Rose-Hulman Undergraduate Mathematics Journal

Volume 13
Issue 1

Article 4

Invariants of Finite Groups Acting as Flag Automorphisms

Dennis Tseng
Massachusetts Institute of Technology, dennisctseng@gmail.com

Rose-Hulman Undergraduate Mathematics Journal

Invariants of finite groups acting as flag automorphisms

Dennis Tseng[a]

Volume 13, No. 1, Spring 2012

Sponsored by

Rose-Hulman Institute of Technology
Department of Mathematics
Terre Haute, IN 47803
Email: mathjournal@rose-hulman.edu
http://www.rose-hulman.edu/mathjournal

[a]Massachusetts Institute of Technology

Rose-Hulman Undergraduate Mathematics Journal
Volume 13, No. 1, Spring 2012

Invariants of finite groups acting as flag automorphisms

Dennis Tseng

Abstract. Let K be a field and suppose that G is a finite group that acts faithfully on $K(x_1, \ldots, x_m)$ by automorphisms of the form $g(x_i) = a_i(g)x_i + b_i(g)$, where $a_i(g), b_i(g) \in K(x_1, \ldots, x_{i-1})$ for all $g \in G$ and all $i = 1, \ldots, m$. As shown by Miyata, the fixed field $K(x_1, \ldots, x_m)^G$ is purely transcendental over K and admits a transcendence basis $\{\phi_1, \ldots, \phi_m\}$, where ϕ_i is in $K(x_1, \ldots, x_{i-1})[x_i]^G$ and has minimal positive degree d_i in x_i. We determine exactly the degree d_i of each invariant ϕ_i as a polynomial in x_i and show the relation $d_1 \cdots d_m = |G|$. As an application, we compute a generic polynomial for the dihedral group D_8 of order 16 in characteristic 2.

Acknowledgements: This research was conducted at Louisiana State University as part of the Research Experience for Undergraduates Program funded by National Science Foundation grant DMS-0648064. The author would like to thank Dr. Jorge Morales for his guidance.

1 Introduction

Let K be a field and G be a subgroup of the symmetric group S_n. The group G acts naturally by permutation of the indeterminates on the field of rational functions $K(x_1, x_2, \ldots, x_n)$. E. Noether asked in 1971 [9] whether the field of invariants $K(x_1, x_2, \ldots, x_n)^G$ is purely transcendental over K, that is, whether it can be generated over K by exactly n invariant functions $\xi_1, \xi_2, \ldots, \xi_n$. If G is the full symmetric group S_n, it is a classical theorem that $K(x_1, \ldots, x_n)^G$ is generated by the n elementary symmetric polynomials. Noether noted that if $\mathbb{Q}(x_1, \ldots, x_n)^G$ is purely transcendental, then G is realizable as a Galois group over $\mathbb{Q}$ by the Hilbert Irreducibility Theorem. It is still an open question whether every finite group is a Galois group over $\mathbb{Q}$.

Noether's question turned out to be very difficult, even for "easy" groups. The first counterexample was given by Swan [10] for $G = C_{47}$, the cyclic group of order 47. More recently, Lenstra [7] settled the question for all abelian groups over $\mathbb{Q}$. He showed in particular that $\mathbb{Q}(x_1, x_2, \ldots, x_8)^{C_8}$ is not purely transcendental.

We can consider more generally a finite matrix subgroup $G \subset GL_n(K)$ acting linearly in the indeterminants of $K(x_1, x_2, \ldots, x_n)$ and ask whether $K(x_1, x_2, \ldots, x_n)^G$ is purely transcendental. This is known as the Linear Noether Problem. If G acts linearly on $K(x_1, \ldots, x_n)$ and $K(x_1, \ldots, x_n)^G$ is purely transcendental over K, then, as described by Kemper [5], there exists a generic polynomial that parameterizes all Galois extensions with Galois group G. We will explore this connection in the last section with an statement of Kemper's result and an example.

Kuniyoshi [6] proved that if G is a $p-$group acting on $K(x_1, \ldots, x_{|G|})$ by the regular representation and K has characteristic p, then K^G is purely transcendental over K, and Gaschütz generalized this result to arbitrary representations [2]. Miyata generalized this to triangular automorphisms acting on a field of arbitrary characteristic and possibly infinite order [8].

Our starting point is a result if Miyata [8, Lemma 1]. We give below a slightly reformulated statement. In particular, we will only need the result for G of finite order.

Proposition 1.1 (Miyata)**.** *Let L be a field and let G be a finite group of automorphisms of $L(x)$ such that G preserves L and $g(x) = a(g)x + b(g)$, where $a(g), b(g) \in L$ for all $g \in G$. Then for any invariant $\phi \in L[x]$ of minimal positive degree in x, $L(x)^G = L^G(\phi)$.*

This result implies in particular that if G is a group of $m \times m$ upper triangular matrices acting linearly on $K(x_1, \ldots, x_m)$, then $K(x_1, \ldots, x_m)^G$ is purely transcendental over K. To see this, we let $L = K(x_1, \ldots, x_{m-1})$ and $x = x_m$ in Proposition 1.1. Then for any polynomial $\phi_m \in K(x_1, \ldots, x_{m-1})[x_m]$ of minimal positive degree in x_m we have $K(x_1, \ldots, x_m)^G = K(x_1, \ldots, x_{m-1})^G(\phi_m)$. We start over with $K(x_1, \ldots, x_{m-1})$ to find ϕ_{m-1} and so on. Constructing one invariant at a time according to this process, we get a transcendence basis $\phi_1, \ldots, \phi_m$ for $K(x_1, \ldots, x_m)^G$.

Our main result (Proposition 3.1 and Corollary 3.5) is the exact determination for all i of the minimal positive degree d_i in the variable x_i occurring in the subring $(K(x_1, \ldots, x_{i-1})[x_i])^G$.

It follows from the above procedure that any set of invariants $\{\phi_1, \ldots, \phi_m\}$, with $\phi_i \in K(x_1, \ldots, x_{i-1})[x_i]$ of degree d_i in x_i, is a transcendence basis for $K(x_1, \ldots, x_m)^G$.

Although Proposition 3.1 can be deduced from the work of Hajja and Kang [3, Theorem 1], our proof is more elementary in that it requires nothing beyond the formula $[E : E^G] = |G|$ for a finite group G acting faithfully on a field E. We present some corollaries to this result and give an application to finding a generic polynomial for the dihedral group D_8 of order 16 in characteristic 2.

In Section 2, we recall some necessary background and present some conditions that are equivalent to the hypotheses given in Proposition 1.1. We present our main result and proof in Section 3 and an example of its application to the construction of generic polynomials in Section 4.

2 Preliminaries

2.1 Definitions

If L is a field containing K, then we say that L is an extension of the field K, denoted L/K. We define $x_1, x_2, \ldots, x_n \in L$ to be algebraically independent over K if they do not satisfy a nontrivial polynomial equation with coefficients in K. The set $\{x_1, \ldots, x_n\} \subset L$ is a transcendence basis for the extension L/K if $K(x_1, \ldots, x_n) = L$ and $x_1, \ldots, x_n$ are algebraically independent. Recall that we can view L as a vector space over K. We let $[L : K]$ be the dimension of this vector space.

A automorphism of a field K is a bijection $\phi : K \to K$ such that $\phi(k_1 + k_2) = \phi(k_1) + \phi(k_2)$ and $\phi(k_1 k_2) = \phi(k_1)\phi(k_2)$. We denote the automorphisms of K as $\mathrm{Aut}(K)$. The automorphisms $\mathrm{Aut}(K)$ form a group, where multiplication is composition of automorphisms. Also, given a field extension L/K, we denote $\mathrm{Aut}(L/K)$ as the subgroup of $\mathrm{Aut}(L)$ that act as the identity when restricted to K.

If L/K is a field extension, then in general $|\mathrm{Aut}(L/K)| \leq [L : K]$. If equality holds, then we say the extension is Galois and $\mathrm{Aut}(L/K)$ is the Galois group $\mathrm{Gal}(L/K)$. Given a field K and a polynomial f with coefficients in K, we call L a splitting field for f if f factors completely into linear factors in $L[x]$ but not over any proper subfield of L containing K. The polynomial f is called separable if it has no repeated roots in its splitting field. A field extension L/K is Galois if and only if it is the splitting field of a separable polynomial over K, see for example Theorem 13, Section 14.2 [1]. The Galois group of a separable polynomial over K is the Galois group of its splitting field over K.

Given a group G of automorphisms of a field L, we define the fixed field L^G of L under the action of G to be $\{\alpha \in L : g(\alpha) = \alpha \ \forall g \in G\}$. Given a subfield $K \subset L$, we say that G preserves K if $g(k) \in K$ for all $k \in K$.

2.2 Equivalent Conditions for Proposition 1.1

We begin by giving conditions equivalent to the condition in Proposition 1.1.

Proposition 2.1. *Let L be a field and suppose that G is a finite group of automorphisms of $L(x)$ that preserves L. Then, the following conditions are equivalent.*

1. *G preserves the polynomial ring $L[x]$.*
2. *$\mathrm{Frac}(L[x]^G) = L(x)^G$ and $L^G \subsetneqq L(x)^G$.*
3. *$L^G \subsetneqq L[x]^G$.*
4. *$g(x) = a(g)x + b(g)$ for all $g \in G$,where $a(g), b(g) \in L$.*
5. *$L[x]^G = L^G[\phi]$, where ϕ has positive degree in x. In particular, ϕ needs to be of minimal degree in x for this to hold.*

Proof. We prove the implications (1) $\implies$ (2) $\implies$ (3) $\implies$ (4) $\implies$ (1) and (4) $\implies$ (5) $\implies$ (3).

(1) $\implies$ (2). The polynomial $\prod_{g\in G} g(x)$ has positive degree and is invariant so it is in $L(x)^G \setminus L^G$. It remains to show that $\mathrm{Frac}(L[x]^G) = L(x)^G$. Let $A/B \in L(x)^G$, with $A, B \in L[x]$. Let $B' = \prod_{g\in G} g(B)$ and let $A' = A\prod_{g\in G\setminus\{1\}} g(B)$. Clearly B' is in $L[x]^G$, and so is A' since $A' = (A/B)B'$. It follows that $A/B = A'/B'$ is in $\mathrm{Frac}(L[x]^G)$.

(2) $\implies$ (3). The ring $L[x]^G$ contains polynomials of positive degree, otherwise its fraction field would be L^G, contrary to the hypothesis.

(3) $\implies$ (4). Let $\phi = c_0 + c_1x + \cdots + c_dx^d$, where $c_0, \ldots, c_d \in L$, be a G-invariant polynomial of positive degree d and let $g \in G$. Since g is an automorphism of $L(x)$, the element $g(x)$ generates $L(x)$ over L, so it is of the form $g(x) = \frac{ax+b}{cx+d}$ with $a, b, c, d \in L$. By the invariance of ϕ we have

$$c_0 + c_1x + \cdots + c_dx^d = g(c_0) + g(c_1)\frac{ax+b}{cx+d} + \cdots + g(c_d)\left(\frac{ax+b}{cx+d}\right)^d,$$

and clearing denominators we get

$$(c_0+c_1x+\cdots+c_dx^d)(cx+d)^d = g(c_0)(cx+d)^d+g(c_1)(cx+d)^{d-1}(ax+b)+\cdots+g(c_d)(ax+b)^d.$$

Since the degrees on both sides of the equality above must match, we have $c = 0$, and hence (4) is true.

(4) $\implies$ (1). Obvious.

(4) $\implies$ (5). Let ϕ in $L[x]^G$ be of minimal positive degree and let $p \in L[x]^G$. Following Miyata [8], we apply Euclidean division to write $p = m\phi + r$, with $\deg(r) < \deg(\phi)$. Since p and ϕ are invariants, applying $g \in G$ yields $p = g(m)\phi + g(r)$ and by the uniqueness of the quotient and the remainder in the Euclidean algorithm we conclude $g(m) = m$ and $g(r) = r$, that is m and r are G-invariant.

By the minimality of the degree of ϕ, the remainder r must be constant in x, that is $r \in L^G$. If the quotient m is not constant in x, we can repeat this process on m. Eventually, we see that we can express p as a polynomial in ϕ.

(5) $\implies$ (3). Clearly ϕ is in $L[x]^G$ but not in L^G, so (3) is satisfied.

□

Remark. We note that if any of the equivalent conditions in Proposition 2.1 is satisfied, then $L(x)^G = \text{Frac}(L[x]^G) = \text{Frac}(L^G[\phi]) = L^G(\phi)$. Thus Proposition 2.1 implies immediately Proposition 1.1.

3 The degree of the invariant $\phi \in L[x]^G$

Unless otherwise mentioned, we will assume in this section that G acts on $L(x)$ faithfully by automorphisms, where G preserves L and $g(x) = a(g)x + b(g)$ with $a(g), b(g) \in L$. Throughout this section, we shall denote by H the subgroup of G that fixes L. In other words, H contains all the elements of G that act as the identity when restricted to L.

Proposition 3.1. *If G is finite, then the minimal positive degree occurring in $L[x]^G$ is equal to $|H|$.*

Proof. The proof will follow immediately from Lemmas 3.2 and 3.3 below. □

For the result below, we do not assume that G is finite.

Lemma 3.2. *If $\phi \in L[x]^G$ is of positive degree in x, then the degree of ϕ in x is at least $|H|$. Also, if H is infinite, then there does not exist $\phi \in L[x]^G$ of positive degree in x.*

Proof. Let $\phi = a_0 + a_1x + \cdots + a_dx^d$ be a polynomial of positive degree in $L[x]^G$. Consider the polynomial $P \in L(x)[Y]$ that is formed by substituting Y in ϕ for x, so that $P = a_0 + a_1Y + \cdots + a_dY^d$. Note that even though P is an element of $L(x)[Y]$, none of its coefficients has the variable x. Also, the degree of P in Y is equal to the degree of ϕ in x.

Consider $P - \phi$ as a polynomial in Y. Since the coefficients a_i are H-invariant, the polynomial $P - \phi$ vanishes when we substitute $Y = h(x)$ for all $h \in H$, so $P - \phi$ is divisible by $Y - h(x)$ in $L(x)[Y]$. Therefore, if H is finite, the polynomial

$$\prod_{h \in H} (Y - h(x))$$

divides $P - \phi$, and therefore ϕ has degree at least $|H|$. If H is infinite, then $P - \phi$ has infinitely many roots, which means $P - \phi = 0$. This can only happen if $\deg_x(\phi) = \deg_Y(P) = 0$. □

We next see that when G is finite, this lower bound is tight.

Lemma 3.3. *If G is finite, then the minimal positive degree occurring in $L[x]^G$ is at most $|H|$.*

Proof. Note that H is normal in G, so the quotient group G/H is defined. The action of G on L induces faithful action of G/H on L so we have the equality $[L : L^G] = [G : H]$. Let B be a basis B for L as a vector space over L^G. Note that B has cardinality $[G : H]$.

Let $\phi \in L[x]^G$ be a polynomial of minimal positive degree and let $d = \deg(\phi)$. Let Bx^i be the set obtained by multiplying every element in B by x^i. We claim that the set $B \cup Bx \cup \cdots \cup Bx^{d-1}$ is linearly independent over $L(x)^G$. Indeed, suppose that we have a linear combination

$$\sum_i a_i b_i = 0, \tag{1}$$

where $a_i \in L(x)^G$ and $b_i \in B \cup Bx \cup \cdots \cup Bx^{d-1}$ are distinct elements. By Proposition 1.1, we can view the a_i as rational functions in ϕ with coefficients in L^G. Clearing out the denominators in (1) we can assume without loss of generality that the a_i are polynomials in ϕ with coefficients in L^G. Write $a_i = \sum_j \alpha_{ij}\phi^j$ with $\alpha_{ij} \in L^G$. We express (1) in the form

$$c_0 + c_1\phi + \cdots + c_l\phi^l = 0, \tag{2}$$

where $c_k = \sum_i \alpha_{ik} b_i$.

If $c_l \neq 0$, then the degree in x of $c_l\phi^l$ is at least dl. No other term can cancel out a power of x with this degree as the maximal degree of $c_j\phi^j$ in x is $dj + (d-1) < dl$ for $j < l$. Therefore, $c_l = 0$. Similarly, $c_{l-1} = c_{l-2} = \cdots = c_0 = 0$.

Since x is transcendental over L and B is linearly independent over L^G, the set $B \cup Bx \cup \cdots \cup Bx^{d-1}$ is linearly independent over L^G. Thus $\alpha_{ik} = 0$ for all i, k, which proves the claim.

Therefore, we have found $[G : H]d$ elements in $L(x)$ that are linearly independent over $L(x)^G = L^G(\phi)$. Since $[L(x) : L(x)^G] = |G|$, we have $[G : H]d \leq |G|$. Hence $d \leq |H|$ as desired. □

Corollary 3.4. *Suppose G is finite. Let $\phi \in L[x]^G$ of minimal positive degree in x. Then, ϕ is expressible in the form*

$$\phi = a\left(\prod_{g \in H} g(x)\right) + b,$$

where $a, b \in L$.

Proof. Let P be the polynomial defined in the proof of Lemma 3.2. We know that $P - \phi$ is divisible by

$$\prod_{g \in H} (Y - g(x)).$$

Since $P - \phi$ has degree $|H|$ in Y from Lemma 3.3,

$$P - \phi = a \prod_{g \in H} (Y - g(x))$$

for some $a \in L$. We set $Y = 0$ on both sides to get

$$b - \phi = a \prod_{g \in H} (-g(x)),$$

where $b = P(0)$ is the constant term of P. Replacing a by $(-1)^{|H|}a$, we get the announced expression.

□

Corollary 3.5. *Let G be a finite group of $m \times m$ upper triangular matrices with coefficients in K. We let G act on $K(x_1, \ldots, x_m)$ by $g(x_i) = \sum_{i=1}^{m} a_{ij}x_j$ for $g = (a_{ij}) \in G$. Let d_i be the minimal positive degree in the variable x_i occurring in the subring $(K(x_1, \ldots, x_{i-1})[x_i])^G$. Let H_i be the subgroup of G that fixes $\{x_1, \ldots, x_i\}$. Then $d_i = [H_{i-1} : H_i]$.*

Proof. Let $L = K(x_1, \ldots, x_{i-1})$. Then G/H_i acts faithfully on $L(x_i)$ The subgroup of G/H_i that fixes L is H_{i-1}/H_i, so by Proposition 3.1 we have $d_i = [H_{i-1} : H_i]$. □

Corollary 3.6. *(With the same hypotheses and notation of Corollary 3.5.) The degrees d_i satisfy $d_1 d_2 \cdots d_m = |G|$.*

Proof. Using Corollary 3.5 we have

$$d_1 d_2 \cdots d_m = \frac{|H_0|}{|H_1|}\frac{|H_1|}{|H_2|} \cdots \frac{|H_{m-1}|}{|H_m|} = |G|.$$

□

4 Generic polynomial for D_8 in characteristic 2

Here, we present an application of the previous section to the problem of constructing generic polynomials, which parametrize all field extensions containing a base field K with a given Galois group G. For the general theory of generic polynomials, see [4].

Definition. Let K be a field and let G be a finite group. A separable polynomial $g(t_1, \ldots, t_m, X) \in K(t_1, \ldots, t_m)[X]$ with coefficients in the rational function field $K(t_1, \ldots, t_m)$ is *generic* for G over K if

1. The Galois group of g as a polynomial in X is G.
2. If L is a field containing K and N/L is a Galois extension with Galois group G, then there exist $\lambda_1, \ldots, \lambda_m \in L$ such that N is the splitting field of $g(\lambda_1, \ldots, \lambda_m, X)$ over L.

Our main tool to compute generic polynomials is a theorem of Kemper [5, Theorem 7] that we restate below.

Theorem 4.1 (Kemper)**.** *Let G be a finite group and let V be a m-dimensional faithful linear representation of G over the field K. Assume that $K(V)^G$ is purely transcendental over K with transcendence basis $\{\phi_1, \ldots, \phi_m\}$. Let $M \subset K(V)$ be a finite, G-stable subset that generates $K(V)$ over $K(V)^G = K(\phi_1, \ldots, \phi_m)$. Let*

$$f(X) = \prod_{y \in M} (X - y) \in K(V)^G[X],$$

so $f(X) = g(\phi_1, \ldots, \phi_m, X)$ with $g \in K(\phi_1, \ldots, \phi_m)[X]$. Then $g(X)$ is a generic polynomial for G over K.

It is a standard fact that a finite p-group G can be realized as a group of triangular unipotent matrices over a field of characteristic p. This can be seen, for instance, by taking a composition series of a faithful linear representation of G over $\mathbb{F}_p$.

We compute a generic polynomial for the dihedral group D_8 of order 16. Recall that this group is given by the presentation

$$D_8 = \langle a, x | a^8 = x^2 = 1, xax^{-1} = a^{-1}. \rangle$$

Using MAGMA, we find a 5-dimensional faithful representation of D_8 over $\mathbb{F}_2$ given by

$$a = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad x = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

MAGMA also provides a fundamental set of invariants $\{t_1, \dots t_5\}$ for D_8 acting on $\mathbb{F}_2[x_1, \dots, x_5]$ via the matrices above.

$$\begin{aligned} t_1 &= x_1 \\ t_2 &= x_2(x_2 + x_1) \\ t_3 &= x_3(x_3 + x_1)(x_3 + x_2)(x_3 + x_2 + x_1) \\ t_4 &= x_1x_4 + x_1x_3 + x_2x_3 + x_3^2 \\ t_5 &= x_2(x_2 + x_1)(x_5)(x_5 + x_1) + x_2^2x_3^2 + x_1^2x_3x_4 + x_1x_3^2x_4 + x_1x_3x_4^2 + x_3^2x_4^2 + x_4^4. \end{aligned}$$

As we will see below, these invariants form actually a transcendence basis for $\mathbb{F}_2(x_1, \dots, x_5)^{D_8}$. Indeed, let d_i be the degree of t_i in x_i. From the expressions above, $d_1 = 1$, $d_2 = 2$, $d_3 = 4$, $d_4 = 1$, and $d_5 = 2$. Hence $d_1d_2d_3d_4d_5 = 16 = |D_8|$. It follows that the d_i are minimal by Corollary 3.6, so $\{t_1, \dots, t_5\}$ is a transcendence basis for the field of invariants. Notice that each invariant is expressed in the form described in Corollary 3.4.

Let M be the orbit of x_5, explicitly $M = \{x_5, x_2 + x_4 + x_5, x_2 + x_3 + x_5, x_2 + x_3 + x_4 + x_5, x_1 + x_5, x_1 + x_2 + x_4 + x_5, x_1 + x_2 + x_3 + x_5, x_1 + x_2 + x_3 + x_4 + x_5\}$. The set M is D_8-stable by construction and it is easy to see that it spans the same vector space over $\mathbb{F}_2$ as $\{x_1, \dots, x_5\}$, so it generates $\mathbb{F}_2(x_1, \dots, x_5)$ over $\mathbb{F}_2$. Thus M satisfies the hypothesis of Theorem 4.1.

In order to find a generic polynomial, we need to express the coefficients of

$$\prod_{y \in M} (X - y)$$

in terms of $t_1, \dots, t_5$. We explain below an algorithmic procedure to do this.

Let $A/B \in \mathbb{F}_2(x_1, \dots, x_5)^G$, where A and B are relatively prime polynomials in x_5. Then $g(A) = \chi(g)A$ and $g(B) = \chi(g)B$, where $\chi(g) \in \mathbb{F}_2(x_1, \dots, x_4)^*$. Since in our case G is a

group of unipotent matrices, the leading coefficient of A and B must be preserved, which means $\chi(g) = 1$ for all $g \in G$, so A and B are actually invariant. Furthermore, by Proposition 1.1, we have $\mathbb{F}_2(x_1, \ldots, x_4)[x_5]^G = \mathbb{F}_2(x_1, \ldots, x_4)^G[t_5]$. We apply to A and B the procedure based on the Euclidean algorithm described in the proof of Proposition 2.1 (part (4) $\Longrightarrow$ (5)) to express A and B as a polynomials in t_5 with coefficients that are rational functions in $x_1, \ldots, x_4$ fixed by G. We apply the same procedure to the numerator and denominator of each of these coefficients to express them as a polynomials in t_4 with coefficients that are rational functions in $x_1, \ldots, x_3$. Continuing this process will eventually result in A/B expressed as a rational function in $t_1, \ldots, t_5$. This process was implemented in Mathematica. We obtain this way the following D_8-generic polynomial over $\mathbb{F}_2$:

$$\frac{1}{t_1^{16}t_2^4}(t_1^{16}t_2^4t_3^2+t_1^{14}t_2^5t_3^2+t_1^{14}t_2^3t_3^3+t_1^{12}t_2^4t_3^3+t_1^{16}t_3^4+t_1^8t_2^4t_3^4+t_1^8t_2^2t_3^5+t_1^8t_3^6+t_3^8+t_1^{16}t_2^5t_3t_4+t_1^{16}t_2^3t_3^2t_4+t_1^{14}t_2^5t_3t_4^2+t_1^{16}t_2^2t_3^2t_4^2+t_1^{12}t_2^2t_3^3t_4^2+t_1^8t_2^2t_3^4t_4^2+t_1^{16}t_2^3t_3t_4^3+t_1^{12}t_2^6t_4^4+t_1^{14}t_2^3t_3t_4^4+t_1^{16}t_3^2t_4^4+t_1^{12}t_2^4t_4^6+t_1^{12}t_2^2t_3t_4^6+t_1^8t_2^2t_3t_4^8+t_1^8t_3^2t_4^8+t_1^8t_2^2t_4^{10}+t_4^{16}+t_1^{16}t_2^6t_5+t_1^{16}t_2^2t_3^2t_5+t_1^{14}t_2^3t_3^2t_5+t_1^{12}t_2^2t_3^3t_5+t_1^8t_2^2t_3^4t_5+t_1^{16}t_2^3t_3t_4t_5+t_1^{16}t_2^4t_4^2t_5+t_1^{16}t_2^2t_3t_4^2t_5+t_1^{14}t_2^3t_3t_4^2t_5+t_1^{12}t_2^4t_4^4t_5+t_1^{12}t_2^2t_3t_4^4t_5+t_1^8t_2^2t_4^8t_5+t_1^{16}t_2^4t_5^2+t_1^{16}t_2^2t_4^2t_5^2+t_1^{16}t_2^2t_5^3+t_1^{16}t_5^4)+\frac{1}{t_1^7t_2}(t_1^8t_2^4+t_1^8t_3^2+t_1^6t_2t_3^2+t_1^4t_3^3+t_3^4+t_1^8t_2t_3t_4+t_1^8t_2^2t_4^2+t_1^8t_3t_4^2+t_1^6t_2t_3t_4^2+t_1^4t_2^2t_4^4+t_1^4t_3t_4^4+t_4^8+t_1^8t_5^2)X+\frac{1}{t_1^8t_2}(t_1^{10}t_2^3+t_1^8t_2^4+t_1^8t_3^2+t_1^6t_2t_3^2+t_1^4t_3^3+t_3^4+t_1^8t_2t_3t_4+t_1^{10}t_2t_4^2+t_1^8t_2^2t_4^2+t_1^8t_3t_4^2+t_1^6t_2t_3t_4^2+t_1^4t_2^2t_4^4+t_1^4t_3t_4^4+t_4^8+t_1^{10}t_2t_5+t_1^8t_5^2)X^2+t_1^3t_2X^3+(t_1^4+t_1^2t_2+t_2^2+t_4^2+t_5)X^4+t_1t_2X^5+t_2X^6+X^8.$$

5 Conclusion

To summarize, given a finite group G acting on $L(x)$ such that G preserves L and $g(x) = a(g)x+b(g)$ for all $g \in G$, $L[x]^G = L^G[\phi]$ for any ϕ of minimal degree in $L[x]^G$. Using elementary methods, we were able to determine much more about the invariant ϕ, as summarized in Corollary 3.4. If G is a finite group of upper triangular matrices acting on $K(x_1, \ldots, x_m)$ linearly on the indeterminants, our results can be applied to test whether a set of invariants $\phi_1, \ldots, \phi_m$ with $\phi_i \in K(x_1, \ldots, x_i) \cap K(x_1, \ldots, x_m)^G$ generates all of $K(x_1, \ldots, x_m)^G$ by looking at the degrees of $\phi_1, \ldots, \phi_m$. This has applications to the computations of generic polynomials, as seen in section 4.

The methods of this paper are specific to triangular groups. We do not expect them to be generalizable to other classes of groups. The Noether Problem and the explicit determination of transcendence bases is still widely open in general.

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[2] W. Gaschütz. Fixkörper von p-Automorphismengruppen rein-transzendener Körpererweiterungen von p-Charakteristik. *Math. Z.*, 71:466–468, 1959.

[3] M. Hajja and M. C. Kang. Finite group actions on rational function fields. *J. Algebra*, 149(1):139–154, 1992.

[4] C. U. Jensen, A. Ledet, and N. Yui. *Generic polynomials*, volume 45 of *Mathematical Sciences Research Institute Publications*. Cambridge University Press, Cambridge, 2002. Constructive aspects of the inverse Galois problem.

[5] G. Kemper and E. Mattig. Generic polynomials with few parameters. *J. Symbolic Comput.*, 30(6):843–857, 2000. Algorithmic methods in Galois theory.

[6] H. Kuniyoshi. Certain subfields of rational function fields. In *Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955*, pages 241–243, Tokyo, 1956. Science Council of Japan.

[7] H. W. Lenstra, Jr. Rational functions invariant under a finite abelian group. *Invent. Math.*, 25:299–325, 1974.

[8] T. Miyata. Invariants of certain groups. I. *Nagoya Math. J.*, 41:69–73, 1971.

[9] E. Noether. Gleichungen mit vorgeschriebener Gruppe. *Math. Ann.*, 78(1):221–229, 1917.

[10] R. G. Swan. Invariant rational functions and a problem of Steenrod. *Invent. Math.*, 7:148–158, 1969.