Relative Invariants in Permutation Groups with Applications to Galois Theory

Mitchell Wadas

Consultant: Prof. Harm Derksen

Northeastern University

April 18, 2024

Outline

Polynomial Algebras

- Let K be an infinite field.
- The set of polynomials in $x_1, \cdots, x_n$ over K is denoted $K[X] = K[x_1, \cdots, x_n]$.
- $K[X]$ forms a commutative, $\mathbb{N}$-graded algebra over K with homogeneous pieces

$$K[X]_d = \{ \text{ homogeneous polynomials of degree } d \text{ } \} \cup \{0\}.$$

Linear Representations

- A linear representation is a group homomorphism $\rho : G \to \mathrm{GL}_n(K)$.
- This defines a G-action on K^n by $\sigma * v = \rho(\sigma)v$.
- We extend this action to $f \in K[X]$ by

$$\sigma * f(\mathbf{x}) = f(\sigma^{-1} * \mathbf{x}).$$

Example.

The *defining representation* of $G \leq S_n$ is given by

$$\rho(\sigma)(\mathbf{e}_i) = \mathbf{e}_{\sigma(i)}.$$

The induced action is equivalent to

$$\sigma * f(x_1, \cdots, x_n) = f\left(x_{\sigma(1)}, \cdots, x_{\sigma(n)}\right).$$

Invariants

Definition.

A polynomial $f \in K[X]$ is G-invariant if $\sigma * f = f$ for all $\sigma \in G$.

Remark.

The G-invariant polynomials form a subalgebra, which we denote $K[X]^G$.

Definition.

If H is a subgroup of G, then we say f is a G-relative H-invariant if

$$\mathrm{Stab}_G(f) = H.$$

The Galois Group

- Let $p \in K[x]$ be a separable polynomial with splitting field N over K.
- $\mathrm{Gal}(N/K)$ is the set of automorphisms of N which leave K fixed.
- $\mathrm{Gal}(N/K)$ acts on the set R of roots of p by $\gamma * r = \gamma(r)$.

Definition.

The action induces an injective homomorphism from $\mathrm{Gal}(N/K)$ into $\mathrm{Sym}(R)$.

The Galois group of p is the image of $\mathrm{Gal}(N/K)$ under this homomorphism.

Stauduhar's Method

Stauduhar's Method

Theorem 1.

Let $H < G \leq S_n$, and assume $\mathrm{Gal}(p) \leq G$. Let f be a G-relative H-invariant such that, for all $\sigma \in G \setminus H$,

$$\sigma * f(r_1, \cdots, r_n) \neq f(r_1, \cdots, r_n). \tag{1}$$

For all σ in G, $\mathrm{Gal}(p) \leq \sigma H \sigma^{-1}$ if and only if $\sigma * f(r_1, \cdots, r_n) \in K$.

Remark.

If (1) does not hold, we can apply a transformation to obtain a new polynomial with the same Galois group as p, whose roots do satisfy (1).

Stauduhar's Method

Algorithm (Stauduhar's Method).

To compute the Galois group of a separable polynomial of degree n,

- Set $G = S_n$.
- Choose a maximal subgroup H and compute a G-relative H-invariant.
- Apply theorem 1 to find a conjugate subgroup $\sigma H \sigma^{-1}$ containing $\mathrm{Gal}(p)$.
- Set $G = \sigma H \sigma^{-1}$, and repeat until $\mathrm{Gal}(p)$ is not contained in any proper subgroup of G.

Generic Invariants

The Reynolds Operator

Definition.

Let G be a finite group with subgroup H. The relative Reynolds operator is defined as the map

$$\mathcal{R}_{G/H} : K[X]^H \to K[X]^G, \quad f \mapsto \frac{1}{|G:H|} \sum_{\sigma H \in G/H} \sigma * f.$$

When $H = \{e\}$, we call this map the Reynolds operator, denoted $\mathcal{R}_G$.

Proposition.

- The relative Reynolds operator is a graded linear transformation.
- The relative Reynolds operator is a projection.

The Reynolds Operator

Consider the restriction of $\mathcal{R}_{G/H}$ to the finite dimensional subspace $K[X]_d^H$:

$$\mathcal{R}_{G/H,d} : K[X]_d^H \to K[X]_d^G.$$

Proposition.

Let H be a maximal proper subgroup of G.

If f is a non-zero element of $\ker \mathcal{R}_{G/H,d}$, then f is a relative invariant.

Method 1

Method 1.

To compute a G-relative H-invariant,

- Choose a degree d so that the kernel of $\mathcal{R}_{G/H,d}$ is non-trivial.
- Compute a basis B for $K[X]_d^H$.
- Construct the matrix of $\mathcal{R}_{G/H,d}$ in this basis.
- Find the kernel by solving a system of linear equations over K.
- Choose any non-zero element in the kernel.

Method 2

Let S be a set of non-identity cosets representatives of G/H.

Define the map

$$\psi : K[X]^H \to \bigoplus_{i=1}^{|S|} K[X], \quad f \mapsto (\sigma * f - f)_{\sigma \in S}.$$

Proposition.

- The map ψ is K-linear.
- If B is a basis for $K[X]_d^H$, then $\psi(B)$ is a spanning set for $\psi(K[X]_d^H)$.

Method 2

Proposition.

Let H be a maximal proper subgroup of G.

If $\psi(f) \neq 0$, then f is a G-relative H-invariant.

Method 2.

To compute a G-relative H-invariant,

- Choose an appropriate degree d.
- Compute a basis for $K[X]_d^H$.
- Apply ψ to each basis element.
- Any element which is not mapped to zero is a relative invariant.

The Hilbert Series

Definition.

Let M be a non-negatively graded vector space of finite type. We define the Hilbert series of M to be the formal power series

$$H(M, t) = \sum_{d=0}^{\infty} \dim(M_d) t^d.$$

Remark.

A formal power series is an algebraic expression, independent of any notion of convergence.

Molien's Formula

Theorem (Molien's Formula).

Let $\rho : G \to \mathrm{GL}(n, K)$ be a representation of a finite group G acting on $K[X]$. The Hilbert series of the invariant algebra is given by

$$H(K[X]^G, t) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - \rho(g)t)}.$$

Applications

Proposition.

The Reynolds operator is a projection *onto* $K[X]_d^G$, so we obtain

$$K[X]_d^H = K[X]_d^G \oplus \ker \mathcal{R}_{G/H,d}.$$

Therefore, the Hilbert series of $K[X]^H$ splits into

$$H(K[X]^H, t) = H(K[X]^G, t) + H(\ker \mathcal{R}_{G/H}, t).$$

We can use this fact to determine the minimal degree of a relative invariant.

Computing a Basis

Proposition.

If B is a basis for $K[X]_d^H$, then the image $\mathcal{R}_{G/H,d}(B)$ spans $K[X]_d^G$.

Algorithm.

To compute a basis for $K[X]_d^G$,

- Apply $\mathcal{R}_G$ to a monomial basis for $K[X]_d$ to obtain a spanning set.
- Refine the spanning set to a basis.

This requires us to apply $\mathcal{R}_G$ to each of the $\binom{n+d-1}{d}$ basis elements.

Each application requires $|G|$ actions.

Computing a Basis

A Better Method.

- Form a chain of groups $\{e\} = H_1 < H_2 < \cdots < H_K = G$.
- Then compute $\mathcal{R}_G = \mathcal{R}_{H_K/H_{k-1}} \circ \cdots \circ \mathcal{R}_{H_2/H_1}$.

The total number of operations is $\sum [H_i : H_{i-1}] \ll \prod [H_i : H_{i-1}] = |G|$.

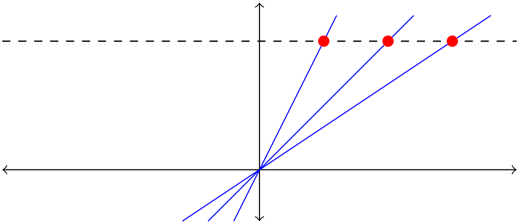
We can refine the spanning set to a basis at each step.

Special Invariants

Projective Space

Definition.

- Given a vector space V over K, the projective space $\mathbb{P}(V)$ is the set of all 1 dimensional subspaces.
- When $\dim V = 2$, we call the projective space a projective line.



The Projective Semi-Linear Group

The invertible linear transformations of V induce permutations $\mathbb{P}(V)$ by

$$g * W = g(W) = \{g(w) : w \in W\}.$$

Definition.

The permutations induced by $\mathrm{GL}(V)$ form the projective linear group $\mathrm{PGL}(V)$.

Definition.

We extend PGL to include the induced action of invertible semi-linear maps by defining the projective semi-linear group

$$\mathrm{P\Gamma L}(V) = \mathrm{PGL}(V) \rtimes \mathrm{Aut}(K).$$

When $V = \mathbb{F}_q^n$, the notation $\mathrm{PGL}(n, q)$ and $\mathrm{P\Gamma L}(n, q)$ is used.

The Particular Case

- We are interested in $\mathrm{PGL}(2,25) \lhd \mathrm{P\Gamma L}(2,25) \leq S_{26}$.
- This is a difficult case where most existing methods do not apply.

Observations.

- $\mathrm{PGL}(2,25)$ acts sharply 3-transitively on $\mathbb{P}(\mathbb{F}_{25}^2)$.
- $\mathrm{Aut}\left(\mathbb{F}_{25}\right)$ is cyclic of order 2 and generated by the Frobenius automorphism:

$$\varphi : \mathbb{F}_{25} \to \mathbb{F}_{25}, \quad x \mapsto x^5.$$

- $\mathrm{P\Gamma L}(2,25)$ consists of $\mathrm{PGL}(2,25)$ and the left coset $\varphi\,\mathrm{PGL}(2,25)$.
- If x is in the prime subfield $\mathbb{F}_5$, then $\varphi(x) = x$. Otherwise, $\varphi(x) \neq x$.

The Cross Ratio

Definition.

For points A, B, C, D on the projective line, the cross ratio is the point $[A, B; C, D] = h(D)$, where h is the unique map sending (A, B, C) to $(\infty, 0, 1)$.

Proposition.

The cross ratio is invariant under the action of $\mathrm{PGL}(V)$.

Observation.

If we choose A, B, C, D so that $[A, B; C, D]$ lies in $\mathbb{F}_{25} \setminus \mathbb{F}_5$, then

$$\mathrm{Stab}_{\mathrm{P\Gamma L}}[A, B; C, D] = \mathrm{PGL}\,.$$

Special Methods

Special Invariant

Choose a value $\lambda \in \mathbb{F}_{25} \setminus \mathbb{F}_5$ and form the sum

$$\sum_{[A,B;C,D]=\lambda} x_A^1 x_B^2 x_C^3 x_D^4 \in K[X].$$

Permutations in $\mathrm{PGL}(2,25)$ will permute the order of the sum.
Permutations in $\mathrm{P\Gamma L} \setminus \mathrm{PGL}$ will send (A,B,C,D) to some tuple not in the sum.

Results

We summarize the computational cost of relative invariants for the pair $\mathrm{PGL}(2,25) \lhd \mathrm{P\Gamma L}(2,25)$ in the table below.

Method	Degree	Products
Benchmark	4	14675
Method 1	4	23400
Method 2	4	11700
Special Method	10	46800

"Benchmark" refers to the generic method of Fieker and Klüners [3].

Future Work

- For carefully chosen λ, the cross ratio is invariant under even permutations of $\{A, B, C, D\}$. We hope to use this symmetry to simplify the special invariant constructed.
- Extend the special method to other pairs, say $\mathrm{PGL}(\mathbb{F}_{p^n}^2) \leq \mathrm{P\Gamma L}(\mathbb{F}_{p^n}^2)$.
- Analyze the computational complexity of the algorithms.
- Apply the generic methods to other pairs.

References

[1] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Vol. 130. Encyclopedia of Mathematical Sciences. Springer, Heidelberg, 2015, pp. xxii+366. ISBN: 978-3-642-07796-8.

[2] Andreas-Stephan Elsenhans. "Improved methods for the construction of relative invariants for permutation groups". In: *Journal of Symbolic Computation* 79 (2017), pp. 211–231.

[3] Claus Fieker and Jürgen Klüners. "Computation of Galois groups of rational polynomials". In: *LMS Journal of Computation and Mathematics* 17.1 (2014), pp. 141–158.

[4] Jean Gallier. *Geometric methods and applications*. Vol. 38. Texts in Applied Mathematics. Springer, New York, NY, 2011, pp. xxviii+680. ISBN: 978-1-4419-9960-3.

[5] K. W. Gruenberg and A. J. Weir. *Linear geometry*. Vol. 49. Graduate Texts in Mathematics. Springer, New York, NY, 1977, pp. x+199. ISBN: 978-0-387-90227-2.

[6] Mara D. Neusel. *Invariant Theory*. Vol. 36. Student Mathematical Library. American Mathematical Society, Providence, RI, 2015, pp. viii+314. ISBN: 978-0-8218-4132-7.

[7] Richard P. Stauduhar. "The determination of Galois groups". In: *Mathematics of Computation* 27 (1973), pp. 981–996.