Computations of Galois Groups and Splitting Fields

Nicole Sutherland

Computational Algebra Group
School of Mathematics and Statistics
The University of Sydney

May 3, 2019

Algebraic Fields

Definition

An *algebraic number field* is a finite algebraic extension of the rational field.

Definition

An *algebraic function field* is an extension field F containing a field k such that F is a finite algebraic extension of a rational function field $k(t)$ for some element $t \in F$ which is transcendental over k .

Relative Extensions

$$\begin{array}{cl}
 & \text{Relative Extension of } k(t) \text{ or } \mathbb{Q}, \\
E & \text{Algebraic Extension of } F \\
| & \\
F & \text{Algebraic Extension of } k(t) \text{ or } \mathbb{Q} \\
| & \\
k(t) \text{ or } \mathbb{Q} &
\end{array}$$

Galois Groups

Definition

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.

- $\mathrm{Gal}(f)$ is a group of permutations of the roots of f.
- All permutations of n roots are in S_n so $\mathrm{Gal}(f) \subseteq S_n$ and is often S_n.

Galois Groups

Definition

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.

- $\mathrm{Gal}(f)$ is a group of permutations of the roots of f.
- All permutations of n roots are in S_n so $\mathrm{Gal}(f) \subseteq S_n$ and is often S_n.
- Previous algorithms for computing Galois groups (except Hulpke [Hul99]) all restricted the degrees of the polynomials they accepted as input.
- Previous algorithms and their degree restrictions :
  - Geißler [Gei03] (23),
  - Geißler and Klüners [GK00] (15),
  - Eichenlaub [Eic96] and Oliver (11),
  - Absolute resolvent methods (11).
- Our approach following [FK14] is based on that of Stauduhar [Sta73].

First Example

Let $f(x) = x^4 - 4x^2 - 5 = (x^2 + 1)(x^2 - 5)$.

The Galois group of f is a subgroup of S_4.

Since the 4 roots of f can be grouped into pairs, a number of these 24 permutations in S_4 do not correspond to automorphisms of $\mathbb{Q}(i, \sqrt{5})$.

The Galois group of f has 4 elements, generated by the permutations

- $i \mapsto -i$ and
- $\sqrt{5} \mapsto -\sqrt{5}$

both of order 2.

The splitting field of $f, \mathbb{Q}(i, \sqrt{5})$, has degree 4 over $\mathbb{Q}$.

Second example

Let $f(x) = x^4 - 2 = (x^2 - \sqrt{2})(x^2 - i^2\sqrt{2})$.

The 4 roots of f are $\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}$ and $-i\sqrt[4]{2}$.

The Galois group of f is again a subgroup of S_4 but this time the symmetries between the roots are different.

The Galois group of f has 8 elements, generated by the permutations

- $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$ of order 4 and
- $i\sqrt[4]{2} \mapsto -i\sqrt[4]{2}$ of order 2.

The splitting field of $f, \mathbb{Q}(\sqrt[4]{2}, i)$, has degree 8 over $\mathbb{Q}$.

Third Example

Let $f = x^4 + x^3 - x^2 + x + 6$ which factors as a linear and a cubic (f_3) over $K = \mathbb{Q}[x]/f$ and as 2 linears and a quadratic over $K[x]/f_3(x)$. There are no other algebraic equations satified by the roots of f and hence there is no symmetry between these 4 roots.

The Galois group of f is S_4 and is generated by the permutations

- $\alpha \mapsto \beta, \beta \mapsto \gamma, \gamma \mapsto \delta, \delta \mapsto \alpha$ of order 4 and
- $\alpha \mapsto \beta$ of order 2

where α, β, γ and δ are the roots of f in some order.

The splitting field of f has degree 24 over $\mathbb{Q}$.

Invariants

Definition

A polynomial $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ such that $I^\tau = I$ for all $\tau \in H$ for some group $H \subseteq S_n$ is said to be *H-invariant*.

Definition

A H-invariant polynomial $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is a *G-relative H-invariant* polynomial if $I^\tau \neq I$ for all $\tau \in G \setminus H, H \subset G \subseteq S_n$, that is, for the stabiliser in G we have $\mathrm{Stab}_G\, I = H$.

Resolvents

Definition

For a G-relative H-invariant polynomial I we can compute a G-relative H-invariant *resolvent polynomial*

$$Q_{(G,H)}(y) = \prod_{\tau \in G//H} (y - I^{\tau}(x_1, \ldots, x_n)),$$

where $G//H$ denotes a system of representatives for the right cosets $H\tau$ of G/H. If $G = S_n$ then we call Q an *absolute resolvent*, otherwise we call Q a *relative resolvent*.

Blocks

Definition

Let G be a transitive permutation group acting on a finite set Ω. A subset $\emptyset \neq \Delta \subset \Omega$ is called a *block* if $\Delta \cap \Delta^\sigma \in \{\emptyset, \Delta\}$ for all $\sigma \in G$.
The orbit of a block Δ under G is called a *block system*.

The blocks we use will be subsets of $\Omega = \{\text{roots of } f\}$.

Stauduhar

Theorem (Generalization of [Sta73], Theorem 5)

Let $f(x)$ be a separable polynomial of degree n over a field F. Let $\alpha_1, \ldots, \alpha_n$ be a fixed ordering of the roots of $f(x)$ in S_f. Suppose G is a subgroup of S_n and suppose that with respect to the given ordering of the roots, the Galois group $\mathrm{Gal}(f)$ of $f(x)$ is a subgroup of G. Let H be a subgroup of G and $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ be a G-relative H-invariant polynomial. Let $\tau_1, \ldots, \tau_k$ be representatives for the right cosets of H in G. For all $i, I^{\tau_i}(\alpha_1, \ldots, \alpha_n)$ is a root of the resolvent polynomial

$$Q_{(G,H)}(y) = \prod_{i=1}^{k}(y - I^{\tau_i}(\alpha_1, \ldots, \alpha_n)) \in F[y].$$

Assume $I^{\tau_i}(\alpha_1, \ldots, \alpha_n)$ is not a repeated root of $Q_{(G,H)}(y)$. Then $\mathrm{Gal}(f) \subseteq \tau_i H \tau_i^{-1}$ iff $I^{\tau_i}(\alpha_1, \ldots, \alpha_n) \in F$.

Stauduhar — Idea of Proof/Use of Invariants

Very roughly,

$$I(\alpha_1, \ldots, \alpha_n) \in F \Rightarrow \sigma(I) = I, \sigma \in \mathrm{Gal}(f) \Rightarrow \mathrm{Gal}(f) \cap G \subseteq H \Rightarrow \mathrm{Gal}(f) \subseteq H$$

$$\sigma \in \mathrm{Gal}(f) \subset H \Rightarrow \sigma(I) = I \Rightarrow I(\alpha_1, \ldots, \alpha_n) \in F$$

When $\mathrm{Gal}(f) \subseteq H$, the symmetries between the roots contribute to $I(\alpha_1, \ldots, \alpha_n) \in F$.

Examples

Invariants for the maximal subgroups of S_4 are :

1. $x1$ (non transitive)
2. $((x1 + x2)^2 + (x3 + x4)^2)$
   - $(-\sqrt[4]{2} + \sqrt[4]{2})^2 + (-i\sqrt[4]{2} + i\sqrt[4]{2})^2 = 0 \in \mathbb{Q}$
   - $(-i + i)^2 + (-\sqrt{5} + \sqrt{5})^2 = 0 \in \mathbb{Q}$
3. $(((x2-x4)*(x3-x4))*(((x1-x3)*(x1-x2))*((x1-x4)*(x2-x3))))$

```
> for x in MaximalSubgroups(Sym(4)) do
for> for y in Sym(4) do
for|for> Evaluate(RelativeInvariant(Sym(4), x`subgroup),
      PermuteSequence([x[1] : x in Roots(f, KKK)], y)) in Q;
for|for> end for;
for> end for;
false false false false false false false false ...
```

The Fieker–Klüners Algorithm

Algorithm (Computation of the Galois group of a polynomial)

Input : a monic, integral, separable polynomial f of degree n 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.*
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*

Setup for Galois group computation

The algorithm was stated in full generality. Here we detail the specific differences for characteristic p function fields.

1. Splitting Field $S_{f,P}$:
   - when F is a number field can use the complex field or a p-adic field.
   - when F is a function field can use a series ring as an analogue of a p-adic field.

   These p-adic completions have better precision management than the complex field.
2. We can compute a smaller starting group using the subfields of $F[x]/f$. For function fields with characteristic p these can now be computed using [vHKN11]. This may save a number of "descent" steps (3) from S_n – a substantial gain for some groups.

Invariants (Step 3.1)

- When F has characteristic 0 invariants in $\mathbb{Z}[X_1, \ldots, X_n]$ can be used.
- When F is a characteristic p function field invariants in $\mathbb{F}_q[t][X_1, \ldots, X_n]$, must be used.
- The general $I(\underline{X}) = \sum_{\tau \in H} (\prod_{i=1}^{n-1} X_i^i)^\tau$ is expensive to use due to many multiplications.
- When $G \not< A_n, H < A_n$, $I(\underline{X}) = \prod_{1 \le k < j \le n} (X_k - X_j)$ (SqrtDisc) is sometimes better but I is G-invariant in characteristic 2.
- In characteristic 2 when $G \not< A_n, H < A_n$ we can use

$$I(\underline{X}) = \prod_{1 \le k < j \le n} (X_k + \bar{u} X_j) = I_1 + \bar{u} I_2 \text{ ([Els13] SqrtDisc)}$$

where I_1 and I_2 are also G-relative H-invariant and $\bar{u}$ is the image of u in $\mathbb{F}_2[u]/\langle u^2 - 1 \rangle$, also $I(\underline{X}) = \sum_{1 \le k < j \le n} X_k \frac{\prod_{1 \le r < s \le n}(X_r + X_s)}{X_k + X_j}$ although the former is the most efficient.

An invariant in characteristic 2

$\mathbf{s_1} \equiv \mathbf{s_m}$ When $G \subseteq S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$ there is a subgroup H with the same block systems as G such that

$$I(\underline{X}) = \prod_{b \in B} E(\{X_j : j \in b\}) \tag{s_m}$$

where E is the efficient [Els13] SqrtDisc invariant and

$$I(\underline{X}) = \sum_{b \in B} \Big(\sum_{j, j' \in b, j < j'} \frac{X_j}{X_j + X_{j'}} \Big) \tag{s_1}$$

are both G-relative H-invariant where $B = \{b_i\}_{1 \leq i \leq l}$ is a block system of both G and H, $\# b_i = n/l$.

Other invariants in characteristic $p \neq 2$

When the characteristic of F is not 2, the following gives polynomials $I(\underline{X}) = I(X_1, \ldots, X_n)$ which are G-relative H-invariant polynomials for some maximal subgroup H when G satisfies the conditions given.

SqrtDisc, [Gei03] Algorithm 6.24 Step 1 When $G \not< A_n, H < A_n$

$$I(\underline{X}) = \prod_{1 \leq i < j \leq n} (X_i - X_j)$$

D, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.2 When G is a subgroup of $S_{n/l} \wr_{\Gamma} S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, H is a subgroup of $S_{n/l} \wr_{\Gamma} A_l$ having the same block systems as G,

$$I(\underline{X}) = \prod_{1 \leq i < j \leq \#B} (y_i - y_j)$$

where $y_j = \sum_{j' \in b_j} X_{j'}$ and B is a block system of both G and H, $|B| = l, \#b_j = n/l, b_j \in B$.

Other invariants

Let H be a maximal subgroup of $G \subseteq S_n$. Then for all characteristics of F, the following gives polynomials $I(\underline{X}) = I(X_1, \ldots, X_n)$ which are G-relative H-invariant polynomials when G and H satisfy the conditions given.

Intransitive, [FK14] Lemma 5.1 When H is an intransitive group and there is an orbit $\mathcal{O}$ of H which is not invariant under G,

$$I(\underline{X}) = \sum_{i \in \mathcal{O}} X_i.$$

ProdSum, [Gei03] Algorithm 6.24 Step 3.1, [FK14] Lemma 5.3, [Els14b]

When there exists a block system B of H which is not a block system of G,

$$I(\underline{X}) = \prod_{b \in B} (\sum_{i \in b} X_i) \text{ and } I(\underline{X}) = \sum_{b \in B} (\sum_{i \in b} X_i)^e$$

where $e = 2$ unless $p = 2$ then $e = 3$.

Theorem ([Fie09], [Gei03] Satz 6.21, Algorithm 6.24 Step 5, [FK14] Lemma 5.8)

Let $H_1, H_2 \subset G \subseteq S_n$ be two distinct subgroups of index 2 in G with G-relative H_i-invariants I_i, $G//H_i = \{\mathrm{Id}, \tau_i\}$. Then, when the characteristic of F is 2,

$$I(\underline{X}) = \begin{cases} I_1 + I_2, & \text{if } I_i^{\tau_i} = I_i + 1 \\ I_1 I_2^{\tau_2} + I_2 I_1^{\tau_1} & \text{otherwise} \end{cases}$$

is a G-relative H-invariant where $H = \langle H_1 \cap H_2, \tau_1\tau_2 \rangle$ and when the characteristic of F is not 2

$$I(\underline{X}) = I_1 I_2, \text{ if } I_i^{\tau_i} = -I_i$$

$$I(\underline{X}) = (I_1 - I_1^{\tau_1})(I_2 - I_2^{\tau_2}) \text{ otherwise}$$

is a G-relative H-invariant where $H = (H_1 \cap H_2) \cup ((G \setminus H_1) \cap (G \setminus H_2))$.

First Example

```
> SetVerbose("GaloisGroup", 3);
> G, R, S := GaloisGroup(x^4-4*x^2-5);

Intransitive case!
 computing Galois groups of factors...
    Found some possible primes:  [
        <7, [ 2, 2 ], 2>
    ]

 computing starting group
starting group order  4
 done, and now the descents...
Start Generic Stauduhar Algo
Trying to descend from group of order 4 = [ <2, 2> ]
```

First Example (cont)

```
Have to consider  3 subgroups (classes of them) initially
Reduce to 3 (using divisor of order 1)
Further reduce to 3 (using rejected subgroups)
Further reduce to 3 (using normal and known subgroups)
Further reduce to 1 (using sieve)
Doing Stauduhar for group 2 of index 2 = [ <2, 1> ] with
                             invariant of type FactorDelta

removed all cosets
Time: 0.000
 Stauduhar returns  0  (subgroup ruled out)
 added wrong subgroup
All subgroups are ruled out.
```

First Example (cont)

```
> G;
Permutation group G acting on a set of cardinality 4
Order = 4 = 2^2
    (1, 2)
    (3, 4)
> Z<z> := Universe(R);
> R;
[ -3*z - 2 + O(7), 3*z + 2 + O(7),
                    -z - 3 + O(7), z + 3 + O(7) ]
> RelativeInvariant(G, Subgroups(G)[3]`subgroup);
((x3 - x4) * (x1 - x2))
```

Second Example

```
> G, R, S := GaloisGroup(x^4-2);
Choose p=  73  of type : [ 1, 1, 1, 1 ]
Finding splitting field
Input over :  73-adic ring
Compute starting group:
Degrees of subfields [ 2 ]
Trying to identify the blocksystem with precision 1
Starting group reached lower bound of order 8
> TransitiveGroupDescription(G); G;
D(4)
Permutation group G acting on a set of cardinality 4
Order = 8 = 2^3
    (1, 2)(3, 4)             (2, 3)
> R;
[ 739032016 + O(73^5), -725592308 + O(73^5),
                725592308 + O(73^5), -739032016 + O(73^5) ]
```

Third Example

```
> G, R, S := GaloisGroup(x^4 + x^3 - x^2 + x + 7);
GetShapes started....
Shapes and primes found:
[ 1, 1, 2 ] [ 7, 41, 47, 61, 79 ]
[ 2, 2 ] [ 59 ]
[ 1, 3 ] [ 5, 11, 17, 19, 23, 29, 31, 43, 53, 83 ]
[ 4 ] [ 13, 37, 71, 73 ]
Choose p=  379  of type : [ 1, 1, 1, 1 ]
Sn found
> TransitiveGroupDescription(G); G;
S(4)
Symmetric group G acting on a set of cardinality 4
Order = 24 = 2^3 * 3
    (1, 2, 3, 4)
    (1, 2)
```

Example over $\mathbb{F}_q(t)$ [Sut15b] Example 1, [Sut15a] Example 12

Let $F = \mathbb{F}_7(t)$ and $f = x^8 + t + 1 \in F[x], \mathrm{Gal}(f) \subseteq S_8$ with order 40320.

```
> SetVerbose("GaloisGroup", 3);
> F<t> := FunctionField(GF(7));
> P<x> := PolynomialRing(F);
> G, R, S := GaloisGroup(x^8 + t + 1);
Degrees of subfields [ 4, 2 ]
Computing group of subfield given by x^4 + t + 1

Proven subfield group (D_4) of order 8 found.
Reduced order of starting group by using subfield groups
to 64, TGI: 8T26 = 1/2[2^4]eD_4
Trying to descend from group of order 64

Have to consider  6 subgroups (classes of them) initially
```

```
Lifting roots in Power series ring over GF(7^16) to
precision 10

Further reduce to 4 (using rejected subgroups)
Further reduce to 2 (using sieve)

Doing Stauduhar for group 1 of index 2 = (TGI: 8T15)
no cosets remaining, group not possible
Doing Stauduhar for group 5 of index 2 = (TGI: 8T15)
Found 2 cosets as simple zeros and 0 cosets as multiples
DESCENT

Trying to descend from group of order 32
Have to consider  6 subgroups (classes of them) initially
Further reduce to 4 (using rejected subgroups)

Doing Stauduhar for group 5 of index 2 = (D_8)
no cosets remaining, group not possible
```

```
Doing Stauduhar for group 1 of index 2 = (TGI: 8T8)

Doing Stauduhar for group 3 of index 2 =  (TGI: 8T8)
no cosets remaining, group not possible

Doing Stauduhar for group 6 of index 2 = (D_8)

Doing Stauduhar for group 1 of index 2 =  (TGI: 8T8)

Doing Stauduhar for group 6 of index 2 = (D_8)
Found 2 cosets as simple zeros and 0 cosets as multiples

DESCENT

Trying to descend from group of order 16
Have to consider 2 subgroups (classes of them) initially
Reduce to 2 (using divisor of order 1)
Further reduce to 0 (using rejected subgroups)

Time: 0.360
```

```
> TransitiveGroupDescription(G); G;
D(8)
Permutation group G acting on a set of cardinality 8
Order = 16 = 2^4
     (2, 8)(3, 7)(4, 6)
     (1, 2)(3, 8)(4, 7)(5, 6)
     (1, 3, 5, 7)(2, 4, 6, 8)
     (1, 5)(2, 6)(3, 7)(4, 8)
> Z<z> := Universe(R); W<w> := CoefficientRing(Z);
> WW<ww> := Parent(Eltseq(Eltseq(R[1])[1])[1]);
> Z, R;
Power series ring in z over GF(7^16)
[   (5*ww + 5)*w^3 + 4*ww*w^3*z + ... + O(z^4),
    (5*ww + 2)*w^3 + (6*ww + 4)*w^3*z + ... + O(z^4),
    (3*ww + 1)*w^3 + 5*w^3*z + 5*w^3*z^2 + ... + O(z^4),
    (4*ww + 1)*w^3 + (ww + 4)*w^3*z + ... + O(z^4),
    .
    .  ]
```

Example over an extension of $\mathbb{F}_q(t)$

```
> F<t> := FunctionField(GF(7));
> P<x> := PolynomialRing(F);
> FF<a> := FunctionField(x^2 + t);
> P<x> := PolynomialRing(FF);
> time G := GaloisGroup(x^8 + a + 1);
Time: 0.460
> G;
Permutation group acting on a set of cardinality 8
Order = 16 = 2^4
    (1, 8)(2, 7)(3, 6)(4, 5)
    (1, 8, 7, 6, 5, 4, 3, 2)
    (1, 3, 5, 7)(2, 4, 6, 8)
    (1, 5)(2, 6)(3, 7)(4, 8)
> TransitiveGroupDescription(G);
D(8)
```

Examples of polynomials with degree > 23

```
> F<t> := FunctionField(GF(7)); P<x> := PolynomialRing(F);
> f := x^103 + t + 4; time G := GaloisGroup(f); G;
Time: 479.330
Permutation group G acting on a set of cardinality 103
Order = 5253 = 3 * 17 * 103
```

```
> f := x^143 + t + 4; time G := GaloisGroup(f); G;
Time:  1338.900
Permutation group G acting on a set of cardinality 143
Order = 8580 = 2^2 * 3 * 5 * 11 * 13
```

```
> f := x^201 + t + 4; time G := GaloisGroup(f); G;
Time: 3554.240
Permutation group G acting on a set of cardinality 201
Order = 13266 = 2 * 3^2 * 11 * 67
```

Splitting Field by Factorization

```
> Fqt<t>:=FunctionField(GF(101)); P<x>:=PolynomialRing(Fqt);
> f := x^6 + 98*t*x^4 + (2*t + 2)*x^3 + 3*t^2*x^2 +
>             (6*t^2 + 6*t)*x + 100*t^3 + t^2 + 2*t + 1;
> tt := Cputime(); F := ext<Fqt | f>;
> time Factorization(Polynomial(F, f));
[
    <$.1 + 100*F.1, 1>,
    <$.1 + 26*t/(t^3 + 2*t^2 + 4*t + 2)*F.1^5 +
        (66*t + 66)/ (t^3 + 2*t^2 + 4*t + 2)*F.1^4 + ....
    <$.1^2 + (13*t/(t^3 + 2*t^2 + 4*t + 2)*F.1^5 + (33*t +
        33)/(t^3 + 2*t^2 + 4*t + 2)*F.1^4 + 24*t^2/(t^3 +
        2*t^2 + 4*t + 2)*F.1^3 + ....
    <$.1^2 + (62*t/(t^3 + 2*t^2 + 4*t + 2)*F.1^5 + (2*t + 2)/
        (t^3 + 2*t^2 + 4*t + 2)*F.1^4 + ....
]
Time: 0.040
```

Splitting Field by Factorization (cont)

```
> FF := ext<F | $1[3][1] : Check := false>;
> time Factorization(Polynomial(FF, DefiningPolynomial(FF)));
[
    <$.1 + 100*FF.1, 1>,
    <$.1 + FF.1 + 13*t/(t^3 + 2*t^2 + 4*t + 2)*F.1^5 + .....
]
Time: 2.860
> time Factorization(Polynomial(FF, $2[4][1]));
[
    <$.1 + 100*FF.1 + 75*t/(t^3 + 2*t^2 + 4*t + 2)*F.1^5 + ...
    <$.1 + FF.1 + 88*t/(t^3 + 2*t^2 + 4*t + 2)*F.1^5 + ....
]
Time: 3.660
> Cputime(tt);
7.170
```

Computing Fixed Fields of Subgroups

Algorithm (Compute a Fixed Field of a subgroup ([FK06]))

Given a subgroup $U \subseteq G = \mathrm{Gal}(f)$ 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 a bound B on the evaluation of I at the roots $\{r_i\}_{i=1}^n$ and compute the roots to a precision that allows the bound B to be used.*
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 using B. The resulting polynomial defines the fixed field of U.*

Computing Fixed Fields of Subgroups

Algorithm (Compute a Fixed Field of a subgroup ([FK06]))

Given a subgroup $U \subseteq G = \mathrm{Gal}(f)$ 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 a bound B on the evaluation of I at the roots $\{r_i\}_{i=1}^n$ and compute the roots to a precision that allows the bound B to be used.*
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 using B. The resulting polynomial defines the fixed field of U.*

$$\beta = I(r_1, \ldots, r_n) \to g(\beta) = 0,$$

$$\sigma \in U \to \sigma(\beta) = I^\sigma(r_1, \ldots, r_n) = I(r_1, \ldots, r_n) = \beta.$$

Computations of a Splitting Field using Fixed Fields

Algorithm (Compute a Splitting Field using a fixed field of the Galois group)

Given a polynomial f over F compute the splitting field of f over F.

1. *Compute $G = \mathrm{Gal}(f)$.*
2. *Compute the fixed field of the subgroup $\{\mathrm{Id}(G)\}$.*

Example of a splitting field computed using a fixed field

```
> tt := Cputime(); G, _, S := GaloisGroup(f); G;
Permutation group G acting on a set of cardinality 6
Order = 12 = 2^2 * 3
    (2, 3)(5, 6)
    (1, 2)(4, 5)
    (1, 4)(2, 5)(3, 6)
> time FunctionField(GaloisSubgroup(S, sub<G | >)));
Algebraic function field defined over Univariate rational
function field over GF(101) by
x^12 + 47*t*x^10 + 3*t^2*x^8 + (65*t^3 + 54*t^2 + 7*t
    + 54)*x^6 + (41*t^4 + 18*t^3 + 36*t^2 + 18*t)*x^4 +
    (14*t^5 + 61*t^4 + 21*t^3 + 61*t^2)*x^2 + 80*t^6 +
    77*t^5 + 75*t^4 + 64*t^3 + 31*t^2 + 88*t + 22
Time: 0.050
> Cputime(tt);
0.500
```

Algorithm (Compute a Splitting Field as a tower of extensions using a Galois group ([FK06]))

Given a polynomial $f \in F[x]$ of degree n, where F is $\mathbb{Q}, \mathbb{Q}(\alpha)$ or $\mathbb{F}_q(t)$, compute a splitting field for f as a tower of extensions of F.

1. *Compute $G = \mathrm{Gal}(f)$. If G is trivial then F is a splitting field.*
2. *Compute a descending chain C of subgroups C_k of G as stabilizers and matching invariants I_k starting with $C_0 = G$.*
3. *for each $C_k \neq G$ in the chain C find the minimal polynomial of a relative primitive element for the next extension F_k by*
    1. *Compute the right transversal $T_k = C_{k-1}//C_k$.*
    2. *Compute the p-adic roots of f to enough precision and transform them.*
    3. *Compute the coefficients of the absolute basis for the power sums of evaluations of I_k at the transformed roots permuted by each permutation in $\tau \in T_k$ multiplied by each permutation π in $\prod_{j<k} T_j$.*
    4. *Map these coefficients back to F and so gain the power sums in F_{k-1}.*
    5. *The monic polynomial whose other coefficients are elementary symmetric functions in the power sums defines F_k.*

Problems in Characteristic p

The elementary symmetric functions using power sums p_m are

$$le_l(x_i) = \sum_{m=1}^{l} (-1)^{m-1} e_{l-m}(x_i) p_m(x_i), 1 \leq l \leq \# T_k$$

Problems in Characteristic p

The elementary symmetric functions using power sums p_m are

$$le_l(x_i) = \sum_{m=1}^{l} (-1)^{m-1} e_{l-m}(x_i) p_m(x_i), 1 \leq l \leq \# T_k$$

What if $\# T_k \geq \mathrm{char}(F)$ so that $l \equiv 0 \mod \mathrm{char}(F)$ occurs?

The elementary symmetric functions using power sums p_m are

$$le_l(x_i) = \sum_{m=1}^{l} (-1)^{m-1} e_{l-m}(x_i) p_m(x_i), 1 \leq l \leq \# T_k$$

What if $\# T_k \geq \mathrm{char}(F)$ so that $l \equiv 0 \mod \mathrm{char}(F)$ occurs?

Can we compute the coefficients of

$$\prod_{\tau \in T_k} (x - I^{\tau}(r_1, \ldots, r_n))$$

without directly using elementary symmetric functions?

Example of a splitting field computed as a tower

```
> time GSF := GaloisSplittingField(f : Roots := false);
Time: 0.750
> Fqta<aa> := CoefficientField(GSF);
> _<y> := PolynomialRing(Fqta);
> GSF:Maximal;
  GSF
   |    y^2 + (62*t/(t^3 + 2*t^2 + 4*t + 2)*aa^5 + (2*t + 2)/
   |    (t^3 + 2*t^2 + 4*t + 2)*aa^4 + 29*t^2/(t^3 + 2*t^2
   |    + 4*t + 2)*aa^3 + (50*t^2 + 50*t)/(t^3 + 2*t^2 + 4*t
   |    + 2)*aa^2 + (8*t^3 + 4*t^2 + 8*t + 4)/(t^3 + 2*t^2 +
   |    4*t + 2)*aa + (92*t^3 + 92*t^2)/(t^3 + 2*t^2 + 4*t +
   |    2))*y + (2*t + 2)/(t^3 + 2*t^2 + 4*t + 2)*aa^5 + ....
Fqta<aa>
   |          x^6 + 98*t*x^4 + (2*t + 2)*x^3 + 3*t^2*x^2 +
   |              (6*t^2 + 6*t)*x + 100*t^3 + t^2 + 2*t + 1
Univariate rational function field over GF(101)
```

Solution of a polynomial by radicals

Algorithm (Solve a polynomial by radicals using its Galois group)

Given a polynomial f over F compute a tower of radical extensions over which f splits.

1. *Compute $G = \mathrm{Gal}(f)$ and check G is solvable.*
2. *Determine which roots of unity are needed and compute the Galois group G of the product of f and the associated cyclotomic polynomials divided by their GCD with f.*
3. *Compute a chain C of subgroups, starting with G, then those which stabilize an increasing number of roots of unity and ending with the rest of the composition series.*
4. *Compute the tower of cyclic fields from C using the Splitting Field Algorithm Step 3.*
5. *Transform cyclic extensions to radical extensions.*

Cyclic extension to radical extension

degree 2 map α, a zero of $x^2 + a_1 x + a_0$, to $\alpha + a_1/2$, a zero of $x^2 - a_0/4$

degree > 2 $\sum_i \zeta^i \sigma^{(n-i)}(a)$, is a primitive element such that its degree-th power is in F_{k-1} where ζ is a root of unity and σ generates the automorphism group of the cyclic extension[1].

[1] B. L. van der Waerden, *Modern algebra*, Frederick Ungar Publishing Co., 1966.

Automorphisms

- Used Galois group when extension was at the top
- Can always use Galois group since each extension in the tower is normal even if the extension is not normal as an extension of the coefficient ring of the polynomial
- Can get the Galois group for free from the Galois correspondence as the cyclic group of order p which is the quotient of two subgroups of the Galois group.
- Even easier than that : all non-identity elements of a cyclic group of order p generate the group so can use any automorphism, that is, map the generator of the cyclic but non radical extension to any one of the roots of the cyclic defining polynomial.
- So at least one of the three problems is solved!

Degree = Characteristic extensions

In characteristic p :

- $x^p - a$ is inseparable : only has one distinct root, not p, derivative 0
- In a cyclic degree p extension F_k/F_{k-1} there exists β such that $\beta^p - \beta \in F_{k-1}$.[2]
- $x^p - x - a = \prod_{i=1}^{p-1}(x - (\beta + i))$ defines an Artin–Schreier extension.
- It is customary to use a wider definition of solvability by radicals in prime characteristic.[3]
- In prime characteristic allow adjoining of elements α such that $\alpha^p - \alpha$ lies in a given field.[4]

[2] H. Stichtenoth, *Algebraic function fields and codes*, Springer, 1993, A13

[3] I. Stewart, *Galois Theory*, Chapman and Hall, 1989, p 129

[4] I. Stewart, *Galois Theory*, Chapman and Hall, 1989, Remark p 147

How to compute a such that $x^p - x + a$ defines the cyclic extension?

S. Lang, Algebra, Springer, 2002, Theorems 6.3 and 6.4 give us

$$\alpha = 1/\mathrm{Tr}(\theta) \sum_{i=1}^{p-1} i\sigma^i(\theta)$$

where $\mathrm{Tr}(\theta) \neq 0$, so

$$a = \alpha^p - \alpha$$

Two problems solved!

Example of a solution of polynomial by radicals

```
> time S := SolveByRadicals(f); CS<cs> := CoefficientRing(S);
Time: 0.940
> _<t> := CoefficientRing(CS); S:Maximal;
    S
    |           $.1^2 + 100*t
  CS<cs>
    |           $.1^3 + 8*t + 8
    |
Univariate rational function field over GF(101^2)
Variables: t
> DefiningPolynomial(ConstantField(S));
t^2 + 26
> _<w> := ConstantField(S); Roots(f, S);
[ <S.1 + (51*w + 25)*cs, 1>,  <100*S.1 + (51*w + 25)*cs, 1>,
  <S.1 + (50*w + 25)*cs, 1>,  <100*S.1 + (50*w + 25)*cs, 1>,
  <S.1 + 51*cs, 1>,           <100*S.1 + 51*cs, 1> ]
```

An example with a degree characteristic extension

```
> f := x^5 + x^4 + t; G := GaloisGroup(f);
> TransitiveGroupDescription(G); IsSoluble(G);
F(5) = 5:4                           true
> S := SolveByRadicals(f); CS<cs> := CoefficientRing(S);
> CCS<ccs> := CoefficientRing(CS);
> S:Maximal;
     S
     |                       $.1^5 + 4*$.1 + 2/t^2*ccs*cs
   CS<cs>
     |                                      $.1^2 + 2*ccs
  CCS<ccs>
     |                                        x^2 + 4*t^3
Univariate rational function field over GF(5)
Variables: t
```

And the radical roots

```
> Roots(f, S);
[    <S.1^4 + S.1^3 + S.1^2 + S.1, 1>,
     <S.1^4 + 3*S.1^3 + 4*S.1^2 + 2*S.1, 1>,
     <S.1^4 + 2*S.1^3 + 4*S.1^2 + 3*S.1, 1>,
     <S.1^4 + 4*S.1^3 + S.1^2 + 4*S.1, 1>,
     <S.1^4 + 4, 1>
]
> Roots(f, FunctionField(f));
[
     <$.1, 1>
]
```

Y. Eichenlaub, *Problémes effectifs de théorie de Galois en degrés 8 á 11*, Ph.D. thesis, Université Bordeaux I, 1996.

A.-S. Elsenhans, *Invariants for the computation of intransitive and transitive Galois groups*, Journal of Symbolic Computation **47** (2012), 315–326.

______, Personal communication, 2013.

______, *A note on short cosets*, Experimental Mathematics **23** (2014), 411–413.

______, *On the construction of relative invariants*, 2014.

C. Fieker, Magma implementation and personal communication, 2009.

C. Fieker and J. Klüners, *Galois group implementations*, MAGMA V2.13 implementation with more recent contributions also from A.-S. Elsenhans, 2006.

- ———, *Computation of Galois groups of rational polynomials*, London Mathematical Society Journal of Computation and Mathematics **17** (2014), no. 1, 141 – 158.
- K. Geißler, *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*, PhD Thesis, Technische Universität Berlin, 2003, available at http://www.math.tu-berlin.de/˜kant/publications/diss/geissler.pdf.
- K. Geißler and J. Klüners, *Galois group computation for rational polynomials*, Journal of Symbolic Computation **30** (2000), no. 6, 653–674.
- Alexander Hulpke, *Techniques for the computation of Galois groups*, Algorithmic algebra and number theory. Selected papers from a conference, Heidelberg, Germany, October 1997 (Berlin) (B. Heinrich Matzat et al., ed.), Springer, 1999, pp. 65–77.
- Richard P. Stauduhar, *The determination of Galois groups*, Mathematics of Computation **27** (1973), 981–996.

- N. Sutherland, *Algorithms for Galois extensions of global function fields*, Ph.D. thesis, The University of Sydney, 2015.
- ______, *Computing Galois groups of polynomials (especially over function fields of prime characteristic)*, Journal of Symbolic Computation **71** (2015), 73–97.
- M. van Hoeij, J. Klüners, and A. Novocin, *Generating subfields*, ISSAC 2011, 2011.