The symmetric group and its action on a ring of multivariate polynomials – with applications to Galois theory

Christian Roettger
Joint work with John Gillespie

380 Carver Hall
Mathematics Department
Iowa State University
https://math.iastate.edu/directory/christian~roettger/

September 9, 2023

Action of the symmetric group on multivariate polynomials I

Let $\mathbb{S}$ be the ring of polynomials in n variables $x_1, \ldots, x_n$ over a ground field K. The symmetric group $G = \mathrm{Sym}(n)$ acts on $\mathbb{S}$ in the natural way. For any subgroup U of G, the polynomials invariant under U form a subring Fix_U. Let $\mathbb{B} = Fix_G$ be the subring of *symmetric polynomials* invariant under all permutations in G. It is well-known that

$$\mathbb{B} = K[e_1, \ldots, e_n]$$

This is a polynomial ring in the *elementary symmetric functions* $e_1, \ldots, e_n$ defined by

$$(x - x_1)(x - x_2) \ldots (x - x_n) = x^n - e_1 x^{n-1} \pm \ldots (-1)^n e_n.$$

Clearly, $\mathbb{S}$ is a $\mathbb{B}$-module.

Action of the symmetric group on multivariate polynomials II

Theorem

$\mathbb{S}$ is a free $\mathbb{B}$-module of rank $n!$. The set of monomials

$$B = \{x_1^{d_1} \cdot \dots \cdot x_n^{d_n} | d_i \leq n - i, i = 1, \dots, n\}$$

is a $\mathbb{B}$-basis of $\mathbb{S}$.

Group ring structure

Definition

The action of G on the ring $\mathbb{S}$ is compatible with the $\mathbb{B}$-module structure:

$$g \cdot (bs) = b(g \cdot s)$$

for all $g \in G$, $b \in \mathbb{B}$, $s \in \mathbb{S}$. So $\mathbb{S}$ is a module over the group ring $\mathbb{B}[G]$, which is the free $\mathbb{B}$-module over the formal basis G, extending the multiplication in G via the distributive law. So both $\mathbb{S}$ and $\mathbb{B}[G]$ are free $\mathbb{B}$-modules of rank n!!

Conjecture $\mathbb{S}$ and $\mathbb{B}[G]$ are isomorphic as $\mathbb{B}[G]$-modules.

Group ring structure

Definition

The action of G on the ring $\mathbb{S}$ is compatible with the $\mathbb{B}$-module structure:

$$g \cdot (bs) = b(g \cdot s)$$

for all $g \in G$, $b \in \mathbb{B}$, $s \in \mathbb{S}$. So $\mathbb{S}$ is a module over the group ring $\mathbb{B}[G]$, which is the free $\mathbb{B}$-module over the formal basis G, extending the multiplication in G via the distributive law. So both $\mathbb{S}$ and $\mathbb{B}[G]$ are free $\mathbb{B}$-modules of rank n!!

Conjecture $\mathbb{S}$ and $\mathbb{B}[G]$ are isomorphic as $\mathbb{B}[G]$-modules.
Exercise for the reader Find two proofs why they are NOT isomorphic as rings for $n \geq 2$.

Group Algebra structure I

Here is some evidence for the conjecture.
Let $\bar{\mathbb{S}}$, $\bar{\mathbb{B}}$ be the fields of fractions of $\mathbb{S}$ and $\mathbb{B}$ respectively.

Theorem

As $\bar{\mathbb{B}}[G]$-module, $\bar{\mathbb{S}}$ is isomorphic to $\bar{\mathbb{B}}[G]$.

Proof.

The set of $n!$ monomials

$$C = \left\{ g \cdot \prod_{I=1}^{n} x_i^i | g \in G \right\}$$

is linearly independent over $\bar{\mathbb{B}}$. Look at a $\bar{\mathbb{B}}$-linear combination. Without loss of generality, the coefficients can be assumed to be in $\mathbb{B}$. Split the coefficients up into their homogeneous components which are still symmetric. □

Group Algebra structure II

We (think that we) can prove the conjecture with explicit computations for $n = 3$.
Exercise for the reader Could it be that the set C of monomials even generates $\mathbb{S}$ as a $\mathbb{B}$-module?

Take a polynomial $f(x)$ over K, with distinct roots $\alpha_1, \ldots \alpha_n$ generating the splitting field L/K. Then L/K is a Galois extension with a group U which embeds into G via its permutations of the roots. The evaluation $x_1 \mapsto \alpha_1, x_2 \mapsto \alpha_2, \ldots$ provides a surjective ring homomorphism from $\mathbb{S}$ to L, and the preimage of K is Fix_U. Finding generators of Fix_U could give general formulas for determining whether a given polynomial f has a Galois group that is contained in U or not.
Here is how the Conjecture would help with determining Fix_U.

Corollary

If the Conjecture is true, then Fix_U is a free $\mathbb{B}$-module of rank $[G : U]$.

Proof.

Let ε be the idempotent associated to the trivial representation of U,

$$\varepsilon = \frac{1}{|U|} \sum_{u \in U} u.$$

It is easy to see that Fix_U is the image of $\mathbb{S}$ under the $\mathbb{B}[U]$-homomorphism

$$h : s \mapsto \varepsilon \cdot s.$$

Now we study the same multiplication by ε operating on $\mathbb{B}[G]$. The image of $\mathbb{B}[G]$ under this map is a free $\mathbb{B}$-module of rank $[G : U]$ (any system of coset representatives of $U \backslash G$ is a basis). Given the conjecture, we conclude the same for the image of the original map h. □

More Galois Theory I

Another consequence is the well-known theorem

Theorem

Let f be polynomial f of degree n over K, with distinct roots $\alpha_1, \ldots \alpha_n$ generating a Galois extension L/K. Define the discriminant $\bar{D}$ of f as

$$\bar{D} = \prod_{i<j} (\alpha_i - \alpha_j)$$

The Galois group of f, viewed as subgroup of $Sym(n)$, is contained in the alternating group $Alt(n)$ iff the discriminant $\bar{D}$ of f is a square in K.

This could be proven using the preimage D of $\bar{D}$ in $\mathbb{S}$,

$$D = \prod_{i<j} (x_i - x_j)$$

More Galois Theory II

It is not hard to show that $Fix_{\mathrm{Alt}(n)} = \mathbb{B}[D]$ (note that D^2 is symmetric, hence in $D^2 \in Fix_{\mathrm{Sym}(n)} = \mathbb{B}$).

Conclusion

Open questions – Conjecture for $n > 3$, algorithm for computing generators of Fix_U... ...

Thank you! Questions??