Using Galois Groups of Reducible Polynomials and Hilbert's Irreducibility Theorem

Nicole Sutherland (nicole.sutherland@sydney.edu.au)
Computational Algebra Group, School of Mathematics and Statistics, The University of Sydney, Australia

Definitions

The *Galois group*, $\mathrm{Gal}(f)$, of a polynomial f over a field F is the automorphism group of the splitting field of f over F, a group of permutations of the roots of f.
The *geometric Galois group* of a polynomial $f \in \mathbb{Q}(t)[x]$, $\mathrm{GeoGal}(f)$, is the Galois group of f considered as a polynomial over $\mathbb{C}(t)$, $\mathrm{Gal}(f/\mathbb{C}(t))$.
Given a function field $F/k(t), K = \{z : z \in F \mid z \text{ is algebraic over } k\}$, the algebraic closure of k in F, is the *full* or *exact constant field* of F.

Compute the Galois group of a polynomial

Let f be a monic, integral, separable polynomial over $F = \mathbb{Q}, \mathbb{F}_q(t)$, $\mathbb{Q}(t)$ or an extension thereof:

1. Compute a splitting field S_f for f over a completion of F and the roots of f in S_f.
2. Find a group $G \subseteq S_n$ which contains $\mathrm{Gal}(f)$
3. While G has maximal subgroups which could contain $\mathrm{Gal}(f)$
   1. For each maximal subgroup H of G, compute a G-relative H-invariant polynomial I_H.
   2. For a cheap maximal subgroup H of G (Stauduhar)
      1. Compute the precision m needed in the roots of f and the roots of f in S_f to precision m.
      2. for the representatives $\tau \in G//H$ of cosets of H in G, evaluate I_H^τ at the roots of f. Decide whether this is the image of an element of F in S_f. If so $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$ and restart the loop (3) with $G = \tau H \tau^{-1}$.
4. $\mathrm{Gal}(f)$ is G

Galois groups of reducible polynomials

This algorithm can also be used for reducible polynomials — just change the starting group!

- Instead of being contained in S_n, the Galois group of a reducible polynomial is contained in the direct product of the Galois groups of its irreducible factors.
- The more the splitting fields of the factors overlap the smaller the splitting field of the reducible polynomial and the Galois group.
- If we can determine that the splitting fields of some factors do not overlap with all the others we do not need to include the associated Galois groups in the starting group for the descent, but compute the product of them with the result of the smaller descent afterwards.
- We can apply some knowledge of ramified and unramified extensions to consider how the splitting fields of the irreducible factors interact.

Algorithm (Compute a Fixed Field of a subgroup ([3]))

Given $U \subseteq G = \mathrm{Gal}(f)$ compute the subfield of the splitting field of f fixed by U.

1. *Compute a G-relative U-invariant polynomial I and the right transversal $G//U$.*
2. *Compute roots $\{r_i\}_{i=1}^n$ to a useful precision.*
3. *Compute the polynomial g with roots $\{I^\tau(r_1, \ldots, r_n) : \tau \in G//U\}$.*
4. *Map the coefficients of g back to the coefficient ring of f. The resulting polynomial defines the fixed field of U.*

References

[1] J. J. Cannon, W. Bosma, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions (V2.24)*, Computational Algebra Group, University of Sydney, 2018, http://magma.maths.usyd.edu.au.

[2] C. Fieker and J. Klüners, *Computation of Galois groups of rational polynomials*, London Mathematical Society Journal of Computation and Mathematics **17** (2014), no. 1, 141 – 158.

[3] A.-S. Elsenhans, C. Fieker and J. Klüners, *Galois group implementations*, Magma.

[4] David Krumm and Nicole Sutherland, *Explicit Hilbert irreducibility*, submitted to JSC, 2017.

[5] Serge Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York 1983.

[6] G. Malle and B.-H. Matzat, *Inverse Galois Theory*, Springer, 1999

[7] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, 1992.

[8] N. Sutherland, *Computing Galois groups of polynomials (especially over function fields of prime characteristic)*, Journal of Symbolic Computation **71** (2015), 73–97.

[9] ———, *Algorithms for Galois extensions of global function fields*, PhD Thesis, University of Sydney, 2015.

Overview

We consider 2 computations using Galois groups and Hilbert's Irreducibility Theorem.

- In order to make Hilbert's Irreducibility Theorem explicit [4], for $P \in Q[t, x]$, let $G = \mathrm{Gal}(P)$ be the Galois group of P over $Q(t)$: for which $c \in \mathbb{Q}$, with $P_c = P(c, x)$, does $\mathrm{Gal}(P_c) \cong G$ and P_c factors the same way as P *not* occur?
- We describe an algorithm to compute geometric Galois groups of polynomials $f \in \mathbb{Q}(t)[x]$. This algorithm is available in Magma [1].

Making Hilbert's Irreducibility Theorem Explicit ([4] Theorem 2.7)

Let $P(t, x) \in \mathbb{Q}[t, x]$, $\mathcal{F}(P)$ be the multiset consisting of the degrees of the irreducible factors of P and $G = \mathrm{Gal}(P)$ be the Galois group of P over $\mathbb{Q}(t)$. Let M_i be representatives of all classes of maximal subgroups of G with fixed fields $F_i/\mathbb{Q}(t)$ generated by a root of $f_i(t, x)$. Suppose that $c \in \mathbb{Q}$ satisfies $\Delta(c)l(c)\prod_{i=1}^r \mathrm{disc}(f_i(c, x)) \neq 0$. Then,

1. If $\mathcal{F}(P_c) \neq \mathcal{F}(P)$, then $\mathrm{Gal}(P_c) \ncong G$.
2. $\mathrm{Gal}(P_c) \ncong G \iff$ there is an index i such that $f_i(c, x)$ has a root in $\mathbb{Q}$.

We need to compute Galois groups over $\mathbb{Q}(t)$, including when P is reducible, and fixed fields of subgroups of $\mathrm{Gal}(P)$. We obtain the f_i and then find suitable c using rational points on the curves defined by f_i.

Example over $\mathbb{Q}(t)$ ([4] Section 4.1)

```
> Qt<t> := FunctionField(Rationals()); P<x> := PolynomialRing(Qt);
> f := x^6 + t^6 - 1; G, r, S := GaloisGroup(f);
> for M in MaximalSubgroups(G) do
for> GaloisSubgroup(S, M`subgroup); end for;
x^2 - 62208*t^30 + 311040*t^24 - 622080*t^18 + 622080*t^12
    - 311040*t^6 + 62208,          x^2 + 6*x + 9*t^6,
x^2 + 1728*t^12 - 3456*t^6 + 1728, x^3 + 12*x^2 + 48*x - 8*t^6 + 72
> HilbertIrreducibilityCurves(f);
{ -1, 1 }
```

It can be shown theoretically [4] that none of the curves defined by these polynomials have a rational root when $c \neq 0, 1, -1$. Therefore, $\mathrm{Gal}(f_c) \cong G$ unless $c = 0, 1, -1$ and f_c must be irreducible when $c \neq 0, 1, -1$ and otherwise reducible.

Example of reducible polynomial over $\mathbb{Q}(t)$ (D. Krumm)

```
> k<t> := FunctionField(Rationals()); _<x> := PolynomialRing(k);
> Phi4 := x^12 + 6*t*x^10 + x^9 + (15*t^2 + 3*t)*x^8 + 4*t*x^7 +
> (20*t^3 + 12*t^2 + 1)*x^6 + (6*t^2 + 2*t)*x^5 + (15*t^4 +
> 18*t^3 + 3*t^2 + 4*t)*x^4 + (4*t^3 + 4*t^2 + 1)*x^3 + (6*t^5 +
> 12*t^4 + 6*t^3 + 5*t^2 + t)*x^2 + (t^4 + 2*t^3 + t^2 + 2*t)*x
> + t^6 + 3*t^5 + 3*t^4 + 3*t^3 + 2*t^2 + 1;
> ep4 := Polynomial([Evaluate(y, (4 - 3*t - t^3)/(4*t)) : y in
>                                          Coefficients(Phi4)]);
> Ep4 := Polynomial([Evaluate(y, (t^2-1)/t) :
>                                      y in Coefficients(ep4)]);
> #GaloisGroup(Phi4); #GaloisGroup(ep4); #GaloisGroup(Ep4);
384 128 64
```

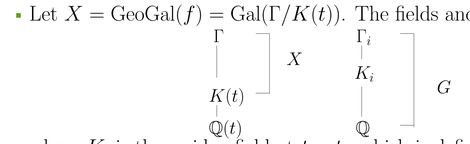
Using the procedure in the first example we determine that Φ_4 has a different factorization type and Galois group when evaluated at something of the form $(4 - 3v - v^3)/4v$. To determine what Galois group Φ_4 specialised at c has in these cases we need to compute the Galois group of the reducible polynomial `ep4`, a product of a degree 8 and a degree 4 polynomial. Further we can apply the procedure above to `ep4` which tells us that when v has the form $(s^2 - 1)/s$ the Galois group and factorization type is different again.

Compute the Geometric Galois Group of $f \in \mathbb{Q}(t)[x]$

1. Specialise t at small integers. Choose $t = t_1, t_2$ such that $\mathrm{Gal}(f(t_i, x)) = \mathrm{Gal}(f) = G$.
2. Compute $H = \mathrm{Gal}(f(t_1, x)f(t_2, x))$.
3. For normal subgroups X of G having index less than that of H in $G \times G$ and order dividing $\#G/c$ where c is the degree of the full constant field of $\mathbb{Q}(t)[x]/f$,
   (a) Compute the defining polynomial of the field K' fixed by X.
   (b) Check whether this is a polynomial over $\mathbb{Q}$ or whether this defines a constant field extension. If so X contains $\mathrm{GeoGal}(f)$ and $K \supseteq K'$.
4. The subgroup X containing $\mathrm{GeoGal}(f)$ with the largest index in G and smallest order corresponds to the largest constant field extension in Γ, and is $\mathrm{GeoGal}(f)$.

The Theory behind the Algorithm

- Since $\mathbb{Q}$ is a subfield of $\mathbb{C}$, the geometric Galois group of f will be a subgroup of $\mathrm{Gal}(f)$.
- Using inexact fields such as $\mathbb{C}$ runs into problems with precision, so we instead compute over the largest algebraic extension of $\mathbb{Q}$ which contains the algebraic numbers we require : the algebraic closure, $K = \Gamma \cap \mathbb{C}$, where Γ is the splitting field of f.
- Since $\mathrm{Gal}(f/K(t)) = \mathrm{Gal}(f/\mathbb{C}(t))$, $\mathrm{GeoGal}(f) = \mathrm{Gal}(f/K(t))$.
- The task is to determine K and which normal subgroup of $\mathrm{Gal}(f)$ fixes $K(t)$. We can narrow down the possible subgroups to consider by deriving constraints on the index of $\mathrm{GeoGal}(f)$ in $\mathrm{Gal}(f)$. We use a known divisor of the index and an upper bound on $[K : \mathbb{Q}]$ (which is equal to this index).
- Using Hilbert's Irreducibility Theorem [7, 5] we have, for infinitely many $t_i \in \mathbb{Q}$,
$$G = \mathrm{Gal}(f) = \mathrm{Gal}(\Gamma) = \mathrm{Gal}(f(t_i, x)) = \mathrm{Gal}(\Gamma_i).$$
- Let $X = \mathrm{GeoGal}(f) = \mathrm{Gal}(\Gamma/K(t))$. The fields and groups we are considering are :



  where K_i is the residue field at $t - t_i$, which is defined by $f(t_i, x)$, and we know $K \subseteq K_i$. So we are looking for a normal subgroup $X \subseteq G$ such that $K(t)$ is the fixed field of X.
- Let $H = \mathrm{Gal}(f(t_1, x)f(t_2, x))$. As computed by [8, 9] $H \subseteq G \times G$. Since $[G \times G : H] = [\Gamma_1 \cap \Gamma_2 : \mathbb{Q}]$ and $K \subseteq \Gamma_1 \cap \Gamma_2$, $[G \times G : H] \geq [K : \mathbb{Q}]$.
- Since K will contain all the constants of $\mathbb{Q}(t)[x]/f \subseteq \Gamma$ the degree of this extension of $\mathbb{Q}$ must divide $[K : \mathbb{Q}]$. This narrows down the number of subgroups which are candidates for $\mathrm{GeoGal}(f)$ to those whose index is at most our bound and divisible by a field degree.
- The fixed field $K(t)$ of the subgroup $X \subseteq G$ is contained in $\mathbb{C}(t)$ so we can discount any subgroups whose fixed fields are not isomorphic to rational function fields over algebraic extensions of $\mathbb{Q}$.

Computations of geometric Galois groups have links to Inverse Galois Theory. See [6].

A Non-Trivial Example

Let
$$f = x^9 - 3x^7 + (-6t - 6)x^6 + 3x^5 + (12t - 6)x^4 + (12t^2 - 84t + 11)x^3 + (-6t - 6)x^2 + (-12t^2 + 12t + 24)x - 8t^3 - 24t^2 - 24t - 6$$
be a polynomial over $\mathbb{Q}(t)$. This polynomial is a defining polynomial of $(\mathbb{Q}(t)[x]/\langle x^3 - 2\rangle)[y]/\langle y^3 - 2t - y\rangle$ over $\mathbb{Q}(t)$. The Galois group of f is $9T8$ of order 36. Specialising f at $t = 1, 2$ gives
$$f_1 = x^9 - 3x^7 - 12x^6 + 3x^5 + 6x^4 - 61x^3 - 12x^2 + 24x - 62,$$
$$f_2 = x^9 - 3x^7 - 18x^6 + 3x^5 + 18x^4 - 109x^3 - 18x^2 - 214$$
whose Galois groups are conjugate to $9T8$. The Galois group of $f_1 f_2$ is an intransitive group of order 216. Therefore the index bound for $\mathrm{GeoGal}(f)$ is $36 \times 36/216 = 6$. The exact constant field of the splitting field of f must contain the exact constant field of $\mathbb{Q}(t)[x]/f$ of degree 3 so the order of $\mathrm{GeoGal}(f)$ must divide $36/3 = 12$. There are 2 normal subgroups of $\mathrm{Gal}(f)$ which satisfy this index and order restriction, both isomorphic to S_3 of order 6. Only one of the fixed fields has a defining polynomial over $\mathbb{Q}$: $x^6 + 78732$. The other fixed field, defined by $x^6 - 54x^4 + 729x^2 + 78732t^2 - 2916$, is not isomorphic to its exact constant field, $\mathbb{Q}$. Therefore the first fixed field is the exact constant field of the splitting field of f and the corresponding group, isomorphic to S_3, is the geometric Galois group of f.