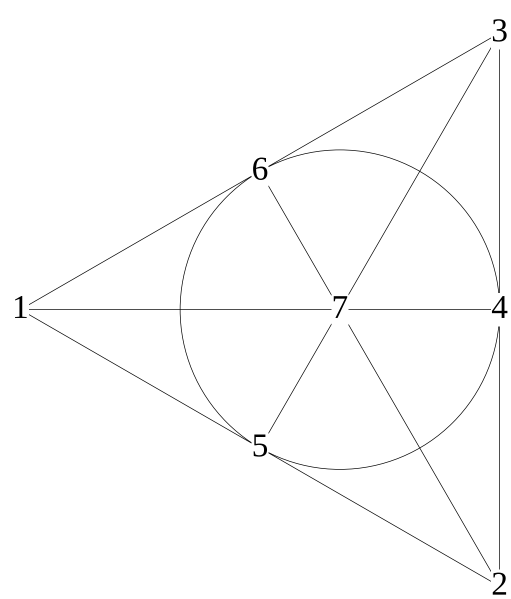
2. The Trinks polynomial and $C = \mathbb{C}$. For $x^7 - 7x - 3$ and $C = \mathbb{C}$, the roots are:

$$\begin{array}{ccccc} & \alpha_3 \approx -0.62 + 1.21i & & \alpha_6 \approx 0.76 + 1.21i & \\ \alpha_1 \approx -1.29 & & \alpha_4 \approx -0.43 & & \alpha_7 \approx 1.44 \\ & \alpha_2 \approx -0.62 - 1.21i & & \alpha_5 \approx 0.76 - 1.21i & \end{array}$$

Form the resolvent

$$g(x) = \prod_{i<j<k} (x - (\alpha_i + \alpha_j + \alpha_k)) = g_7(x) g_{28}(x).$$

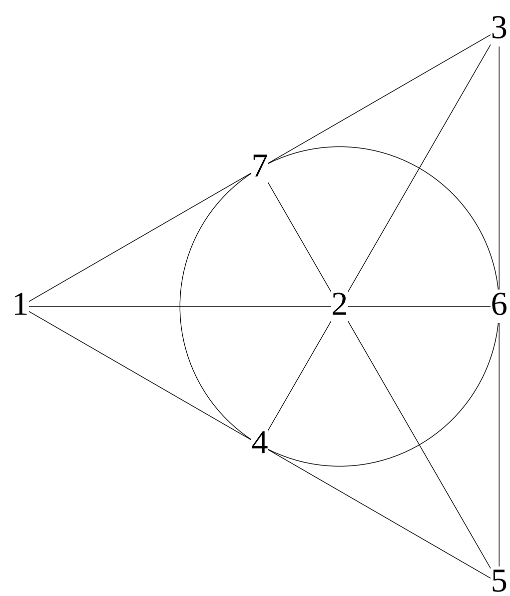
Working in sixteen digit precision, all coefficients of $g(x) \in \mathbb{Z}[x]$ are approximated within 0.00003. Identifying roots of $g_7(x)$ as lines in $\mathbb{P}^2(\mathbb{F}_2)$, the Galois group becomes the symmetry group of a projective plane:



3. The Trinks polynomial and $C = \mathbb{Q}_{1879}$. For $x^7 - 7x - 3$ and $C = \mathbb{Q}_{1879}$, the roots are $(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7) \approx$

$$(-508,\ -194,\ 82,\ 298,\ 407,\ 883,\ 911).$$

Working mod 1879^3 suffices to correctly identify $g_{35}(x)$. The seven roots of $g_7(x)$ are $\beta_1 + \beta_2 + \beta_6$, ... Again the Galois group becomes the symmetry group of a projective plane:



The pairings (α_1, β_1), (α_2, β_5), (α_3, β_3), (α_4, β_6), (α_5, β_4), (α_6, β_7), (α_7, β_2) give one of the 168 structure-preserving correspondences with the previous slide.

4. Comparing two choices of auxiliary fields.

If one works with two auxiliary fields C_v and C_w, one has two Galois groups

$$\begin{aligned} G_v = \mathsf{Gal}(F^{\mathsf{gal},v}/Q) &\subseteq \mathsf{Sym}(X_v), \\ G_w = \mathsf{Gal}(F^{\mathsf{gal},w}/Q) &\subseteq \mathsf{Sym}(X_w). \end{aligned}$$

Galois theory says that $F^{\mathsf{gal},v}$ and $F^{\mathsf{gal},w}$ are isomorphic and hence G_v and G_w are isomorphic. Different isomorphisms

$$i_1, i_2 : F^{\mathsf{gal},v} \to F^{\mathsf{gal},w}$$

induce different bijections $X_v \stackrel{\sim}{\to} X_w$. They induce typically different isomorphisms $G_v \stackrel{\sim}{\to} G_w$.

However these isomorphisms $G_v \stackrel{\sim}{\to} G_w$ are always conjugate. Thus one has unambiguous agreement on things like *conjugacy classes*, *complex characters*, *abelianizations*, and *cohomology groups*. Notationally, one has unambiguous objects $G^\natural$, $\widehat{G}$, G^{ab}, and $H^*(G,\mathbb{Z})$. One can expect to compute them *purely algebraically, never leaving Q, with no reference to explicit roots anywhere.*

5. Decomposition groups for $Q = \mathbb{Q}$. Working with $\mathbb{C}$ as the auxiliary field gives an important piece of structure for free: a homomorphism from $\text{Gal}(\mathbb{C}/\mathbb{Q}) = \{\text{Id}, \sigma_\infty\}$ to G_∞ or equivalently a complex conjugation element $\sigma_\infty \in G_\infty$.

Taking $\overline{\mathbb{Q}}_p$ gives much more, as it gives a homomorphism $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to G_p$. The image is the decomposition group $D_p \subseteq G_p$. It comes with a decreasing filtration measuring ramification and its wildness. In particular if p is unramified, one gets a canonical element $\sigma_p \in G_p$, the Frobenius element. If it is tamely ramified, one gets a canonical element $\tau_p \in G_p$.

At the level of conjugacy classes, these elements σ_v and τ_p all sit in the same set $G^\natural$. At the level of the ambient symmetric groups they all become *partitions*. Thus Galois theory *coordinates* the local invariants of number fields.

6. T**-numbers.** Let $\mathcal{T}_n$ be the set of conjugacy classes of transitive subgroups of S_n. As examples,

$$\mathcal{T}_4 = \{4T1, 4T2, 4T3, 4T4, 4T5\} = \{C_4, V, D_4, A_4, S_4\}$$

$$\mathcal{T}_5 = \{5T1, 5T2, 5T3, 5T4, 5T5\} = \{C_5, D_5, F_5, A_5, S_5\}$$

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\lvert\mathcal{T}_n\rvert$	1	1	2	5	5	16	7	50	34	45	8	301	9

The *fine* problem of computing Galois groups of number fields has an irreducible $f(x) \in \mathbb{Q}[x]$ and a place v of $\mathbb{Q}$ as input. As output it has the root-set X_v and the Galois group $G_v \subseteq \text{Sym}(X_v)$.

The *coarse* problem of computing Galois groups has just $f(x) \in \mathbb{Q}[x]$ as input. As output it has the corresponding nTj.

The fine and the coarse level each have their own advantages. The next slides cover elementary coarse-level techniques. Friday will include fine-level computations.

7. Use Magma!

```
>PR<x> := PolynomialRing(Integers());
>GaloisGroup(x^7-7*x-3);
Permutation group acting on a set of cardinality 7
Order = 168 = 2^3 * 3 * 7
    (2, 4)(3, 7)
    (1, 6, 4, 3)(5, 7)
[ 31615*$.1^6 - 21962*$.1^5 + 31333*$.1^4
     - 24197*$.1^3 +   7399*$.1^2
     + 42492*$.1 - 75664 + O(11^5),  ... ]
GaloisData over Z_11
>G, r, S := GaloisGroup(x^7-7*x-3: Prime:=13);
>G;
Order = 168 = 2^3 * 3 * 7
    (2, 5)(6, 7)
    (1, 7)(2, 6, 3, 4)
>r;
[ -61424*$.1^3 + 47369*$.1^2 - 26589*$.1
  + 178417 + O(13^5), ...]
> TransitiveGroupDescription(G);
L(7) = L(3,2)
```

8. Frobenius partitions. To get lower bounds on Galois groups one can use Frobenius partitions. For example,

$$\begin{aligned} x^{12} - 6x^{11} - 6x^{10} + 40x^9 + 105x^8 + 120x^7 \\ -1790x^6 + 2070x^5 + 885x^4 + 480x^3 \\ -2520x^2 - 1440x - 240 \end{aligned}$$

has field discriminant the perfect square $D = 2^{18}\,3^{18}\,5^{12}$ and thus $G \subseteq A_{12}$. Factorization patterns begin

$$(\lambda_7, \lambda_{11}, \lambda_{13}, \lambda_{17}) = (6\,6,\ 11\,1,\ 8\,2\,1\,1,\ 8\,4).$$

This is more than enough to reduce the 301 possibilities to $G \in \{M_{12}, A_{12}\}$.

There is a canonical Bayesian formula for guessing G based on say an *a priori* assumption of 1-to-1 odds for M_{12}. Each appearance of a partition λ either definitively proves $G = A_{12}$ or increases the odds for M_{12} by the ratio $r(\lambda) = \text{prob}(M_{12}, \lambda)/\text{prob}(A_{12}, \lambda)$, as in e.g. $r(8\,2\,1\,1) = (1/8)/(1/16) = 2$. After 100 good primes, the odds are about 6.05×10^{34}-to-1 for M_{12}.

9. Lower bounds from bad primes. There are many ways to use the bad primes to get lower bounds on Galois groups. For example F from the last slide has discriminant $2^{18}\,3^{18}\,5^{12}$. Since all exponents are ≥ 12, all bases are wildly ramified. Thus $|G|$ is divisible by 2, 3, and 5.

In a more elementary way, another polynomial defining F, with coefficients factored, is

	x^{12}	x^{11}	x^{10}	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x	1
2 :	1		4	8	8	8	4	8	8	8	16		8
3 :	1		9	1	3	3	1	3	3	9	9		3
5 :	1		1	5	5	5	5	25	25	125	25		25
rest :	1	0	−1	−1	1	7	149	11	17	1	1	0	−1

The nonzero slopes of the Newton polygon at $p = 2$, 3, and 5 are $1/4$, $1/6$, and $1/5$. Thus there are p-adic roots of the form (unit)$2^{1/4}$, (unit)$3^{1/6}$, and (unit)$5^{1/5}$. Thus $|G|$ is divisible by 4, 6, and 5, and hence 60 (still leaving the possibilities at M_{12} and A_{12}).

10. Resolvents. To compute Galois groups exactly, one can use constructions canonically building new sets from n-element sets X and their corresponding resolvents. For example, the passage from X to $X \times X - \Delta$ corresponds to passing from a polynomial with roots α_i to one with roots $\alpha_i - \alpha_j$, with $i \neq j$. Algebraically, this is achieved by

$$f(x) \mapsto \mathrm{Res}_y(f(y), f(y+x))/y^n.$$

The general resolvent from $X \mapsto \mathrm{Subsets}_3(X)$ nearly distinguishes all possibilities for $n = 7$:

C_7	D_7	F_7^+	F_7	$L_3(2)$	A_7	S_7
$7T1$	$7T2$	$7T3$	$7T4$	$7T5$	$7T6$	$7T7$
7^5	$14\ 7^3$	$21\ 7^3$	$21\ 14$	$28\ 7$	35	35

To distinguish M_{12} from A_{12}, the lowest degree absolute resolvent is $\mathrm{Partitions}_{6,6}(X)$ with degree $\frac{1}{2}\binom{12}{6} = 462 = 2 \cdot 3 \cdot 7 \cdot 11$. For A_{12} fields it is irreducible, while for M_{12} fields it factors as $396 + 66 = 2^2 \cdot 3^2 \cdot 11 + 2 \cdot 3 \cdot 11$. In our case, the coefficients average 313 digits and *Magma* factors the polynomial in about a second.