[Rose-Hulman Undergraduate Mathematics Journal](https://scholar.rose-hulman.edu/rhumj)

Volume 14
Issue 1

Article 9

Generic Polynomials for Transitive Permutation Groups of Degree 8 and 9

Bradley Lewis Burdick
The Ohio State University, burdick.28@buckeyemail.osu.edu

Jonathan Jonker
Michigan State University

Rose-Hulman Undergraduate Mathematics Journal

Generic Polynomials for Transitive Permutation Groups of Degree 8 and 9

Bradley Lewis Burdick[a] Jonathan Jonker [b]

Volume 14, No. 1, Spring 2013

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]The Ohio State University
[b]Michigan State University

Rose-Hulman Undergraduate Mathematics Journal
Volume 14, No. 1, Spring 2013

Generic Polynomials for Transitive Permutation Groups of Degree 8 and 9

Bradley Lewis Burdick   Jonathan Jonker

Abstract. We compute generic polynomials for certain transitive permutation groups of degree 8 and 9, namely SL(2,3), the generalized dihedral group: $C_2 \ltimes (C_3 \times C_3)$, and the Iwasawa group of order 16: M_{16}. Rikuna proves the existence of a generic polynomial for SL(2,3) in four parameters in [13]; we extend a computation of Gröbner in [5] to give an alternative proof of existence for this group's generic polynomial. We establish that the generic dimension and essential dimension of the generalized dihedral group are two. We establish over the rationals that the generic dimension and essential dimension of $\mathrm{SL}(2,3)$ and M_{16} are four.

Acknowledgements: This work was completed as a part of the Louisiana State University's 2012 Math REU. The authors would like to thank NSF for funding the REU, Dr. Jorge Morales for guidance and direction, and the referee for referring us to [9] and the idea for Theorems 3.9 and 5.11.

1 Introduction

Since Galois first proved his correspondence theorem the main conjecture of Galois theory has been to construct Galois extensions with any given Galois groups. This conjecture is called "the inverse Galois problem." An early advancement of Noether, since named the "Noether Problem," gives a computational solution to the inverse Galois problem. Suppose a group G can be faithfully represented as a subgroup of $\mathrm{GL}_n(k)$, then we extend the action of G to the field of rational functions in n variables, $k(\boldsymbol{x})$, by composition, i.e. if $f \in k(\boldsymbol{x})$, then $g(f) = f \circ g^{-1}$. Noether's problem is then concerned with $k(\boldsymbol{x})^G$, the subset fixed by the action of G, and it can be phrased as follows.

> Noether's Problem: *Is $k(\boldsymbol{x})^G$ rational, i.e. does there exist an algebraically independent k-basis for $k(\boldsymbol{x})^G$?*

Over a number field, to have a solution to Noether's problem implies a solution to the inverse Galois problem (it follows from Hilbert's irreducibility theorem). But having a solution to Noether's problem is actually a more stringent property than having a solution to the inverse Galois problem. In 1969, Swan [14] showed that C_{47} fails to have a solution for the former, yet all cyclic groups are Galois groups over the rationals and so have a solution for the latter.

So perhaps Noether's problem is too crude. When thinking of Galois extensions as splitting fields of polynomials it becomes natural to ask an intermediate question. One might call it the "generic polynomial problem," and it phrased as follows.

> Generic Polynomial Problem: *Is there a generic polynomial for G over k?*

Where by "generic," we mean that all Galois extensions with a certain group G over a field k are the splitting field of the polynomial (see Definition 2.1). One might hope that all groups for which there exists Galois extensions have generic polynomials, but this is not the case. For instance, C_8 has no generic polynomial over the rationals, though there are most definitely Galois extensions with group C_8 [12].

We restrict our attention to answering the generic polynomial problem for three groups of interest, namely $\mathrm{SL}_2(\mathbb{F}_3)$, $C_2 \ltimes (C_3 \times C_3)$, and M_{16}. We will introduce our notation and procedure in Section 2. The final three sections are each devoted to an individual group, its background in the generic polynomial question, and then the computations necessary to exhibit its generic polynomial. The significant facts of our results can be stated as follows.

Results 1.1. *There exists a generic polynomial for $C_2 \ltimes (C_3 \times C_3)$ in two parameters (4.6) and for M_{16} and $SL_2(\mathbb{F}_3)$ in four parameters (3.6,5.10). Moreover, over $\mathbb{Q}$ the generic and essential dimensions for $C_2 \ltimes (C_3 \times C_3)$ are two (4.9,4.11) and for M_{16} and $SL_2(\mathbb{F}_3)$ are four (5.11,3.9).*

2 Background

Throughout this paper G will be a finite group, and k will be a field assumed to have characteristic relatively prime to the order of the group being considered (namely neither two nor three). For ease of notation we will give the following notation and presentations to our three groups of interest.

$$\Gamma_1 = \mathrm{SL}_2(\mathbb{F}_3),\ \Gamma_2 = C_2 \ltimes (C_3 \times C_3) = \langle x, y, z | x^2 = y^3 = z^3, xyx = y^2, xzx = z^2\rangle,$$
$$\Gamma_3 = M_{16} = \langle x, y | x^2 = y^8, xyx = y^5\rangle.$$

Where the special linear group's presentation is implicit. The notation and definitions introduced in Section 1 will be maintained through the paper.

The purpose of this paper is to answer the generic polynomial problem for Γ_1, Γ_2, and Γ_3 over k of characteristic relatively prime to the group's order. As stated, the generic polynomial of G over k provides every polynomial whose splitting field over k has as a Galois group a subgroup of G. To be precise:

Definition 2.1. *A monic, separable polynomial $P(\boldsymbol{x}, T) \in k(\boldsymbol{x})[T]$, where $\boldsymbol{x}$ is a vector of length n, is a* generic polynomial *for G* over *k if the following conditions are met.*

1. *$Gal(P/k(\boldsymbol{x})) \cong G$.*
2. *If m/l is Galois with group G and $k \subseteq l$, then m is the splitting field for $P(\boldsymbol{a}, T)$ for some $\boldsymbol{a} \in l^n$.*

While the explicit polynomial can vary depending on choice of transcendence basis for $k(\boldsymbol{x})$, the second condition gives a map from any one generic polynomial to another. Thus, while our problem is to prove the existence of such polynomials, uniqueness is very much opposed to genericness. Instead, generic polynomials provide an arithmetic function on finite groups.

Definition 2.2. *The minimal length of the vector $\boldsymbol{x}$ in Definition 2.1 is called the* generic dimension *of G over k and is denoted $gd_k(G)$. If there is no generic polynomial for G over k, then $gd_k(G) = \infty$.*

Since having a generic polynomial is a weaker condition then satisfying the Noether problem, it is also harder to establish the existence of one. An elementary example is given by Artin-Schreier theory.

Example 2.3. *$x^p - x - t \in \mathbb{F}_p[x, t]$ is C_p-generic over $\mathbb{F}_p$ [11].*

To establish that this was a generic polynomial is nonconstructive, whereas to establish that C_p satisfies the Noether problem over $\mathbb{F}_p$ only requires the construction of a transcendence basis.

Though the focus of this paper is the existence of generic polynomials, our main work is actually the computations involved in solving Noether's problem for these groups. The following theorem of Kemper and Mattig will do all the theoretical work needed to prove that the polynomials we exhibit are generic. The theorem proves that an answer to Noether's Problem implies the existence of a generic polynomial. The theorem is constructive.

Theorem 2.4. *[10, Theorem 3] Let G be a finite group and V an m-dimensional, faithful linear representation of G over a field k. If $\boldsymbol{x}$ is a basis for V, then $k(V) := k(\boldsymbol{x})$. Assume that $k(V)^G = k(\boldsymbol{v})$, where $\boldsymbol{v}$ is a transcendence basis. Choose a finite G-stable subset $\mathcal{M} \subseteq k(V)$ such that $k(V) = k(V)^G(\mathcal{M})$. If*

$$f(T) := \prod_{y \in \mathcal{M}} (T - y) \in k(V)^G[T],$$

then $f(T)$ is a polynomial with coefficients in $k(\boldsymbol{v})$ and is a generic polynomial for G over k.

Our procedure will follow the construction in this theorem. For each group, we will define a representation (the theorem does not specify a choice of representation). Then we will determine the fixed field. Since each group we are interested in is solvable, we will consider the subnormal series. We will compute the fixed fields of each successive group in the subnormal series, and this will resolve with the fixed field of the full group. After completing this process we will have shown that each group satisfies the Noether problem, and by Theorem 2.4 we conclude that a generic polynomial exists.

We would also like to exhibit the smallest possible generic polynomials in the sense that the number of parameters in minimal. There is a concept related to generic dimension called *essential dimension.*

Definition 2.5. *[7] The essential dimension of a group G over a field k is denoted as follows. If V is the regular representation of G, then*

$$ed_k(G) = min\{trdeg_k E : G \text{ acts faithfully on } E \subseteq k(V)\}.$$

Where a group need not have a defined generic dimension, every group has finite essential dimension. The following lemma is well known, and an open conjecture strengthens it to equality.

Lemma 2.6. *[6, Proposition 8.2.10] $ed_k(G) \leq gd_k(G)$.*

We will use this lemma to verify that equality holds for each of our groups and that our polynomials are indeed minimal.

3 A Generic Polynomial for $\mathrm{SL}_2(\mathbb{F}_3)$ in Four Parameters

Let Γ_1 be the special linear group of degree two over the field of order three. We will compute the generic polynomial by the method of Kemper and Mattig.

We begin by defining a faithful linear representation of Γ_1 in dimension 4 over k (of characteristic not 2 nor 3). Let $\{x_1, x_2, x_3, x_4\}$ be a basis of V such that the following act by left multiplication of column vectors.

$$i := \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \tau := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

Proposition 3.1. $\langle i, \tau \rangle \cong \Gamma_1$.

Proof. Using the fact that $\Gamma_1 \cong C_3 \ltimes Q_8$ (where C_3 acts on the quaternion group by permuting i, j, and k), one may check that i, $j := \tau i \tau^{-1}$, and $k := \tau j \tau^{-1}$ interact as the usual generators of Q_8 and that τ generates a disjoint cyclic subgroup of order three inside $\mathrm{GL}_4(k)$ and conclude that $\langle i, \tau \rangle \cong C_3 \ltimes Q_8 \cong \Gamma_1$. □

At the time [6] was written, the existence (or nonexistence) of a generic polynomial had been established for groups of order ≤ 32 except for Q_{16} (the generalized quaternions) and Γ_1. For Q_{16}, the Noether problem has since been answered in the negative, and the generic polynomial problem has been answered in the negative over the rationals as noted in [8] as a result of [4] . It would seem that Γ_1 remains the last unknown for groups of order ≤ 32, but in an unpublished work [13], Rikuna proves an affirmative answer of Noether's problem for Γ_1. If true, this would imply the existence of a generic polynomial. We proceed in a similar but simpler manner. As noted above, $\Gamma_1 \cong C_3 \ltimes Q_8$, and both C_3 and Q_8 are known to satisfy Noether's problem [6], [5]. We utilize these facts to make easy work of the heretofore stubborn group $\mathrm{SL}_2(\mathbb{F}_3)$.

3.1 The Fixed Field of Γ_1

Our choice of representation is meant to coincide with the result of Gröbner. If $A := \langle i, j, k \rangle$, then $A \cong Q_8$ and has the representation used in [5]. We will provide the basis of $k(x_1, x_2, x_3, x_4)^A$, and examine the action of $\langle \tau \rangle$ on this basis. After finding the fixed points of this action, the computation of $k(x_1, x_2, x_2, x_4)^{\Gamma_1}$ will be complete.

3.1.1 The Fixed Field of A

The following theorem was computed entirely in Gröbner's paper [5].

Theorem 3.2. *[5, Formula 9] If A has the representation given above, then $k(x_1, x_2, x_3, x_4)^A = k(j_1, j_2, j_3, j_4)$ where j_i is as follows.*

$$j_1 = -\frac{2(x_2x_3 - x_1x_4)(-x_1x_3 + x_2x_4)}{x_1x_3 + x_2x_4}$$
$$j_2 = \frac{x_1^2 + x_2^2 - x_3^2 - x_4^2}{x_1x_3 - x_2x_4}$$
$$j_3 = -\frac{x_2x_3 + x_1x_4}{-x_1x_3 + x_2x_4}$$
$$j_4 = 2(x_1^2 + x_2^2 + x_3^2 + x_4^2)$$

3.1.2 The Fixed Field of $\langle\tau\rangle$

Let us now consider the action of τ induced on $\{j_1, j_2, j_3, j_4\}$ by acting on each y_i. One may check that it is described as follows.

$$\tau : (j_1, j_2, j_3, j_4) \to \left(\frac{j_1 j_4 (4j_1 + j_1 j_2^2 + 4j_1 j_3^2 + j_2 j_3 j_4)}{2j_3(4j_1^2 + j_1^2 j_2^2 + 4j_1^2 j_3^2 + j_4^2)}, \frac{j_1 j_2 j_3 - j_4}{j_1(1 + j_3^2)}, \frac{j_1 j_2 + j_3 j_4}{2j_1(1 + j_3^2)}, j_4 \right).$$

Since this is highly nonlinear (save for the action on j_4, which is constant), finding a basis for the field $k(j_1, j_2, j_3, j_4)^{\langle\tau\rangle}$ would seem arduous. As mentioned, if τ were to act by cyclic permutation, then a basis for the field of invariants is well known [6]. The solution set, $\tau(j_1, j_2, j_3, j_4) = (j_1, j_2, j_3, j_4)$, is a rational curve over $k(j_4)$. This suggests that τ would be conjugate to a linear action. Indeed the miracle is that we can reduce our problem to such an action via the following lemma.

Lemma 3.3. *If* $(r_1, r_2, r_3, r_4) = (j_2, \tau(j_2), \tau^2(j_2), j_4)$, *then* $k(j_1, j_2, j_3, j_4) = k(r_1, r_2, r_3, r_4)$.

Proof. It suffices to express j_1 and j_3 in terms of r_1, r_2, r_3, and r_4. A calculation shows the following.

$$\begin{aligned} j_1 &= -\frac{r_4(-8 + r_1 r_2 r_3)^2}{(16 + 4r_1^2 + r_1^2 r_2^2)(4r_2 + 2r_1 r_3 + r_2 r_3^2)} \\ j_3 &= \frac{2r_1 r_2 + 4r_3 + r_1^2 r_3}{-8 + r_1 r_2 r_3}. \end{aligned}$$

□

We now have $k(x_1, x_2, x_3, x_4)^A = k(r_1, r_2, r_3, r_4)$ and the action of τ simplified to the following.

$$\tau : (r_1, r_2, r_3, r_4) \longmapsto (r_2, r_3, r_1, r_4).$$

Now we may cite the following theorem.

Lemma 3.4. *[6, Section 2.1]* $k(r_1, r_2, r_3, r_4)^{\langle\tau\rangle} = k(d_1, d_2, d_3, d_4)$, *where*

$$\begin{aligned} d_1 &= \frac{(r_1 - r_2)^2(r_2 - r_3) + (r_1 - r_2)(r_2 - r_3)^2}{(r_1 - r_2)^2 + (r_1 - r_2)(r_2 - r_3) + (r_2 - r_3)^2} \\ d_2 &= \frac{(r_1 - r_2)^3 - 3(r_1 - r_2)(r_2 - r_3)^2 - (r_2 - r_3)^3}{(r_1 - r_2)^2 + (r_1 - r_2)(r_2 - r_3) + (r_2 - r_3)^2} \\ d_3 &= r_1 + r_2 + r_3 \\ d_4 &= r_4 \end{aligned}$$

Since $A \trianglelefteq \Gamma_1$, we have that $k(x_1, x_2, x_3, x_4)^{\Gamma_1} = (k(x_1, x_2, x_3, x_4)^A)^{\Gamma_1/A}$. This proves the following theorem.

Theorem 3.5. $k(x_1, x_2, x_3, x_4)^{\Gamma_1} = k(r_1, r_2, r_3, r_4)$.

3.2 A Generic Polynomial of Γ_1 in Four Parameters

To apply Theorem 2.4 we need only to choose a Γ_1-stable subset $\mathcal{V}$ that satisfies $k(x_1, x_2, x_3, x_4)^{\Gamma_1}(\mathcal{V}) = k(x_1, x_2, x_3, x_4)$. The easiest choice is the set generated by $\{x_1, x_2, x_3, x_4\}$ under the action of Γ_1. This is just $\mathcal{V} = \{\pm x_1, \pm x_2, \pm x_3, \pm x_4\}$. Then we let h be as follows.

$$h(T) := \prod_{i=1}^{4}(T^2 - y_i^2) \in k(x_1, x_2, x_3, x_4)^{\Gamma_1}[T].$$

Now one may replace the coefficients of h with functions in $k(r_1, r_2, r_3, r_4)$. Then $h(T) = j(T) \in k(x_1, x_2, x_3, x_4)^{\Gamma_1}[T]$. Our computations have yielded an explicit $j(r_1, r_2, r_3, r_4, T)$, which these margins are too narrow to contain. We do, however, have the following existence theorem.

Theorem 3.6. *$j \in k(r_1, r_2, r_3, r_4)[T]$ is an even, degree 8 generic polynomial in four parameters for $SL_2(\mathbb{F}_3)$ over k.*

3.2.1 The Minimality of j

We have answered the generic polynomial problem for Γ_1 by answering the Noether problem. We would additionally like to say that j is minimal, minimal in the sense of degree and the number of parameters. The minimal degree of the polynomial depends on the permutation group's degree, and Γ_1 is indeed a degree 8 permutation group. We will now establish that j has the minimal number of parameters, i.e. that j realizes $\mathrm{gd}_k(\Gamma_1)$. Theorem 3.6 already provides an upper bound for $\mathrm{gd}_k(\Gamma_1)$, namely 4. The following will be used to conclude in Theorem 3.9 that the number of parameters of j is indeed the generic dimension.

Lemma 3.7. *[6, Proposition 8.2.7] If $H \leq G$, then $ed_k(H) \leq ed_k(G)$.*

Theorem 3.8. *[9, Theorem 4.1] Let G be a p-group and k a field of characteristic different from p containing a primitive p-th root of unity. Then $ed_k(G)$ coincides with the least dimension of a faithful representation of G over k.*

Theorem 3.9. *$ed_{\mathbb{Q}}(\Gamma_1) = gd_{\mathbb{Q}}(\Gamma_1) = 4$.*

Proof. As we have remarked, $Q_8 \hookrightarrow \Gamma_1$, so from Lemma 3.7, $\mathrm{ed}_{\mathbb{Q}}(Q_8) \leq \mathrm{ed}_{\mathbb{Q}}(\Gamma_1)$. We apply Theorem 3.8 to Q_8 over $\mathbb{Q}$. Indeed Q_8 is a 2-group and $\mathbb{Q}$ contains the square roots of unity. We find then that $\mathrm{ed}_{\mathbb{Q}}(Q_8)$ is the least degree of a faithful representation of Q_8 over $\mathbb{Q}$. This is known to be 4. So we have that $4 = \mathrm{ed}_{\mathbb{Q}}(Q_8) \leq \mathrm{ed}_{\mathbb{Q}}(\Gamma_1) \leq \mathrm{gd}_{\mathbb{Q}}(\Gamma_1) \leq 4$. $\square$

4 A Generic Polynomial for $C_2 \ltimes (C_3 \times C_3)$ in Two Parameters

Let Γ_2 be the generalized dihedral group of the elementary abelian group of order nine. We will compute the generic polynomial by the method of Kemper and Mattig.

We begin by defining a faithful linear representation of Γ_2 in dimension 4 over k (of characteristic not 2 nor 3). Let $\{x_1, x_2, x_3, x_4\}$ be a basis of V such that the following act by left multiplication of column vectors.

$$\zeta := \begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad \eta := \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \theta := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

Proposition 4.1. $\langle \zeta, \eta, \theta \rangle \cong \Gamma_2$.

Proof. One may check that $\zeta^2 = \eta^3 = \theta^3 = 1$, and that $\zeta\eta\zeta = \eta^2$ and $\zeta\theta\zeta = \theta^2$. $\square$

This action can then be compressed faithfully to a subfield of transcendence degree 2. If we let $x = x_1/x_2$ and $y = x_3/x_4$, and let Γ_2 act on numerators and denominators independently, one may check that this defines the following actions.

$$\zeta : (x, y) \longmapsto (1-x, 1-y) \quad \eta : (x, y) \longmapsto \left(\frac{1}{1-x}, y\right) \quad \theta : (x, y) \longmapsto \left(x, \frac{1}{1-y}\right).$$

This is no longer a linear representation of Γ_2. We will first find the field fixed by this action, $k(x, y)^{\Gamma_2}$, and then use it to compute the field fixed by the linear action, $k(x_1, x_2, x_3, x_4)^{\Gamma_2}$. The result will allow us to compute a generic polynomial with 2 rather than 4 parameters.

4.1 The Fixed Field of Γ_2 Acting on $k(x, y)$

We proceed first by considering the normal subgroup of index 2 isomorphic to $C_3 \times C_3$ generated by η and θ. Once this is done we consider the action of $\Gamma_2/\langle \eta, \theta \rangle = \langle \overline{\zeta} \rangle$ on $k(x, y)^{\langle \eta, \theta \rangle}$ to establish the generators of the full fixed field.

4.1.1 The Fixed Field of $\langle \eta, \theta \rangle$

Since the orbits of x and y under η and θ are disjoint (i.e. only intersecting at x and y), we may consider the fixed fields of the subgroups $\langle \eta \rangle$ and $\langle \theta \rangle$ separately. Indeed since η acts on (x, y) identically to how θ acts on (y, x), we need only compute $k(x, y)^{\langle \eta \rangle}$ to find the basis of $k(x, y)^{\langle \eta, \theta \rangle}$.

Lemma 4.2. $k(x, y)^{\langle \eta, \theta \rangle} = k(x + \eta(x) + \eta^2(x), y + \theta(y) + \theta^2(y))$

Proof. By symmetry, it suffices to prove that $k(x,y)^{\langle\eta\rangle} = k(x+\eta(x)+\eta^2(x),y)$. Since $x+\eta(x)+\eta^2(x)$ is the trace of x with respect to $\langle\eta\rangle$, it is contained in $k(x,y)^{\langle\eta\rangle}$. We define a polynomial over $k(x+\eta(x)+\eta^2(x),y)[T]$ that x satisfies. Note this trace is written in terms of x as follows.

$$x+\eta(x)+\eta^2(x) = \frac{-x^3+3x-1}{(1-x)(x)}.$$

So x satisfies the following equation of rational functions and similarly the equivalent polynomial equation.

$$\frac{-T^3+3T-1}{(1-T)(T)} = x+\eta(x)+\eta^2(x) \iff -T^3+3T-1-(x+\eta(x)+\eta^2(x))(1-T)(T) = 0.$$

So x is a root of a cubic polynomial over $k(x+\eta(x)+\eta^2(x),y)$, and

$$[k(x,y) : k(x+\eta(x)+\eta^2(x),y)] \leq 3.$$

Moreover since $k(x,y)$ over the fixed field is a degree three extension, we have

$$\begin{aligned}[k(x,y) : k(x+\eta(x)+\eta^2(x),y)] &= [k(x,y) : k(x,y)^{\langle\eta\rangle}][k(x,y)^{\langle\eta\rangle} : k(x+\eta(x)+\eta^2(x),y)] \\ &= 3[k(x,y)^{\langle\eta\rangle} : k(x+\eta(x)+\eta^2(x),y)] \leq 3.\end{aligned}$$

Thus we have that $[k(x,y)^{\langle\eta\rangle} : k(x+\eta(x)+\eta^2(x),y)] = 1$. □

4.1.2 The Fixed Field of $\langle\zeta\rangle$

For ease of notation we make the following our transcendence basis of $k(x,y)^{\langle\eta,\theta\rangle}$.

$$u := x+\eta(x)+\eta^2(x) \quad v := y+\theta(y)+\theta^2(y).$$

For ease in future computation we relabel again.

$$a := u-\zeta(u) \qquad b := v-\zeta(v).$$

It is clear that $k(x,y)^{\langle\eta,\theta\rangle} = k(a,b)$, now with the added bonus that $\zeta(a,b) = (-a,-b)$.

Lemma 4.3. *$k(u,v)^{\langle\zeta\rangle} = k(a^2,ab)$.*

Proof. Note that $\zeta(a^2,ab) = ((-a)^2,(-a)(-b)) = (a^2,ab)$, so $k(a^2,ab) \subseteq k(u,v)^{\langle\zeta\rangle}$. Furthermore $T^2-a^2 \in k(a^2,ab)[T]$ is irreducible with splitting field $k(u,v)$, so $[k(u,v) : k(a^2,ab)] = 2$. Since $[k(u,v) : k(u,v)^{\langle\zeta\rangle}] = 2$, we must have that $k(u,v)^{\langle\zeta\rangle} = k(a^2,ab)$. □

4.1.3 The Fixed Field of Γ_2 Acting on $k(x, y)$

Combining all the work thus far, we have proved the following theorem.

Theorem 4.4. $k(x, y)^{\Gamma_2} = k(a^2, ab)$.

Peeling back substitutions we get the following transcendence basis of $k(x, y)^{\Gamma_2}$ in terms of x and y.

$$\begin{aligned} a^2 &= \frac{(-2+x)^2(1+x)^2(-1+2x)^2}{(-1+x)^2x^2} \\ ab &= \frac{(-2+x)(1+x)(-1+2x)(-2+y)(1+y)(-1+2y)}{(-1+x)x(-1+y)y}. \end{aligned}$$

4.2 The Fixed Field of Γ_2

Consider the following functions.

$$c = \frac{x_1x_2(x_1+x_2)}{x_1^2+x_1x_2+x_2^2}, \text{ and } d = \frac{x_3x_4(x_3+x_4)}{x_3^2+x_3x_4+x_4^2}.$$

One may check that $c, d \in k(x_1, x_2, x_3, x_4)^{\Gamma_2}$. We would like to express $k(x_1, x_2, x_3, x_4)^{\Gamma_2}$ in terms of a^2, ab, c, and d.

Theorem 4.5. $k(x_1, x_2, x_3, x_4)^{\Gamma_2} = k(a^2, ab, c, d)$.

Proof. We apply the special case of Lüroth's Theorem phrased at the end of [6, §1.1] to c and d. Since they are homogeneous of degree 1 we may conclude the following.

$$k(x_1, x_2)^{\langle\eta\rangle} = k(x, c)^{\langle\eta\rangle} = k(x)^{\langle\eta\rangle}(c) \text{ and } k(x_3, x_4)^{\langle\theta\rangle} = k(y, d)^{\langle\theta\rangle} = k(y)^{\langle\theta\rangle}(d).$$

And since η and θ only act nontrivially on respectively $\{x_1, x_2\}$ and $\{x_3, x_4\}$, we may conclude the following.

$$k(x_1, x_2, x_3, x_4)^{\langle\eta,\theta\rangle} = k(x, y)^{\langle\eta,\theta\rangle}(c, d).$$

Now since $k(x, y, c, d) \subseteq k(x_1, x_2, x_3, x_4)$, we have the following.

$$\begin{aligned} 9 &= [k(x_1, x_2, x_3, x_4) : k(x_1, x_2, x_3, x_4)^{\langle\eta,\theta\rangle}] \\ &= [k(x_1, x_2, x_3, x_4) : k(x, y, c, d)][k(x, y, c, d) : k(x_1, x_2, x_3, x_4)^{\langle\eta,\theta\rangle}] \\ &= [k(x_1, x_2, x_3, x_4) : k(x, y, c, d)][k(x, y, c, d) : k(x, y)^{\langle\eta,\theta\rangle}(c, d)] \\ &= [k(x_1, x_2, x_3, x_4) : k(x, y, c, d)](9). \end{aligned}$$

So $k(x_1, x_2, x_3, x_4) = k(x, y, c, d)$. And finally:

$$k(x_1, x_2, x_3, x_4)^{\Gamma_2} = k(x, y, c, d)^{\Gamma_2} = k(x, y)^{\Gamma_2}(c, d) = k(a^2, ab, c, d).$$

□

4.3 A Generic Polynomial of Γ_2 in Two Parameters

Having found the fixed field of the action of Γ_2, we may now apply Theorem 2.4. In order to do so, we need a Γ_2-stable subset $\mathcal{N}$ such that $k(x_1, x_2, x_3, x_4)^{\Gamma_2}(\mathcal{N}) = k(x_1, x_2, x_3, x_4)$. Since c and d are already in $k(x_1, x_2, x_3, x_4)^{\Gamma_2}$, adjoining any set containing x and y works. So in order to get a Γ_2-stable subset containing x and y, we just let $\mathcal{N} = \{g(x), g(y) : g \in \Gamma_2\}$. Since η and θ act trivially on y and x respectively, there are only 12 distinct elements of $\mathcal{N}$. Regardless, we have that the following polynomial can be written in terms of a^2 and ab.

$$f(T) := \prod_{\nu \in \mathcal{N}} (T - \nu) \in k(x, y)^{\Gamma_2}[T].$$

Now one may replace the coefficients of f with functions in $k(a^2, ab)$. If we let $\xi_1 := a^2$ and $\xi_2 := ab$, then $f(T) = g(T) \in k(x, y)^{\Gamma_2}[T]$ where g is as follows.

$$g(T) = -\frac{1}{16\xi_1}(-4 + 12T + 3T^2 - 26T^3 + 3T^4 + 12T^5 - 4T^6 + T^2\xi_1 - 2T^3\xi_1 + T^4\xi_1)$$
$$(-T^2\xi_2^2 + 2T^3\xi_2^2 - T^4\xi_2^2 + 4\xi_1 - 12T\xi_1 - 3T^2\xi_1 + 26T^3\xi_1 - 3T^4\xi_1 - 12T^5\xi_1 + 4T^6\xi_1).$$

This however is not irreducible, and one would expect a generic polynomial for Γ_2 to have degree nine, since $\Gamma_2 \leq S_9$. One can choose a better Γ_2-stable subset satisfying the conditions of Theorem 2.4; take for instance $\mathcal{W} = \{g(xy^{-1} + \zeta(xy^{-1})) : g \in \Gamma_2\}$. Then

$$\phi(T) := \prod_{\mu \in \mathcal{W}} (T - \mu) \in k(x, y)^{\Gamma_2}[T]$$

can be factored so that $\phi(T) = \psi(T) \in k(\xi_1, \xi_2)$ where ψ is as follows.

$$\begin{aligned}
\psi(T) = -(&-64T^9\xi_2^3 - 32T^8\xi_1\xi_2^3 + 288T^8\xi_2^3 - 4T^7\xi_1^2\xi_2^3 + 84T^7\xi_1^2\xi_2^2 + 128T^7\xi_1\xi_2^3 + \\
&36T^7\xi_2^4 + 396T^7\xi_2^3 + 24T^6\xi_1^3\xi_2^2 + 12T^6\xi_1^2\xi_2^3 - 324T^6\xi_1^2\xi_2^2 + 8T^6\xi_1\xi_2^4 - 32T^6\xi_1\xi_2^3 - \\
&180T^6\xi_2^4 - 3540T^6\xi_2^3 + T^5\xi_1^4\xi_2^2 - 21T^5\xi_1^4\xi_2 - 64T^5\xi_1^3\xi_2^2 - 38T^5\xi_1^2\xi_2^3 + 126T^5\xi_1^2\xi_2^2 - \\
&24T^5\xi_1\xi_2^4 - 136T^5\xi_1\xi_2^3 + 189T^5\xi_2^4 + 2655T^5\xi_2^3 - 2T^4\xi_1^5\xi_2 - 2T^4\xi_1^4\xi_2^2 + 36T^4\xi_1^4\xi_2 - \\
&2T^4\xi_1^3\xi_2^3 + 46T^4\xi_1^3\xi_2^2 + 90T^4\xi_1^2\xi_2^3 + 330T^4\xi_1^2\xi_2^2 - 6T^4\xi_1\xi_2^4 - 932T^4\xi_1\xi_2^3 + 288T^4\xi_2^4 + \\
&10458T^4\xi_2^3 + T^3\xi_1^6 + 2T^3\xi_1^5\xi_2 + 5T^3\xi_1^4\xi_2^2 + 18T^3\xi_1^4\xi_2 + 4T^3\xi_1^3\xi_2^3 - 40T^3\xi_1^3\xi_2^2 - 62T^3\xi_1^2\xi_2^3 + \\
&765T^3\xi_1^2\xi_2^2 + 52T^3\xi_1\xi_2^4 + 2222T^3\xi_1\xi_2^3 - 495T^3\xi_2^4 - 17256T^3\xi_2^3 - 2T^2\xi_1^5\xi_2 - 4T^2\xi_1^4\xi_2^2 + \\
&6T^2\xi_1^4\xi_2 - 2T^2\xi_1^3\xi_2^3 + 62T^2\xi_1^3\xi_2^2 + 34T^2\xi_1^2\xi_2^3 - 1278T^2\xi_1^2\xi_2^2 - 6T^2\xi_1\xi_2^4 - 1076T^2\xi_1\xi_2^3 - \\
&54T^2\xi_2^4 + 2448T^2\xi_2^3 - 36T\xi_1^4\xi_2 - 80T\xi_1^3\xi_2^2 - 68T\xi_1^2\xi_2^3 - 132T\xi_1^2\xi_2^2 - 24T\xi_1\xi_2^4 - 88T\xi_1\xi_2^3 + \\
&252T\xi_2^4 + 5040T\xi_2^3 + 8\xi_1^3\xi_2^2 + 16\xi_1^2\xi_2^3 - 72\xi_1^2\xi_2^2 + 8\xi_1\xi_2^4 - 176\xi_1\xi_2^3 - 72\xi_2^4 + 800\xi_2^3)(64\xi_2^3)^{-1}
\end{aligned}$$

Then as a direct result of Theorems 2.4 and 4.4 we have proved the following theorem.

Theorem 4.6. *$\psi(T) \in k(\xi_1, \xi_2)[T]$ is an odd, degree 9 generic polynomial for $C_2 \ltimes (C_3 \times C_3)$ over k.*

4.3.1 The Minimality of ψ

We have successfully answered the generic polynomial problem for Γ_2 by answering the Noether problem. We again note that ψ has the minimum degree as a permutation group of degree 9. We would also like to show that ψ is indeed a minimal generic polynomial in the sense that $\mathrm{gd}_k(\Gamma_2) = 2$. The following lemmas will be used to prove this in Theorem 4.9.

Lemma 4.7. *[6, Proposition 8.1.4] If there is a generic polynomial for G over k in one parameter, then $G \hookrightarrow PGL_2(k)$.*

Lemma 4.8. *[1, Lemma 2.1] If $G \leq PGL_2(k)$ and $G \cong C_p^r$, then $r \leq 1$ if p is odd and $r \leq 2$ if p is 2.*

Theorem 4.9. *$gd_k(\Gamma_2) = 2$.*

Proof. By Lemma 4.8 and Lemma 4.7, we know that $\mathrm{gd}_k(\Gamma_2) \neq 1$ lest $(C_3 \times C_3) \hookrightarrow \mathrm{PGL}_2(k)$. Since Γ_2 is nontrivial, $\mathrm{gd}_k(\Gamma_2) \neq 0$ by [7]. Finally, Theorem 4.6 provides explicitly a generic polynomial in two parameters. $\square$

We make one further note along this line of thought. As mentioned in Section 2 we would like to verify that $\mathrm{ed}_k(\Gamma_2) = \mathrm{gd}_k(\Gamma_2)$. We will use the following lemma to conclude this in Theorem 4.11.

Lemma 4.10. *[2, Lemma 7.2] If the essential dimension for G over k is one, then $G \hookrightarrow PGL_2(k)$.*

Theorem 4.11. *$ed_k(\Gamma_2) = gd_k(\Gamma_2) = 2$.*

Proof. By Lemma 4.10 and 4.8, we know that $\mathrm{ed}_k(\Gamma_2) \neq 1$ lest $C_3 \times C_3 \hookrightarrow \mathrm{PGL}_2(k)$. Since Γ_2 is nontrivial, $\mathrm{ed}_k(\Gamma_2) \neq 0$. And by Lemma 2.6, $1 < \mathrm{ed}_k(\Gamma_2) \leq \mathrm{gd}_k(\Gamma_2) = 2$. $\square$

5 A Generic Polynomial for M_{16} in Four Parameters

Let Γ_3 be the Iwasawa group of order 16. We will compute the generic polynomial by the method of Kemper and Mattig.

We begin by defining a faithful linear representation of Γ_3 in dimension 4 over k (of characteristic not 2). Let $\{x_1, x_2, x_3, x_4\}$ be a basis of V such that the following act by left multiplication of column vectors.

$$\sigma := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \text{ and } \rho := \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

We will proceed by finding a basis for the fixed field of $k(x_1, x_2, x_3, x_4)$, and then apply Theorem 2.4.

Proposition 5.1. $\langle \sigma, \rho \rangle \cong \Gamma_3$.

Proof. One may check that $\sigma^2 = \rho^8 = 1$ and $\sigma\rho\sigma = \rho^5$. □

Γ_3 was called a *modular* 2-*group* by Iwasawa in his classification of finite groups with modular subgroup latices [3, Ex. 8], thus the notation M_{2^n}. A lattice is modular if for any element $x \leq y$ and any element z the identity $x \vee (z \wedge y) = (x \vee z) \wedge y$ holds. One may check that Γ_3 with the given presentation has the subgroup lattice on the right and that this lattice is modular. In [11], Ledet exhibits a generic polynomial for Γ_3 in 5 parameters.

$$
\begin{array}{ccc}
 & \langle \rho, \sigma \rangle & \\
\diagup & | & \diagdown \\
\langle \rho \rangle & \langle \rho\sigma \rangle & \langle \rho^2, \sigma \rangle \\
| & \diagup \quad \diagup & | \\
\langle \rho^2 \rangle & \langle \rho^2\sigma \rangle & \langle \rho^4, \sigma \rangle \\
| & \diagup \quad \diagup & | \\
\langle \rho^4 \rangle & \langle \rho^4\sigma \rangle & \langle \sigma \rangle \\
\diagdown & | & \diagup \\
 & \langle 1 \rangle &
\end{array}
$$

Among abelian groups of this order, any with C_8 as a subgroup has no generic polynomial over $\mathbb{Q}$ [6]. one sees that there is difficulty for a generic polynomial to exist. It is an established fact that an abelian group with C_8 as a subgroup has no generic polynomial over $\mathbb{Q}$ [6, §2.6]. The dihedral and quasi-dihedral groups, do have generic polynomials, but the generalized quaternion group Q_{16} does not. To lower the number of parameters in Ledet's result we note the subnormal series $\langle \rho^4, \sigma \rangle \trianglelefteq \langle \rho^2, \sigma \rangle \trianglelefteq \Gamma_3$.

5.1 The Fixed Field of Γ_3

Determining the fixed field of such a group action is in general computationally hard, and though there are computer programs that can compute invariants, they do not produce transcendence bases. Thus the method we employ is iterative. We proceed by finding an invariant basis of a normal subgroup H and repeat for the group Γ_3/H. This process terminates with the full basis since Γ_3 is indeed solvable.

To eliminate the action of σ we begin by considering the subgroup $H_1 = \langle \sigma, \rho^4 \rangle \cong V_4$. Since there are only three elements of order two in Γ_3 and since any single order two element is the product of the other two, there is only one subgroup isomorphic to V_4, and thus it is normal. After determining the fixed field of H_1, we pass to the quotient $G_1 = \Gamma_3/H_1 \cong C_4$. Note that $G_1 = \langle \overline{\rho} \rangle$, where $\overline{\rho}$ is the quotient class. In the body of this section we will drop the over-line, since $\overline{\rho}$ and ρ will be acting the same just that $\overline{\rho}$ will act on elements previously fixed by the quotient subgroup. Rather than considering the whole group G_1 (since the action will be quite complicated by this time), we consider the unique subgroup of order 2 denoted by $H_2 = \langle \overline{\rho^2} \rangle \cong C_2$. After establishing the fixed field of this subgroup we pass to one final quotient, $G_2 = G_1/H_2 = \langle \overline{\overline{\rho}} \rangle \cong C_2$. Note that G_2 is also isomorphic to the quotient group of Γ_3 with respect to the unique normal subgroup of index 2, $N = \langle \sigma, \rho^2 \rangle \cong C_2 \times C_4$. After finding the fixed field of G_2, we will have finished the computation.

5.1.1 The Fixed Field of H_1

Let $H_1 := \langle \sigma, \rho^4 \rangle$. Note that in the specified representation $\rho^4 = -I$. First focusing on σ, we see that we want to group x_1 with x_2 and x_3 with x_4 since each couple shares a sign under the action. So x_1x_2 and x_3x_4 are fixed by both σ and ρ^4, but we also should have all the squares x_i^2. For convenience we choose to add $x_2x_1^{-1}$ and $x_4x_3^{-1}$.

Lemma 5.2. $k(x_1x_2, x_3x_4, x_2x_1^{-1}, x_4x_3^{-1}) = k(x_1, x_2, x_3, x_4)^{H_1}$.

Proof. First we check explicitly that our proposed field is fixed by the action H_1.

$$\sigma : (x_1x_2, x_3x_4, x_2x_1^{-1}, x_4x_3^{-1}) \longmapsto (x_1x_2, (-x_3)(-x_4), x_2x_1^{-1}, (-x_4)(-x_3)^{-1}).$$
$$\rho^4 : (x_1x_2, x_3x_4, x_2x_1^{-1}, x_4x_3^{-1}) \mapsto ((-x_1)(-x_2), (-x_3)(-x_4), (-x_2)(-x_1)^{-1}, (-x_4)(-x_3)^{-1}).$$

So indeed $k(x_1x_2, x_3x_4, x_2x_1^{-1}, x_4x_3^{-1}) \subseteq k(x_1, x_2, x_3, x_4)^{H_1}$. To see that equality holds, it suffices to check that $k(x_1, x_2, x_3, x_4)/k(x_1x_2, x_3x_4, x_2x_1^{-1}, x_4x_3^{-1})$ is an extension with group H_1. We note that $(T^2 - x_1x_2(x_2x_1^{-1}))(T^2 - x_3x_4(x_4x_3^{-1}))$ has roots $\pm x_2$ and $\pm x_4$, and thus the splitting field has group V_4 (changing the signs of the roots). Furthermore $k(x_1x_2, x_3x_4, x_2x_1^{-1}, x_4x_3^{-1})(x_2, x_4) = k(x_1, x_2, x_3, x_4)$. □

We relabel indeterminates to avoid index overload.

$$t_1 := x_1x_2, \quad t_2 := x_3x_4, \quad t_3 := x_2x_1^{-1}, \quad t_4 := x_4x_3^{-1}.$$

The action of ρ is now of order four (generating $G_1 = G/H_1$) on $k(t_1, t_2, t_3, t_4)$:

$$\rho : (t_1, t_2, t_3, t_4) \longmapsto (-t_2, t_1, -t_4^{-1}, t_3).$$

5.1.2 Eliminating t_1 and t_2

At this point one notices that we no longer are dealing with a linear action, so finding an invariant basis is going to get sticky. One notices however that G_1 continues to act linearly on $k(t_1, t_2)$, so we would hope to first deal with these. Indeed if we let $L = k(t_3, t_4)$ then we can think of $k(t_1, t_2, t_3, t_4)$ as a two dimensional vector space over L, i.e. $k(t_1, t_2, t_3, t_4) \cong Lt_1 + Lt_2$. The action of G_1 on this, as a vector space, is now semi-linear, i.e. $\rho(wt_1 + zt_2) = \rho(w)\rho(t_1) + \rho(z)\rho(t_2)$. We would like to say that we can pick a new basis of this space that is preserved by ρ. We have the following lemma from classical invariant theory.

Lemma 5.3. *[6, Invariant Basis Lemma] Let M/K be a finite Galois extension with group G, and let W be a finite-dimensional M-vector space on which G acts semi-linearly. Then W has an M-basis invariant under G.*

In our instance we let $k(t_3, t_4)/k(t_3, t_4)^{G_1}$ to be M/K and $W = k(t_3, t_4)t_1 + k(t_3, t_4)t_2$. The proof of the lemma provides a method of constructing the basis. Given a representation r there is a matrix $B = \sum_\rho r(\rho)\rho(C)$ (where C is some invertible matrix that exists due to

Hilbert's Theorem 90 [11]) such that B applied to the basis gives an invariant basis. In our instance we know that

$$r(\rho) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ and let } C = \begin{pmatrix} t_3 & 0 \\ 0 & t_3 \end{pmatrix}.$$

The importance of C is only that B be invertible; it is otherwise arbitrary.

Corollary 5.4. *$v_1 = (t_3^{-1} + t_3)t_1 + (t_4^{-1} + t_4)t_2$ and $v_2 = (-t_4^{-1} - t_4)t_1 + (t_3^{-1} + t_3)t_2$ are a G_1 invariant L-basis of W.*

Proof. We directly apply the construction given in the proof of Lemma 5.3 in [6, p. 21].

$$B = \sum_{i=0}^{3} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^i \rho^i(t_3) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} (t_3^{-1} + t_3) & (t_4^{-1} + t_4) \\ (-t_4^{-1} - t_4) & (t_3^{-1} + t_3) \end{pmatrix}.$$

□

It is now clear that $k(t_1, t_2, t_3, t_4)^{G_1} = L^{G_1}(v_1, v_2)$, and after the following corollary we will restrict our attention to the action of G_1 on $k(t_3, t_4)$.

Corollary 5.5. $k(t_1, t_2, t_3, t_4)^{G_1} = k(t_3, t_4)^{G_1}(v_1, v_2)$

5.1.3 The Fixed Field of H_2

$H_2 = \langle \rho^2 \rangle$, and ρ^2 acts on $k(t_3, t_4)$ as follows

$$\rho^2 : (t_3, t_4) \longmapsto (-t_3^{-1}, -t_4^{-1}).$$

We proceed by finding a spanning set for $k(t_3, t_4)^{H_2}$ and refining that to a basis.

Lemma 5.6. *$k(t_3, t_4)^{H_2}$ is generated by $\{t_3 - t_3^{-1}, t_4 - t_4^{-1}, (t_3 + t_3^{-1})(t_4 + t_4^{-1})\}$*

Proof. First we explicitly check that the field generated above is contained in $k(t_3, t_4)^{H_2}$. The first two elements are the traces of t_3 and t_4 respectively and thus contained in the fixed field. Also ρ^2 fixes $(t_3 + t_3^{-1})(t_4 + t_4^{-1})$, since

$$\rho^2 : (t_3 + t_3^{-1})(t_4 + t_4^{-1}) \mapsto (-t_3^{-1} + -t_3)(-t_4^{-1} + -t_4).$$

Note that $k(t_3, t_4)/k(t_3, t_4)^{H_2}$ is a degree two extension. However $k(t_3, t_4)/k(t_3 - t_3^{-1}, t_4 - t_4^{-1})$ is degree four, since the following polynomial of degree four defines the extension:

$$p(X) = (X^2 - (t_3 - t_3^{-1})X - 1)(X^2 - (t_4 - t_4^{-1})X - 1).$$

So $k(t_1, t_2)^{H_2}$ is the intermediate extension of degree two. Let q be as follows.

$$q(X) = X^2 - ((t_3 - t_3^{-1})^2 + 4)((t_4 - t_4^{-1})^2 + 4).$$

One sees that q has $(t_3 + t_3^{-1})(t_4 + t_4^{-1})$ as a root, and so

$$[k(t_3 - t_3^{-1}, t_4 - t_4^{-1}, (t_3 + t_3^{-1})(t_4 + t_4^{-1})) : k(t_3 - t_3^{-1}, t_4 - t_4^{-1})] = 2.$$

Thus $k(t_3 - t_3^{-1}, t_4 - t_4^{-1}, (t_3 + t_3^{-1})(t_4 + t_4^{-1})) = k(t_3, t_4)^{H_2}$. □

Note however that this set is not a transcendence basis since q is an algebraic relation between the three. Now we begin the process of finding a basis from this set. To prevent confusion, we relabel indeterminates again.

$$a_1 = t_3 - t_3^{-1}, \quad a_2 = t_4 - t_4^{-1}, \quad a_3 = (t_3 + t_3^{-1})(t_4 + t_4^{-1}).$$

We have the following algebraic relation between the three given by q.

$$a_3^2 - (a_1^2 + 4)(a_2^2 + 4) = 0.$$

We may think of this as a conic over $k(a_1)$ in the variables a_2 and a_3. From a trick of geometry we know that we can parameterize conics with a single variable. We do so by parameterizing the projection onto the a_2-axis. We pick the obvious rational point $(a_1, a_1^2 + 4)$. Now we parameterize the line between this point and an arbitrary point $(2z, 0)$ ($2z$ is chosen for ease in later computation) on the a_2-axis.

$$l(t) = (1 - t)(a_1, a_1^2 + 4) + t(2z, 0).$$

The nontrivial intersection of this line with the conic should give a single generator of $k(a_1)(a_2, a_3)$. So one solves the following in terms of t.

$$(l(t)_2)^2 - ((l(t)_1)^2 + 4)(a_2^2 + 4) = 0.$$

One finds that $t = 0$ or $t = (2 + a_1 z)(1 + a_1 z - z^2)^{-1}$. Now we plug this t back into $l(t)$ to get a new generic point on the conic.

$$(a_2, a_3) = \left(-\frac{-a_1 + 4z + a_1 z^2}{-1 - a_1 z + z^2}, -\frac{(4 + a_1^2)(1 + z^2)}{a + a_1 z - z^2} \right).$$

This proves the following claim.

Lemma 5.7. $k(t_3, t_4)^{H_2} = k(a_1, z)$.

We now want to put this back in terms of t_1 and t_2, to define the action of ρ on z and a_1. To solve for z in these terms we set the a_3 component of the above generic point equal to the definition of a_3 and solve for z:

$$-\frac{(4 + a_2^2)(1 + z^2)}{a + a_2 z - z^2} = (t_3 + t_3^{-1})(t_4 + t_4^{-1}).$$

One finds that there is a choice of two solutions; we pick the following.

$$a_1 = (t_3 - t_3^{-1}), \quad z = \frac{-t_3 - t_4}{-1 + t_3 t_4}.$$

5.1.4 The Fixed Field of G_2

Since we have found the fixed field of H_2 we may now consider the action of $G_2 = G_1/H_2$. Finding $k(a_1, z)^{G_2}$ will complete the computation of $k(x_1, x_2, x_3, x_4)^{\Gamma_3}$.

Note that ρ now acts with order two on a_1 and z as follows:

$$\rho : (a_1, z) \longmapsto \left(\frac{(z^2-1)a_1 + 4z}{za_1 + (1-z^2)}, -z^{-1} \right).$$

The action of ρ on a_1 is relatively complicated compared to the action on z, but it is just the Möbius transformation corresponding to the following class in $\mathrm{PGL}_2(k(z))$.

$$\begin{bmatrix} (z^2-1) & 4z \\ z & (1-z^2) \end{bmatrix} \sim \begin{bmatrix} -(1+z^2) & 0 \\ 0 & (1+z^2) \end{bmatrix}.$$

This diagonalized matrix's companion matrix applied to a_1 (as a Möbius transformation) will give a new basis element that ρ will act on nicely. For aesthetic purpose, let $z := z_1$, then let

$$z_2 := \begin{bmatrix} -\frac{2}{z_1} & 2z_1 \\ 1 & 1 \end{bmatrix} (a_1) = -\frac{(a_1 - 2z_1)z_1}{2 + a_1 z_1}.$$

Now one can see that $\rho(z_2) = -z_2^{-1}$, and z_2 and z_1 are still a basis of $k(t_1, t_2)^{H_2}$.

The question now is to find a basis for $k(z_1, z_2)^{G_2}$. We have that $G_2 = \langle \rho \rangle$ and $\rho(z_1, z_2) = (-z_1^{-1}, -z_2^{-1})$. But this is completely analogous to §5.1.3, only with the symbols (t_1, t_2) replaced by (z_1, z_2). So, we have already symbolically found a basis of the fixed field, and it is given by a_1 and z with the substitutions of $(t_3, t_4) \mapsto (z_1, z_2)$.

$$w_1 = z_1 - z_1^{-1}, \quad w_2 = \frac{-z_1 - z_2}{z_1 z_2 - 1}.$$

Corollary 5.8. $k(a_1, z)^{G_2} = k(w_1, w_2)$.

5.1.5 The Fixed Field of Γ_3

Combining all of our efforts thus far, we remember that $k(t_1, t_2, t_3, t_4)^{\Gamma_3} = k(t_3, t_4)^{G_1} v_1 + k(t_3, t_4)^{G_1} v_2$. Along with the conclusion of Corollary 5.8 we have shown the following.

Theorem 5.9. $k(x_1, x_2, x_3, x_4)^{\Gamma_3} = k(v_1, v_2, w_1, w_2)$.

Peeling back the various substitution, v_1, v_2, w_1, w_2 can be written in terms of x_1, x_2, x_3, x_4 as follows.

$$v_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2$$
$$v_2 = \frac{x_1x_2x_3}{x_4} + \frac{x_1x_2x_4}{x_3} - \frac{x_1x_3x_4}{x_2} - \frac{x_2x_3x_4}{x_1}$$
$$w_1 = \frac{-4x_1x_2x_3x_4 + x_1^2(x_3^2 - x_4^2) + x_2^2(-x_3^2 + x_4^2)}{(x_2x_3 + x_1x_4)(-x_1x_3 + x_2x_4)}$$
$$w_2 = -\frac{(x_2x_3 + x_1x_4)(x_1x_3 - x_2x_4)(x_2(-x_3 + x_4) + x_1(x_3 + x_4))}{x_1^3x_3x_4(-x_3 + x_4) + x_2^3x_3x_4(x_3 + x_4) + x_1x_2^2(x_3^3 - 2x_3^2x_4 + 2x_3x_4^2 - x_4^3) + x_1^2x_2(x_3^3 + 2x_3^2x_4 + 2x_3x_4^2 + x_4^3)}$$

5.2 A Generic Polynomial of Γ_3 in Four Parameters

To apply Theorem 2.4 we need only to choose a Γ_3-stable subset $\mathcal{M}$ that satisfies $k(x_1, x_2, x_3, x_4)^{\Gamma_3}(\mathcal{M}) = k(x_1, x_2, x_3, x_4)$. The easiest choice is the set generated by $\{x_1, x_2, x_3, x_4\}$ under the action of Γ_3. This is just $\mathcal{M} = \{\pm x_1, \pm x_2, \pm x_3, \pm x_4\}$. Then we let f be as follows.

$$f(T) = \prod_{i=1}^{4}(T^2 - x_i^2).$$

This polynomial can be written in terms of the functions $k(v_1, v_2, w_1, w_2)$. Actually computing such a polynomial is not feasible due to the complexity of the fixed field, however we do have the following existence theorem.

Theorem 5.10. *There exists an even, degree 8 generic polynomial $g(T) \in k(v_1, v_2, w_1, w_2)[T]$ for M_{16} in four parameters over k.*

5.2.1 The Minimality of g

We have answered the generic polynomial problem for Γ_3 by answering the Noether problem. Since Γ_3 is a permutation group of degree 8, g has the minimal degree, and we will conclude that g also has the least number of parameters.

Theorem 5.11. *$ed_{\mathbb{Q}}(\Gamma_3) = gd_{\mathbb{Q}}(\Gamma_3) = 4$.*

Proof. We apply Theorem 3.8 to Γ_3 over $\mathbb{Q}$. Indeed, Γ_3 is a 2-group, and $\mathbb{Q}$ contains the square roots of unity. Thus $\mathrm{ed}_{\mathbb{Q}}(\Gamma_3)$ is the least degree of a faithful representation of Γ_3 over $\mathbb{Q}$. This is known to be 4. So by Lemma 2.6, $4 = \mathrm{ed}_{\mathbb{Q}}(\Gamma_3) \leq \mathrm{gd}_{\mathbb{Q}}(\Gamma_3) \leq 4$. $\square$

References

[1] Arnaud Beauville. p-elementary subgroups of the Cremona group. *J. Algebra*, 314(2):553–564, 2007.

[2] Grégory Berhuy and Giordano Favi. Essential dimension: a functorial point of view (after A. Merkurjev). *Doc. Math.*, 8:279–330 (electronic), 2003.

[3] Garret Birkhoff. *Lattice Theory*, volume 25 of *American Mathematical Society Colloquium Publications*. Harvard University Press, Cambridge, 1999.

[4] S. Garibaldi, A. Markurjev, and J-P. Serre. Cohomological invariants in galois cohomology. 28, 2003.

[5] W. Gröbner. Minimalbasis der Quaternionengruppe. *Monatsh. Math. Phys.*, 41(1):78–84, 1934.

[6] Christian U. Jensen, Arne Ledet, and Noriko Yui. *Generic polynomials*, volume 45 of *Mathematical Sciences Research Institute Publications*. Cambridge University Press, Cambridge, 2002.

[7] M. C. Kang. Essential dimensions of finite groups. *ArXiv Mathematics e-prints*, November 2006.

[8] M.-c. Kang and J. Zhou. Noether's problem for $\hat{S}_4$ and $\hat{S}_5$. *ArXiv e-prints*, June 2010.

[9] Nikita A. Karpenko, Alexander, and S. Merkurjev. Essential dimension of finite p-groups. *Inventiones Math*, pages 491–508, 2008.

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

[11] Arne Ledet. Generic polynomials for quasi-dihedral, dihedral and modular extensions of order 16. *Proceedings of the American Mathematical Society*, 128(8):2213–2221, 1999.

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

[13] Yūichi Rikuna. The existence of a generic polynomial for SL(2,3) over Q. *Murorran Number Theory Assembly*, 3(4), 2004.

[14] R. G. Swan. Invariant rational functions and a problem of steenrod. *Invent. Math.*, (7):148–158, 1969.