Methods for computing Galois groups

Joachim König

KAIST, Daejeon

Dresden Summer School, July 13th 2019

Some generalities

- $f \in K[X]$ a separable polynomial over some field K; $G = Gal(f/K)$, the Galois group of (the splitting field of) f over K, embeds naturally into S_n via its action on the roots of f.
- G is a transitive group in this action $\Leftrightarrow$ f is irreducible.

Dedekind's reduction criterion

Theorem (Dedekind)

Let $f \in \mathbb{Z}[X]$ be a separable polynomial of degree n over the rationals, and let $G \leq S_n$ be its Galois group. Let p be a prime number and denote by $\overline{f} \in (\mathbb{F}_p)[X]$ the modulo-p reduction of f. If $\overline{f}$ is separable of degree n, then $Gal(\overline{f}/\mathbb{F}_p)$ is a subgroup of G.

Remarks:

- Only finitely many primes fail the assumptions of the theorem (namely, prime divisors of the discriminant of f, and of the leading coefficient of f).
- The theorem remains true in a much more general setup. Instead of the coefficient ring $R = \mathbb{Z}$, one may choose for R any "Dedekind domain" (e.g., the ring of integers O_K of a number field K, or a polynomial ring $K[t]$). The reduction should then be modulo a maximal ideal of R.

Dedekind's reduction criterion

Particularly useful application:

Theorem (Dedekind)

If f mod p is separable of degree n and splits into irreducible factors of degrees $n_1, \dots, n_k$ over $\mathbb{F}_p$, then G contains an element of cycle structure $[n_1, \dots, n_k]$.

- This is because $Gal(\overline{f}/\mathbb{F}_p) \leq S_n$ is cyclic, with orbits exactly the roots of the respective irreducible factors.

Example I

Take $f = X^5 - X + 1 \in \mathbb{Z}[X]$.

- f mod 2 is $(X^3 + X^2 + 1)(X^2 + X + 1)$, so $Gal(f)$ contains an element of cycle structure $[3, 2]$
- f mod 3 is irreducible, so $Gal(f)$ contains a 5-cycle.
- In total, $Gal(f)$ is a subgroup of S_5 containing elements of order 5 and 6. In particular, its order is a multiple of 30, and then it must be S_5.

- **Example II**: Construction of polynomials with Galois group S_n for any n (Exercise!).
- **Deeper result**:

Frobenius (or Chebotarev) density theorem

If one moves p through the set of all prime numbers, every cycle structure of the Galois group G will eventually occur (infinitely often) as a factorization pattern of $\overline{f} = f \bmod p$.

p-adic fields, inertia and decomposition groups

- Dedekind's criterion applies to almost all primes. However, it is often exactly the few primes that were "sorted out" which provide the most useful information!
- A "classical" example: Eisenstein's criterion. Reduction mod p gives $\overline{f} = X^n$, so seemingly no information.
  But then one reduces also mod p^2, and everything is fine!
  This is the first example of considering an integer polynomial over the p-adic field $\mathbb{Q}_p$.

p-adic fields, inertia and decomposition groups

Ramification and splitting of prime ideals

- p a prime number, $K/\mathbb{Q}$ a finite extension, O_K the ring of integers of K.
- Then the ideal $p \cdot O_K$ has a unique factorization $p \cdot O_K = \prod \mathfrak{p}_i^{e_i}$ into prime ideals of O_K (the $\mathfrak{p}_i$ are said to **extend** p).
- e_i: The **ramification index** of the ideal $\mathfrak{p}_i$ in $K/\mathbb{Q}$.
- $O_K/\mathfrak{p}_i$ is a finite extension of $\mathbb{Z}/p\mathbb{Z}$. The degree d_i of this extension is called the **(residue) degree** of $\mathfrak{p}_i$.

p-adic fields, inertia and decomposition groups

- **Important special case**: $K/\mathbb{Q}$ a Galois extension, with group G. Then G acts transitively on the set of all $\mathfrak{p}_i$ extending p. In particular, the degree d_i and ramification index e_i depend only on p (not on i).
- The stabilizer in G of $\mathfrak{p}_i$ is called the **decomposition group** of $\mathfrak{p}_i$ over p, denoted $D(\mathfrak{p}_i/p)$. The conjugacy class of this subgroup in G depends only on p, often denoted D_p.
- $D(\mathfrak{p}_i/p)$ acts on the residue field extension $(O_K/\mathfrak{p}_i)/(\mathbb{Z}/p\mathbb{Z})$. The kernel of this action is called the **inertia group** $I(\mathfrak{p}_i/p)$. If the ramification index is coprime to p, then the inertia group is **cyclic**.

Completions, inertia and decomposition groups

From now: Assumption $K/\mathbb{Q}$ Galois.

- Let $\mathbb{Q}_p \supset \mathbb{Q}$ the field of all p-adic numbers $\sum_{i=k}^{\infty} a_i p^i$ (with $k \in \mathbb{Z}$, $a_i \in \{0, \dots, p-1\}$, $a_k \neq 0$). Then the compositum $K_p := K \cdot \mathbb{Q}_p$ is the **completion** of K at $\mathfrak{p}_i$.
- The decomposition group D_p is isomorphic to the Galois group $Gal(K_p/\mathbb{Q}_p)$.
  (... and even **permutation-isomorphic** as a subgroup of $Gal(f)$!)
- The extension $K_p/\mathbb{Q}_p$ also has a ramification theory as above (but now, $p \cdot \mathbb{Z}_p$ is the **only** maximal ideal of the ring $\mathbb{Z}_p$).
- There is a unique maximal subextension $K_p^{ur}/\mathbb{Q}_p$ of $K_p/\mathbb{Q}_p$ in which the maximal ideal (p) has ramification index 1. Then $I(\mathfrak{p}_i/p)$ is isomorphic to $Gal(K_p/K_p^{ur})$ (and $[K_p^{ur} : \mathbb{Q}_p] = [D_p : I_p]$ is the residue degree of $\mathfrak{p}_i$).

- To obtain information about the Galois group $G = Gal(K/\mathbb{Q})$, it is obviously useful to find out about the structure of decomposition groups in G.
- If $e_i = 1$ (p is **unramified** in $K/\mathbb{Q}$), then the decomposition group $D_p(= D_p/I_p)$ is cyclic! This is the case that Dedekind's criterion deals with.

  (In particular, **Hensel's lemma** guarantees that a separable factorization of f mod p yields a factorization into the same degrees over $\mathbb{Q}_p$.)

Newton polygons

The Newton polygon is a graphical tool designed to give information about the factors of a polynomial over $\mathbb{Q}_p$, the orbits of the decomposition group D_p, and/or the inertia group I_p.

Definition (Newton polygon)

Let $f \in \mathbb{Q}_p[X]$ a polynomial of degree n. For each $j \in \{1, \dots, n\}$, let $\nu(j) \in \mathbb{Z} \cup \{+\infty\}$ be the p-adic valuation of the coefficient of f at X^j.
Draw all the points $(j, \nu(j))$ with $\nu(j) < \infty$ in the plane $\mathbb{R}^2$,
The **Newton polygon** of f is defined as the lower convex hull of this set of points.

Example: $f = 25X^5 + 5X^4 + X^3 + 5X + 5$ over $\mathbb{Q}_5$ gives vertices $(0,1)$, $(1,1)$, $(3,0)$, $(4,1)$, and $(5,2)$. The lower convex hull is spanned by the points $(0,1)$, $(3,0)$, $(5,2)$.

Newton polygons

Theorem

Let $\ell_1, \ldots, \ell_r$ be the line segments of the Newton polygon, let Δx_i and Δy_i be the respective lengths and heights, and let $s_i = \frac{\Delta y_i}{\Delta x_i} = \frac{a_i}{b_i}$ be their slopes (with $a_i \in \mathbb{Z}, b_i \in \mathbb{N}$ coprime).

i) *Then f factors over $\mathbb{Q}_p$ into (not necessarily irreducible) polynomials of degrees Δx_i.*

ii) *In particular, the sequence $[n_1, \ldots, n_k]$ of orbit lengths of D_p (on the roots of f) is a refinement of the partition $[\Delta x_1, \ldots, \Delta x_r]$ of n.*

iii) *On the other hand, any orbit length of the inertia group I_p corresponding to the line segment ℓ_i is a multiple of b_i.*

(Note that from the definition, the sequence of slopes is strictly increasing!)

Newton polygons

Example I

- $f = 25X^5 + 5X^4 + X^3 + 5X + 5$ over $\mathbb{Q}_5$ gives two line segments of lengths $\Delta x_1 = 3$, $\Delta x_2 = 2$, with slopes $-1/3$ and 1 respectively.
- Then f must split into an **irreducible** degree 3-factor, and a (possibly reducible) degree-2 factor.
- In particular, the inertia group is cyclic, generated either by $(1, 2, 3)$ or by $(1, 2, 3)(4, 5)$.
- (Actual result: $f = (X^3 - 25X^2 - 20X + 5)(25X^2 + 5X + 1) + O(5^3)$ is an irreducible factorization over $\mathbb{Q}_5$.)

Newton polygons

Example II: Eisenstein's criterion

Let $f \in \mathbb{Z}[X]$ be a degree-n polynomial fulfilling the assumption of Eisenstein's criterion for the prime p (leading coefficient not divisible by p, all others divisible, and constant coefficient not divisible by p^2). Then the Newton polygon consists of a single line segment of slope $-\frac{1}{n}$. Therefore, the inertia group $I_p \leq Gal(f)$ is transitive! In particular, f is irreducible not only over $\mathbb{Q}$, but also over $\mathbb{Q}_p$.

So far, all tools presented were designed to find **lower** bounds for the Galois group of a given polynomial. How to find **upper** bounds?

- Let's not forget some easy special cases. E.g., if $f(X) = g(h(X))$ is a composition of two polynomials of degree n and m, then $Gal(f)$ naturally becomes a subgroup of the **wreath product** $S_n \wr S_m = (S_n \times ... \times S_n) \rtimes S_m$. This does give an upper bound without any complicated computations!

Resolvents

A noteworthy special case: The discriminant

Recall: $\Delta(f) = \prod_{i<j}(\alpha_i - \alpha_j)^2$, where $\alpha_1, \ldots, \alpha_n$ are the roots of f.
Rather obviously, this expression is fixed under action of the Galois group of f (i.e., lies in the base field).
On the other hand $\sqrt{\Delta(f)}$ is fixed exactly under the **even** permutations in $Gal(f)$.

"Moral" of this example: The expression $\sqrt{\Delta(f)} = \prod_{i<j}(\alpha_i - \alpha_j)$ is an **invariant** of the group A_n. I.e., if $\Delta(f)$ is actually a square in the base field, then the Galois group must be contained in A_n. This gives a "descent argument" for the Galois group from S_n to A_n.
If the Galois group is in fact still smaller, we need similar arguments to descend even further.

Resolvents

The following approach to compute Galois groups was essentially outlined by Jordan (1870), and made practical for computation by Stauduhar 100 years later.

- Let $g \in S_n$, and for $F \in \mathbb{Z}[X_1, \ldots, X_n]$, define $F^g := F(X_{g(1)}, \ldots X_{g(n)})$. This gives an action of S_n on the multivariate polynomial ring.
- Now let $G \leq S_n$, and let $f \in \mathbb{Z}[X]$ be a monic degree-n polynomial with simple roots $\xi_1, \ldots, \xi_n$. Assume now that we have found a polynomial $F \in \mathbb{Z}[X_1, \ldots, X_n]$ whose stabilizer is G, i.e., $F^g = F$ if and only if $g \in G$.
- Let $F_1, \ldots, F_m$ be the conjugates of F in S_n (i.e., $m = [S_n : G]$) and set $\theta_G(f, F) = \prod_{j=1}^m (X - F_j(\xi_1, \ldots, \xi_n))$. $\theta_G f, F$ is called a **resolvent** for G.

Resolvents

Theorem

$\theta_G(f, F)$ is in $\mathbb{Z}[x]$, and if it is additionally separable, then: $Gal(f)$ is conjugate (in S_n) to a subgroup of G if and only if $\theta_G(f, F)$ has a root in $\mathbb{Z}$.

- Argument why $\theta_G(f, F)$ has integer coefficients: Let $F = X^n + a_{n-1}X^{n-1} + \ldots + a_0 = (X - \xi_1) \cdots (X - \xi_n)$ be a **generic** polynomial (with transcendentals a_i as coefficients). Then $\theta_G(f, F)$ is invariant under action of S_n, so the coefficients are integer polynomials in the **symmetric functions** of the ξ_i, i.e., in the coefficients a_i.

Resolvents

- In practice, one may use numerical approximations of the roots of f. These approximations then need to be sufficiently good to recognize with certainty when a certain approximate root of $\theta_G(f, F)$ is actually an integer.
- It remains to find a polynomial F with stabilizer G in the first place.
- **Simple example**: For $G = A_n \leq S_n$, the polynomial $F = \prod_{1 \leq i < j \leq n}(X_i - X_j)$ works. The resolvent then becomes $X^2 - \Delta(f)$.
- **Simple example**: For $G = D_4 \leq S_4$, the polynomial $F = X_1X_3 + X_2X_4$ works (Exercise!).

Some improvements

- The degree of $\theta_G(f, F)$ constructed above is huge as soon as G is small compared to S_n. A more effective way is to define **relative resolvents** for any pair of groups $G \leq H(\leq S_n)$. One can then descend from S_n to the correct Galois group one step at a time.
- The above version of resolvent gives a result only depending on whether the resolvent has or does not have a rational root. That's a bit of a waste, considering the large amount of possible factorizations of a polynomial. The following kind of resolvent gives a result depending on whether or not the resolvent is **irreducible**:

Linear resolvents

An important invariant is the linear polynomial $X_1 + \cdots + X_k \in \mathbb{Z}[X_1, \ldots, X_n]$.

Linear resolvents

For f of degree n with roots $\xi_1, \ldots, \xi_n$, and $1 \leq k \leq n-1$, define

$$\Theta_f(X) = \prod_{S \subset \{1,\ldots,n\}; |S|=k} (X - \sum_{i \in S} \xi_i).$$

Assuming $\Theta_f(X)$ is separable, the degrees of its irreducible factors over $\mathbb{Q}$ correspond 1-to-1 to the orbit lengths of $Gal(f)$ acting on k-subsets of $\{1, \cdots, n\}$! In particular, if $Gal(f)$ is k-fold transitive, then Θ_f must be irreducible.

(Recall: A transitive group $G \leq S_n$ is called 2-transitive if the stabilizer of 1 is transitive on $\{2, \ldots n\}$.

A 2-transitive group is 3-transitive, if the pointwise stabilizer of 1 and 2 is transitive on $\{3, \ldots, n\}$, etc.)

Example: A polynomial with Galois group $PSL_3(2) < S_7$

(The following example is taken from Cox, Galois Theory:)

Theorem

The polynomial $x^7 - 154x + 99$ has Galois group $PSL_3(2)$ over $\mathbb{Q}$.

Proof.

First, form the resolvent of degree $\binom{7}{3} = 35$ coming from action on 3-sets.

Galois group equals $PSL_3(2)$ if and only if this resolvent factors into two irreducibles of degrees 7 and 28 respectively.

Group-theoretical explanation: The action of $PSL_3(2)$ on 3-sets in $\{1, \ldots, 7\}$ is intransitive (this is because the image of $a + b \in \mathbb{F}_2^3$ under any element of $GL_3(2)$ is fixed with a and b), with an orbit of length 7 coming from the sets $\{a, b, a + b\}$. □

1. Local tools: Reduction and completion

2. Invariants of Galois groups

3. Galois groups in infinite families
   - Multi-parameter polynomials of fixed degree: function field methods
   - Families of polynomials of unbounded degree

4. Some recent developments

Function field methods

Bounding Galois groups from above via resolvents is often very tedious business.

In some cases, there are much nicer ways of finding upper bounds, coming from methods over function fields, such as **monodromy**.

Lemma

*Let $F(t,X) = f(X) - tg(X)$, with coprime polynomials $f, g \in \mathbb{Q}[X]$, and let $G = Gal(F/\mathbb{Q}(t))$. Then the degrees of the irreducible factors of $f(X)g(Y) - g(X)f(Y) \in \mathbb{Q}[X, Y]$ are exactly the lengths of the orbits of a point stabilizer in G. In particular, $Gal(F/K(t))$ is 2-**transitive** if and only if the polynomial $\frac{f(X)g(Y)-g(X)f(Y)}{X-Y} \in K[X, Y]$ is irreducible.*

Proof.

Let y be a root of F over $\mathbb{Q}(t)$. Then $t = \frac{f(y)}{g(y)}$, so over $\mathbb{Q}(y)$, we have $F = f(X) - \frac{f(y)}{g(y)}g(X)$. But $Gal(F/\mathbb{Q}(y))$ is exactly a point stabilizer in G. □

Example: A polynomial for the sporadic Higman-Sims group

- HS is a finite simple group with a primitive, but not 2-transitive permutation action of degree 100. This action extends to the automorphism group $Aut(HS) = HS \rtimes C_2$.
- The following polynomial with Galois group $Aut(HS) = HS \rtimes C_2$ over the field $\mathbb{Q}(t)$ was computed by Barth and Wenz (2016):

Theorem

Let $p(X) = (7X^5 - 30X^4 + 30X^3 + 40X^2 - 95X + 50)^4 \cdot (2X^{10} - 20X^9 + 90X^8 - 240X^7 + 435X^6 - 550X^5 + 425X^4 - 100X^3 - 175X^2 + 250X - 125)^4 \cdot (2X^{10} + 5X^8 - 40X^6 + 50X^4 - 50X^2 + 125)^4$, *and* $q(X) = (X^4 - 5)^5 \cdot (X^8 - 20X^6 + 60X^5 - 70X^4 + 100X^2 - 100X + 25)^{10}$. *Then* $f(t, X) = p(X) - tq(X)$ *has Galois group* $Aut(HS)$ *over* $\mathbb{Q}(t)$.

Proof.

$p(X)q(Y) - q(X)p(Y) = (X - Y)f_1(X, Y)f_2(X, Y) \in \mathbb{Q}[X, Y]$, with $\deg(f_1) = 22$ and $\deg(f_2) = 77$. Therefore $Gal(f)$ cannot be 2-transitive, i.e., cannot be S_{100} or A_{100}.
Now, only need to find cycle structures in $Gal(f)$ via Dedekind's criterion. One of them is $(11^9.1)$, which forces $Gal(f)$ to be primitive. Then, in the list of primitive groups of degree 100, $Aut(HS)$ is the only one with all those cycle structures. □

A variant of the above.

Lemma

Let $f(t,X) \in \mathbb{Q}(t)[X]$ be irreducible. Assume that there exists a non-constant rational function $g(Y) \in \mathbb{Q}(Y)$ of degree d such that $f(g(Y),X)$ is reducible over $\mathbb{Q}(Y)$, but does not possess a root. Then the splitting field of f over $\mathbb{Q}(t)$ contains a rational function field $\mathbb{Q}(y)$ of degree $[K(y):K(t)]$ dividing d, and whose Galois group is an intransitive subgroup of G.

This is often applicable nicely for detecting **linear** groups as Galois groups.

Theorem (K., 2014)

The polynomial $f(t,x) = (x^5 - 95x^4 - 110x^3 - 150x^2 - 75x - 3)^3(x^5 + 4x^4 - 38x^3 + 56x^2 + 53x - 4)^3(x-3) - t(x^2 - 6x - 1)^8(x^2 - x - 1)^4(x+2)^4 x$ *has Galois group $PSL_5(2)$ over $\mathbb{Q}(t)$.*

Proof.

That polynomial was computed as part of a family $F(\alpha, t, x)$ with an extra parameter α, already specialized above. Now among that family, there will be a second value α' for which the polynomial $F(\alpha', t, x) =: g(t, x)$ has exactly the same branch points as $f(t, x)$ (this reflects the fact that inside the splitting field of $f(t, x)$, there is a second, non-conjugate subfield with the same ramification structure!). Write $f(t, x) = f_1(x) - tf_2(x)$ and $g(t, x) = g_1(x) - tg_2(x)$, and factor the polynomial $f - 1(x)g_2(y) - f_2(x)g_1(y)$. This corresponds to the factorization of $f(t, x)$ over $\mathbb{Q}(y)$, where y is a root of g! The polynomial turns out to factor into degrees 15 and 16, corresponding to the fact that the second index-31 subgroup of $PSL_5(2)$ has orbit lengths 15 and 16 in the action of the cosets of the first index-31 subgroup.

Since no other degree-31 transitive group has such a behaviour, the Galois group must be $PSL_5(2)$! □

- As seen above, computation of the Galois group of one fixed polynomial is essentially an algorithmic problem.
- In particular, if a fixed degree-n polynomial has "large" Galois group (S_n or A_n), it will "give it away" rather easily (Dedekind's criterion, Chebotarev's theorem).
- Verifying the Galois group of an infinite family (of unbounded degree) of polynomials is a whole different matter.
- Even though such families "morally" (often) tend to have large Galois group, the strict verification can be very hard!
- In the following, we look at some examples where "local" methods help.

Truncated exponential series: A result by Schur

Theorem (Schur, 1930)

Let $f_n = 1 + x + \frac{x^2}{2} + ... + \frac{x^n}{n!}$ *(the n-th Taylor polynomial of the exponential function). Then* $Gal(f_n/\mathbb{Q}) = \begin{cases} A_n, & \text{if } 4|n \\ S_n, & \text{else} \end{cases}$.

Auxiliary results from group theory

Theorem (Jordan, 1870s)

Assume that $G \leq S_n$ is a primitive permutation group containing a p-cycle for some prime $p < n-2$. Then $G \in \{A_n, S_n\}$.
If additionally, $p > n/2$, then the assumption of primitivity can be weakened to transitivity.

Note: A **primitive** permutation group is a transitive group whose point stabilizer is a maximal subgroup. Equivalently, the action of G does not preserve a non-trivial **block system**.

Theorem (Chebyshev ("Bertrand's postulate"))

If $n \geq 8$, then there exists at least one prime number p with $n/2 < p < n-2$.

A modern proof of Schur's theorem

Due to Coleman (1987).

Due to above auxiliary results, it suffices to show the following:

a) f_n is irreducible.
b) $Gal(f_n)$ contains a p-cycle for some $n/2 < p < 2$.
c) $\Delta(f_n)$ is a square if and only if $4|n$.

Lemma

The slopes of the Newton polygon of f_n *are* $-\frac{p^{n_i}-1}{p^{n_i}(p-1)}$, *where* $n_1 > \cdots > n_s$ *are the exponents of* p *occurring in a* p*-adic expansion of* n. *In particular, if* $p^k \leq n$, *then* p^k *divides the degree of the splitting field of* f_n *over* $\mathbb{Q}_p$

□

- Now assertion b) follows immediately from Bertrand's postulate (plus the fact that any element of such order $p > n/2$ in S_n must be a p-cycle).
- Furthermore, from above Lemma it follows that if p^m divides n, then it also divides the order of **each** irreducible factor over $\mathbb{Q}_p$.
  In total, f_n must be irreducible over $\mathbb{Q}$.
- To conclude, it suffices to show the following

Lemma

$\Delta(f_n) = (-1)^{\frac{n(n-1)}{2}} \cdot (n!)^n$.

Generalized Laguerre polynomials

Definition

The polynomial $L_m^{\alpha}(x) = \sum_{j=0}^{m} \frac{(m+\alpha)(m+\alpha-1)\cdots(j+\alpha+1)\cdot(-x)^j}{(m-j)!j!}$ is called **generalized Laguerre polynomial**.

Interesting special cases

- $L_m^{(-m-1)}(x)$ is the truncated exponential series.
- $L_m^0(x) = \sum_{j=0}^{m} \begin{pmatrix} m \\ j \end{pmatrix} \frac{(-1)^j}{j!} x^j$ are the "classical" Laguerre polynomials.

Theorem (Schur)

$Gal(L_m^{(0)}(x)) = S_m$, for each $m \in \mathbb{N}$.
$Gal(L_m^{(1)}(x)) = A_m$ if $m > 1$ is odd or of the form $k^2 - 1$; and S_m otherwise.

Laguerre polynomials

Theorem (Gow, 1989)

If m is even such that $L_m^{(m)}$ is irreducible, then $Gal(L_m^{(m)}(x)) = A_m$.

(Filaseta/Williams: Most of them are actually irreducible.)

Generalized Fibonacci polynomials

Definition

The polynomial $f_n(X) := X^n - X^{n-1} - \cdots - X - 1$ is called **generalized Fibonacci polynomial** of degree n.

Reason for the naming: The generalized Fibonacci sequence is defined by the recursion $a_{n+k} = a_{n+k-1} + ... + a_n$. The ratio a_{k+1}/a_k of two subsequent elements of the series then converges to a root of the equation $x^k = x^{k-1} + \cdots + x + 1$.

Generalized Fibonacci polynomials

Theorem (Martin, 2004)

If n is even or a prime number, then $Gal(f_n/\mathbb{Q}) = S_n$.

Generalized Fibonacci polynomials

Some remarks about the proof:

- $f_n(x)$ has a real root between 1 and 2, and all other roots have absolute value < 1.
  Exercise: Then f_n must be irreducible.
- $f_n(x) \cdot (x-1) = x^{n+1} - 2x^n + 1$. This is useful, since discriminants of trinomials are easy to calculate.
- By considering some auxiliary polynomial, one finds that for every prime $p > 2$ dividing the discriminant, there is **only one** double root, and otherwise simple roots, for f mod p.

Generalized Fibonacci polynomials

- Now what does this mean for the inertia group I_p?
  - Either I_p is trivial (so p was actually unramified).
  - Or I_p is generated by a transposition!
- Now a transitive group of prime degree q with a transposition is S_q.
- If the degree is even, then one can show additionally that 2 does not divide the discriminant of f. So **all** the non-trivial inertia groups are generated by transpositions.
- **Fact**: The inertia groups generate the whole Galois group.
- And a transitive group generated by transpositions is also always the full symmetric group.

1. Local tools: Reduction and completion
2. Invariants of Galois groups
3. Galois groups in infinite families
   - Multi-parameter polynomials of fixed degree: function field methods
   - Families of polynomials of unbounded degree
4. Some recent developments

An idea by Elkies for determination of multiply transitive Galois groups

- There are known polynomials for the Galois group M_{23} (Mathieu group acting on 23 points), not over $\mathbb{Q}$, but over some small number fields.
  This group is 4-fold, but not 5-fold transitive.
- To strictly verify the Galois group, one could now use the intransitivity of the action on M_{23} on 5-sets, to distinguish it from A_{23}. This would boil down to the computation of a resolvent of degree $\binom{23}{5} = 33649$. That is, however, not practical!
- Instead, the following has been suggested (and applied successfully) by Noam Elkies:

Determination of multiply transitive Galois groups

- Assume given an irreducible degree-n equation $f(t,X) \in \mathbb{Q}[t,X]$, such that the cycle structures (in S_n) of the inertia group generators $\sigma_1, \dots, \sigma_r$ over $\mathbb{Q}(t)$ are known.
  (This is not a big assumption; the cycle structures can often be read of from factorizations of $f(t_0, X)$, where $t_0 \in \overline{\mathbb{Q}}$ is a branch point).
- Now in the splitting field $\Omega/\mathbb{Q}(t)$ of f, consider the fixed field E_k of the stabilizer of a k-**set** $(2 \leq k \leq n-2)$. This field has a certain **genus** - a group-theoretical invariant which can be computed from the cycle structure of the σ_i in the action on k-sets. If G is k-fold transitive, then these cycle structures, and therefore the genus of E_k can be estimated by rather simple combinatorial methods!

Determination of multiply transitive Galois groups

- Moreover, modulo "most" primes p, the mod-p reduction of E_k still retains the genus of E_k. From the **Hasse-Weil bound**, one can then estimate (from below and above) the number of degree-1-places ($=\mathbb{F}_p$-rational points) of E_k mod p.
- On the other hand, from the given equation $f(t, X)$, one can actually explicitly compute the number of such $\mathbb{F}_p$-rational points (without knowing an equation for E_k, just by factoring $f(t_0, X)$ for all $t_0 \in \mathbb{F}_p$.
- If that number contradicts what the Hasse-Weil bound would have predicted for the genus (under the assumption "G is k-transitive"), then obviously G wasn't k-transitive.
- In particular, since A_n and S_n are the only groups which are more than 5-transitive, this method is well-suited to rule out these groups as Galois groups!