

## Extension of Constants, Rigidity and the Chowla-Zassenhaus Conjecture

MICHAEL D. FRIED

ABSTRACT. Let  $f \in \mathbb{Q}[y]$  be a polynomial of degree  $n$  over the rationals. Assume  $f$  is *indecomposable* and consider the splitting field  $\Omega_f$  of  $f(y) - x$  over  $\mathbb{Q}(x)$ . Denote the constants of  $\Omega_f$  by  $\hat{\mathbb{Q}}_f$ . Then,  $\hat{\mathbb{Q}}_f \subset \mathbb{Q}(\zeta_n)$  where  $\zeta_n$  is a primitive  $n$ -th root of 1. When  $n = p$ , a prime, and  $f = x^p$  (cyclic polynomial), then  $\hat{\mathbb{Q}}_f = \mathbb{Q}(\zeta_p)$ . When  $f = T_p$ , the  $p$ -th Chebychev polynomial, then  $\hat{\mathbb{Q}}_f = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Cohen raised the following question. If  $\hat{\mathbb{Q}}_f$  is nontrivial ( $f$  has nontrivial extension of constants), is it then true that  $f$  is linearly equivalent over  $\bar{\mathbb{Q}}$  to a cyclic or Chebychev polynomial. We show this is false for each non-square odd integer  $n$ . This uses elementary group theory and the *Branch Cycle Argument*. Such  $f$  also give counterexamples to a conjecture of Chowla-Zassenhaus: For infinitely many  $p$ , there is no  $b \in \mathbb{F}_p$  so that  $f(x) - b$  is irreducible over  $\mathbb{F}_p$ . Also, for these  $p$ , there is no  $b \in \mathbb{F}_p$  so that  $f(x) - b$  splits completely over  $\mathbb{Z}/p$ . Further, using Müller's classification of geometric monodromy groups of polynomials we show  $n$  must be odd for such counterexamples. These are  $(A_n, S_n)$  *realizations* by polynomials over  $\mathbb{Q}$ . More delicate examples from §4 require *rigidity* applied to non-Galois covers. These contrast the arithmetic of covers with and without using *braid operations* on branch cycle descriptions. Braid operations appear only in Ex. 4.7 describing four families of covers that include the renowned *Davenport polynomials* of degree 7.

Basic tools for analyzing properties of a polynomial  $f : \mathbb{C}\mathbb{U}\{\infty\} \rightarrow \mathbb{C}\mathbb{U}\{\infty\}$  by  $x \mapsto f(x)$  appear in §1. This includes reminders of Riemann's existence theorem

---

1991 *Mathematics Subject Classification*. Primary 12E20, 12E25, 12F12; Secondary 11G20, 11G25, 11G35, 11R58, 11T71.

Supported by NSA grant #MSPR-129-90, NSF #DMS-99305590 and partly written while enjoying two weeks of intellectual hospitality at the U. of Florida Math. Dept.

Gary Mullen reminded me of Cohen's question at the IMA conference in July, 1994 on finite fields. I showed him Prop. 2.2 there. [GM] notes the necessity of taking  $f$  to be indecomposable in these questions to avoid easy counterexamples from composing  $f$  from linear changes of cyclic and Chebychev polynomials. John Thompson responded to the partition question arising in Ex. 4.4 with the recently written [RT].

and some perturbations of the *Branch Cycle Argument*. We clarify the use of the latter for non-Galois covers and applications to forms of *rigidity* in §3. For each odd, non-square integer  $n > 3$ , Prop. 2.2 gives counterexamples to Cohen's question, and so to the Chowla-Zassenhaus conjecture (Finite Field App. 3.2) by reduction modulo suitable primes  $p$ . These examples are polynomials over  $\mathbb{Q}$  whose *geometric monodromy group* is the alternating group  $A_n$ , but whose *arithmetic monodromy group* is  $S_n$  (see §1). Call this an  $(A_n, S_n)$  realization over  $\mathbb{Q}$ . With no loss for computation of arithmetic and geometric monodromy groups, take  $f$  monic. This can simplify notation. From Hilbert's time, many have considered realizing alternating groups as Galois groups of regular extensions of  $\mathbb{Q}$ . For example, [Se, §9.2] uses Mestre's examples [Me] to realize the *spin group cover* of  $A_n$ .

The present paper considers a subtle complement of this problem: Find degree  $n$  extensions  $L/\mathbb{Q}(x)$  with the constants of  $L$  equal to  $\mathbb{Q}$ , giving an  $(A_n, S_n)$  realization. We only consider the sub-case where  $L$  is of genus zero and it has a totally ramified place over  $\mathbb{Q}(x)$ . Prop. 2.2 and Ex. 4.3 use little theory. We show, however, why a classification of  $f \in \mathbb{Q}[y]$  (by their *branch cycles* as in §1) giving  $(A_n, S_n)$  realizations is probably very difficult. It requires forms of *rigidity* and its generalizations. §4 lists examples, more challenging than Prop. 2.2, in increasing difficulty and historical interest. Still, they display practical tools for the arithmetic of covers.

Prop. 2.2 doesn't work when  $n$  is an odd square. Ex. 4.4 discusses alternative approaches to Prop. 2.2 in this case using irrational conjugacy classes other than the  $n$ -cycle. These don't produce  $(A_n, S_n)$  realizations, for example, when  $n = 9$ . This is evidence they may not exist when  $n$  is an odd square. Ex. 4.5 is a three branch point cover where the transitivity assumption for rigidity fails. This gives polynomials where the *cyclotomic character*, via the *Branch Cycle argument* of §1, doesn't correctly identify their field of definition.

Finally, Ex. 4.7 contrasts two cases: all finite branch cycles are 3-cycles (Ex. 4.3); and all finite branch cycles are products of two disjoint 2-cycles. The former is almost trivial. For the latter, the first serious case,  $n = 7$ , is entirely nontrivial. We analyze this up to a mystery. Here there are four connected families of polynomials. Two pairs of families are conjugate over  $\mathbb{Q}(\sqrt{-7})$  and they have geometric monodromy group  $\mathrm{PSL}_3(\mathbb{Z}/2)$ . While this is a proper subgroup of  $A_7$ , we include this example as it hasn't been done before in the literature. Doing so illustrates how the method must contend with subgroups having generating conjugacy classes resembling those of the target group. See [Se, §7] or [Fr3, §5] for this event in Thompson's proof the Monster simple group is a Galois group over  $\mathbb{Q}$ . In Ex. 4.7, these produce families of polynomial pairs  $(f, g)$  of degree 7 over  $\mathbb{Q}(\sqrt{-7}) = K$ . This is the smallest degree for the following arithmetic phenomena: For almost all prime ideals of the ring of integers of  $K$ ,

$f$  and  $g$  have exactly the same ranges on the residue class fields of the prime ideal. Yet,  $f$  is indecomposable (§1) and not linearly related to  $g$  (even over  $\mathbb{C}$ ). Historical Remarks 4.2 tells the significance of there being only six such families with this arithmetic property. None have polynomial members defined over  $\mathbb{Q}$ .

In the second pair of families in Ex. 4.7, the polynomial members have geometric monodromy group  $A_7$ . Do polynomials in these families give  $(A_7, S_7)$  realizations? Ex. 4.7 shows the families are unirational varieties over a field  $K$  with  $[K : \mathbb{Q}] \leq 2$ . If  $[K : \mathbb{Q}] = 2$ , the families are conjugate and they produce no  $(A_7, S_7)$  realizations by polynomials over  $\mathbb{Q}$ . If, on the other hand,  $K = \mathbb{Q}$ , they produce many such realizations. We haven't yet found an explanation of which case occurs. Synopsis 4.9 has a short list of problems on  $(A_n, S_n)$  realizations we consider charming, challenging and likely to be helpful for other researchers.

This paper shows what you can do without using *Hurwitz spaces*. Still, as Ex. 4.7 shows, they afford more precise analysis. Rational function covers offer a variant on these problems with many known applications. There has been considerable work on the classification of (geometric) monodromy groups of rational functions [GT]. We expect general results similar to Müller's [M]. The gist: cyclic, elementary affine (in  $\mathbb{Z}/n \times^s (\mathbb{Z}/n)^*$ ), symmetric and alternating groups occur in abundance, but there should be only finitely many other monodromy groups of indecomposable rational functions. Inspecting arithmetic monodromy groups is more difficult. For rational functions, even dihedral group covers offer more difficult arithmetic than do polynomials [Fr3, §8].

*Comment on use of group theory.* In most notation for the action of groups on a set, this paper places group elements on the left of the elements of the set. For example, in §3,  $C_{\tau(i)}$  has  $\tau$  the symmetric group  $S_r$  on  $\{1, \dots, r\}$  acting on the left of the integer  $i$ . In, however, a group computation, we multiply from left to right, with action on the right of the set. Thus,  $(1\ 2\ 3)(1\ 3\ 4) = (1\ 2\ 4)$  takes 1 to 2, and not 1 to 1 as you would have with action on the left.

We often use Marggraf's Theorem from 1892 without explicitly citing it [Wi, p. 38, Th. 13.8]. It says a primitive group  $G$  of degree  $n$  containing a  $t$ -cycle with  $1 < t < n$  is  $n-t+1$ -fold transitive. If  $t \leq n/2$ , then  $G = A_n$  or  $S_n$ .

### §1. Basic field theory tools

Let  $F$  be an arbitrary subfield of  $\mathbb{C}$  and let  $\bar{F}$  be its algebraic closure. Suppose  $L/F(x)$  is a finite extension of degree  $n$ . We say  $L/F(x)$  is *regular* (over  $F$ ) if  $L \cap \bar{F} = F$ ; the constants of  $L$  are just  $F$ . Let  $\hat{L}/F(x)$  be its Galois closure: the least Galois extension of  $F(x)$  containing  $L$ . The featured extensions of this paper have  $L/F(x)$  regular, but  $\hat{L}/F(x)$  is not. Use  $\hat{F}_L$  to denote the constants  $\hat{L} \cap \bar{F}$  of  $\hat{L}$ . By acting on a primitive generator for  $L/F(x)$ ,  $\hat{G} = G(\hat{L}/F(x))$  faithfully embeds in  $S_n$  as a transitive subgroup. This embedding is unique up to conjugation of the image by an element of  $S_n$ .

The extension is *primitive* if the representation is primitive. This is equivalent to no group being properly between  $\hat{G}$  and the stabilizer  $\hat{G}(1)$  of the integer 1 in  $\hat{G}$ . From Galois theory, this means there are no fields properly between  $L$  and  $F(x)$ . If  $L = F(y)$ ,  $x = f(y)$  for some rational function  $f$ . Then,  $L/F(x)$  is primitive if and only if  $f$  is *indecomposable* over  $F$ :  $f(y) \neq f_1(f_2(y))$  for any  $f_1, f_2 \in F(y)$  with  $\deg(f_i) > 1$ ,  $i = 1, 2$ . Degree is as usual for rational functions, maximum of degrees of the numerator and denominator, when these are relatively prime. Polynomials are indecomposable over  $F$  (in characteristic 0), if and only if they are indecomposable over  $\bar{F}$ : we just say they are indecomposable [Fr5].

For any  $x' \in \bar{F} \cup \{\infty\}$ , denote formal Laurent series in  $x - x'$  by  $\bar{F}((x - x'))$ . Replace  $x - x'$  by  $1/x$  if  $x' = \infty$ . The algebraic closure of  $\bar{F}((x - x'))$  is  $\bigcup_{e=1}^{\infty} \bar{F}(((x - x')^{1/e}))$ . Thus, the absolute Galois group of  $\bar{F}((x - x'))$  is pro-cyclic. Its generator  $\sigma_{x'}$  maps  $(x - x')^{1/e}$  to  $\zeta_e(x - x')^{1/e}$ ,  $e = 2, 3, \dots$ . Here  $\zeta_e = e^{2\pi i/e}$ . Since  $\hat{L}\bar{F}((x - x'))/\bar{F}((x - x'))$  is Galois, there is a minimal integer  $e$  with  $\hat{L}$  embedding in  $\bar{F}(((x - x')^{1/e}))$  as the identity on  $\bar{F}(x)$ . Compose one embedding  $\psi_{x'} : \hat{L} \rightarrow \bar{F}(((x - x')^{1/e}))$  with an automorphism of  $\hat{L}$ , to get any other. So, restriction of  $\sigma_{x'}$  to  $\hat{L}$  defines a conjugacy class of elements in  $G(\hat{L}/\bar{F}(x)) = G$ .

Only finitely many  $x'$  have  $e = e_{x'} > 1$ . Label these  $\mathbf{x} = (x_1, \dots, x_r)$ , the *branch points* of the cover. If  $\psi_i$  is the embedding attached to  $x_i$ , name the corresponding automorphism  $\sigma_i$ . The  $r$ -tuple  $\mathbf{x}$  thus gives  $\mathbf{C} = (C_1, \dots, C_r)$ , an  $r$ -tuple of conjugacy classes in  $G$ , the *branch cycle* conjugacy classes of  $L/F(x)$ . We say  $x_i$  is *totally ramified* if  $\sigma_i$  is an  $n$ -cycle: conjugate in  $S_n$  to  $(12 \dots n)$ . Let  $e_i$ , the *ramification index* of  $x_i$ , be the  $e$  attached to  $x_i$ .

RIEMANN'S EXISTENCE THEOREM 1.1 [Se, Chap. 6]. We may choose  $\psi$ s,  $i = 1, \dots, r$ , so

- (i)  $\sigma_1 \cdots \sigma_r = 1$ , and
- (ii) the  $\sigma_i$ s generate (the transitive group)  $G$ .

Conversely, suppose  $x_1, \dots, x_r \in \bar{F}$  are distinct, and  $\sigma_1, \dots, \sigma_r \in S_n$  satisfy (i) and (ii) with  $G$  transitive in  $S_n$ . Then, there exists  $L/\bar{F}(x)$  producing this data as above. Such extensions, up to isomorphism over  $\bar{F}(x)$ , are in one-one association with  $\boldsymbol{\sigma} \in S_n^r$  satisfying (i) and (ii) up to conjugation by  $S_n$ .

An  $r$ -tuple arising from  $L/\bar{F}(x)$ , satisfying (i) and (ii), is a description of its *branch cycles*. Now we explain the *Branch Cycle Argument* from [Fr1, prelude to Th. 5.1]. Suppose  $L/\mathbb{Q}(x)$  is a regular extension. Let  $\hat{L}/\mathbb{Q}(x)$  be its Galois closure. Denote the constants of  $\hat{L}$  as  $\hat{\mathbb{Q}} = \hat{\mathbb{Q}}_L$ . The *arithmetic monodromy* group of  $L/\mathbb{Q}(x)$  is  $\hat{G} = G(\hat{L}/\mathbb{Q}(x))$ . Similarly, the *geometric monodromy* group is  $G = G(\hat{L}/\hat{\mathbb{Q}}(x))$ . Elements of  $G_{\mathbb{Q}}$ , the absolute Galois group of  $\mathbb{Q}$ , permute the branch points  $x_1, \dots, x_r$  of  $L/\mathbb{Q}(x)$ . This attaches a valuable permutation representation of  $G_{\mathbb{Q}}$  to  $L/\mathbb{Q}(x)$ .

Adjoin all roots of 1 to  $\mathbb{Q}$  to get  $\mathbb{Q}^{\text{yc}}$ . Let  $\tau \in G_{\mathbb{Q}}$  act on roots of 1 through

restriction:  $G_{\mathbb{Q}} \rightarrow G(\mathbb{Q}^{\text{cyc}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^*$ . Identify the image of  $\tau$  with a supernatural integer  $m_{\tau} \in \hat{\mathbb{Z}}^*$  from the invertible integers of the profinite completion of  $\mathbb{Z}$ . Also, use  $\tau$  for the action of  $\tau$  on  $x_1, \dots, x_r$  and so on  $C_1, \dots, C_r$ . Suppose  $\mathbf{C}' = (C'_1, \dots, C'_r)$  is a collection of conjugacy classes of  $G$ . Let the least common multiple of orders of all elements in  $\mathbf{C}'$  be  $N_{\mathbf{C}'} = N$ . We say  $\mathbf{C}'$  is a *rational union* if putting elements of  $C'_1 \cup \dots \cup C'_r$  to any power  $m$  prime to  $N$  gives the same set. Let  $G$  be a subgroup of  $H$ . Elements of a conjugacy class  $C$  of  $G$  define a unique conjugacy class in  $H$ . Denote this  $C^H$ . Take an embedding  $\hat{L} \subset \bar{\mathbb{Q}}(((x - x_i)^{1/e_i}))$ .

**BRANCH CYCLE ARGUMENT 1.2.** *Assumptions on  $L/\mathbb{Q}(x)$  and the  $x_i$ s are as above. The conjugacy classes  $C_i^{\hat{G}}$  and  $(C_{\tau(i)}^{m_{\tau}})^{\hat{G}}$ , in  $\hat{G}$ , are the same,  $i = 1, \dots, r$ . For each  $i$ , denote the union over  $\tau \in G_{\mathbb{Q}}$  of the conjugacy classes  $C_{\tau(i)}^{\hat{G}}$ , by  $\hat{C}(i)$ . Then,  $\hat{C}(i)$  is a rational union in  $\hat{G}$  for each  $i = 1, \dots, r$ . Further, consider  $\beta \in \hat{G}$  and  $\tau \in G_{\mathbb{Q}}$  whose restrictions to  $\hat{\mathbb{Q}}_L$  are equal. Then, with  $m = m_{\tau}$ , the conjugacy classes  $\beta C_i \beta^{-1}$  and  $C_{\tau(i)}^m$  of  $G$  are equal,  $i = 1, \dots, r$ .*

**AN ILLUSTRATIVE CASE.** Suppose  $x_1 \in \mathbb{Q}$ . Let  $m$  be an integer relatively prime to  $\text{ord}(\sigma_1)$ ,  $\sigma_1 \in C_1$ . The result says the  $m$ -th power of  $\sigma_1$  is conjugate to  $\sigma_1$  in  $\hat{G}$ . Here's why. Choose  $\tau \in G_{\mathbb{Q}}$  with  $\tau(\zeta_{e_1}) = \zeta_{e_1}^m$ . Apply  $\tau$  to the coefficients of elements in  $\bar{\mathbb{Q}}(((x - x_1)^{1/e_1}))$ . Restricting  $\tau$  to the image of an embedding of  $\hat{L}$  gives an automorphism of  $\hat{L}$ . Compute the action of conjugation by  $\tau$  on  $\sigma_1$ :

$$\tau \sigma_1 \tau^{-1}((x - x_1)^{1/e_1}) = \tau(\zeta_{e_1}(x - x_1)^{1/e_1}) = \zeta_{e_1}^m (x - x_1)^{1/e_1}.$$

It has the same effect as  $\sigma_1^m$ .

This leaves the statement on  $\beta \in \hat{G}$ . Consider the effect  $\beta$  has on the conjugacy class  $C_1$  in  $G$ . Since  $x_1 \in \mathbb{Q}$ ,  $\tau$  acts on Puiseux expansions around  $x_1$ . Thus,  $\tau$  determines a decomposition group element for a place of  $\hat{L}$  above  $x_1$ . Conclude from the first paragraph argument.  $\square$

The Branch Cycle Argument has a more general statement over any field  $F$ . The complication is keeping track of the intersection of  $F$  with  $\mathbb{Q}^{\text{cyc}}$ . Prop. 2.2 and the §4 examples show how to apply the Branch Cycle Argument.

## §2. Counterexamples to Cohen's question

The Branch Cycle Argument easily gives polynomial counterexamples to Cohen's conjecture for each squarefree, odd integer  $n$ . A reader interested only in such can read Prop. 2.1 and the first part of the proof of Prop. 2.2. These require little exposition. §4 describes many counterexamples, and it analyzes more difficult points characterizing when polynomials over  $\mathbb{Q}$  give  $(A_n, S_n)$ . Examples of the technique apply to many problems: [Fr2] and its applications to the

Schur conjecture for rational functions, and in [Fr6]. That we are investigating polynomials simplifies Prop. 2.2 and the examples of §4. The arithmetic theory of covers with more than three branch points requires considerable additions to *rigidity*. This accounts for the length of [Fr1], [FrV] and its antecedents, whose general goals include understanding the whole inverse Galois problem. There will soon be books ([MM] and [V]) that give complete treatment of many aspects of Riemann's existence theorem. This includes applications of braid group actions, which [Se] does not illustrate.

Let  $f \in \mathbb{Q}[y]$ . Then,  $f$  gives a map from  $\mathbb{P}_y^1 = \bar{\mathbb{Q}} \cup \infty \rightarrow \mathbb{P}_x^1$  by  $y \mapsto f(y) = x$ . Consider the *arithmetic* monodromy group  $G_f$  of  $f$ : the Galois group of the splitting field  $\Omega_f$  of  $f(y) - x$  over  $\mathbb{Q}(x)$ . Denote constants of  $\Omega_f$  by  $\hat{\mathbb{Q}}_f$  (or  $\hat{\mathbb{Q}}$  if the context is clear). Let  $x_1, \dots, x_r$  be the branch points of the map. Choose  $x_r$  to be  $\infty$ , for  $\infty$  is among the branch points. As in Riemann's existence theorem, let  $\sigma_1, \dots, \sigma_r$  be a corresponding description of the branch cycles. Proposition 2.1 applies to an  $n$ -cycle in the proof of Prop. 2.2. Ex. 4.4 uses the general case.

PROPOSITION 2.1. *Let  $L/\mathbb{Q}(x)$  be any regular extension of degree  $n$  with a branch point  $x_i \in \mathbb{Q}$ . As in §1,  $G(\hat{L}/\hat{\mathbb{Q}}_L(x)) = G$ , with  $\hat{\mathbb{Q}}_L$  the constants of  $\hat{L}$ . Let  $C_i$  be the conjugacy class in  $G$  corresponding to  $x_i$ . Suppose,  $C_i$  isn't rational in  $G$ . Then,  $\hat{\mathbb{Q}}_L \neq \mathbb{Q}$ . Now, assume  $C_i$  has this property.*

- (†)  $\sigma \in C_i$  has disjoint cycle form  $(m_1)(m_2) \cdots (m_t)$ , including  $m_i$  s equal 1.
- (‡)  $m_i \neq m_j$  for  $1 \leq i < j \leq t$ .

Then,  $\hat{\mathbb{Q}}_L \subset \mathbb{Q}(\zeta_m)$  where  $m$  is the least common multiple of  $m_1, \dots, m_t$ . In particular, with  $f$  as above and  $C_r$  not rational in  $G_f$ ,  $\hat{\mathbb{Q}}_f \cap \mathbb{Q}(\zeta_n) \neq \mathbb{Q}$ .

PROOF. To prove the first statement, apply Branch Cycle Argument 1.2 to the branch point  $x_i \in \mathbb{Q}$ . Conclusion: The conjugacy class of  $C_i$  is rational in  $\hat{G}$ . By assumption, it isn't rational in  $G$ . Therefore,  $G$  is a proper subgroup of  $\hat{G}$ . This concludes the first part.

Now assume  $C_i$  satisfies (†) and (‡). Each place of  $L$  above  $x_i$  corresponds to one disjoint cycle of the branch cycle for  $x_i$ . The place of the cycle of length  $m_j$  has ramification index  $m_j$ . Since  $x_i \in \mathbb{Q}$ ,  $G_{\mathbb{Q}}$  permutes the places above  $x_i$ . Action of  $G_{\mathbb{Q}}$  preserves the ramification indices. So, (‡) implies each of these places is also  $\mathbb{Q}$  rational. The place corresponding to the cycle of length  $m_j$  gives an embedding of  $L$  into  $\bar{\mathbb{Q}}(((x - x_i)^{1/m_j}))$ . Call the image field  $L_j$ . We show the Galois closure of  $L_j\mathbb{Q}(((x - x_i)^{1/m_j})/\mathbb{Q}(((x - x_i)^{1/m_j}))$  is actually into  $\mathbb{Q}(\zeta_{m_j})(((x - x_i)^{1/m_j}))$ . Then  $\hat{L}$  embeds in the composite,  $\mathbb{Q}(\zeta_m)((x - x_i)^{1/m})$ , of  $\mathbb{Q}(\zeta_{m_j})(((x - x_i)^{1/m_j})$ ,  $j = 1, \dots, t$ . The constants of this field extension are just  $\mathbb{Q}(\zeta_m)$ , so  $\hat{L}$  is a subfield of this. Our next statements use ramification theory [CaF, §1.6–§1.9].

With no loss we now assume  $L/\mathbb{Q}((x - x_i))$  totally ramifies. For our applications consider  $L = \mathbb{Q}(y)((1/x))$  with  $f(y) = a_0y^n + a_1y^{n-1} + \cdots + a_n = x$ .

We want the Puiseux expansions for  $y$  over  $x = \infty$ . The general case follows by taking a nonsingular model for  $L$  giving a cover of the  $x$ -line. Similarly, this has a local equation for each place over  $x_i$  defining the cover; exchange  $1/x$  for a Laurent series in  $x - x_i$ . (See Th. 1 of p. 29 and Cor. 1 of p. 32 of [CaF].)

In our case, expand  $y$  as a Laurent series in  $x_* = x/a_0$  of the form

$$y = y(x_*^{-1/n}) = x_*^{1/n} + b_0 + b_1 x_*^{-1/n} + b_2 x_*^{-2/n} + \dots$$

To see this, plug the formal expression for  $y$  into  $f(y) = x$ . Equate like terms in  $x_*^{-1/n}$  on both sides. Thus, inductively solve linear equations with coefficients in  $\mathbb{Q}$  for  $b_0, b_1, \dots$ . The other solutions of  $f(y) = x$  are  $y(\zeta_n^k x_*^{-1/n})$ ,  $k = 1, \dots, n$ .

Our notation is now set for the last conclusion of the proposition:  $\Omega_f$  embeds in  $\mathbb{Q}(\zeta_n)((x_*^{-1/n}))$ . The constants of this latter field are clearly  $\mathbb{Q}(\zeta_n)$ . Thus,  $\mathbb{Q}(\zeta_n)$  contains the constants of  $\Omega_f$ .  $\square$

Denote  $(12\dots n)$  by  $\sigma_\infty$ . An  $n$ -cycle is in  $A_n$  if and only if  $n$  is odd. Write  $n$  as  $\prod_{i=1}^t p_i^{u_i}$  with the  $p_i$ s distinct primes and the  $u_i$ s positive. Define:

$$M_n = \{k \in (\mathbb{Z}/n)^* \mid \sigma_\infty^k \text{ is conjugate to } \sigma_\infty \text{ in } A_n\}.$$

**IRRATIONAL CYCLE LEMMA.** *Suppose  $n > 4$  is odd. The conjugacy class of  $\sigma_\infty$  in  $S_n$  breaks into two conjugacy classes in  $A_n$ . Suppose  $n$  is not a square; there is a prime  $p_1 \mid n$  such that  $u_1$  is odd. Let  $k \in (\mathbb{Z}/n)^*$  have these properties: its image in  $(\mathbb{Z}/p_1^{u_1})^*$  is a generator of this cyclic group; and its image in  $(\mathbb{Z}/p_i^{u_i})^*$  is 1,  $i = 2, \dots, t$ . Then,  $\sigma_\infty^k$  isn't conjugate to  $\sigma_\infty$  in  $A_n$ . Conversely, if  $n$  is an odd square,  $\sigma_\infty^k$  is conjugate to  $\sigma_\infty$  in  $A_n$  for all  $k \in (\mathbb{Z}/n)^*$ . Let  $J$  be the integers from 1 to  $t$  with  $u_j$  odd. Denote  $\sqrt{\prod_{j \in J} (-1)^{(p_j-1)/2} p_j}$  by  $\alpha_n$ . For all odd  $n$ , the fixed field of  $M_n$  in  $\mathbb{Q}(\zeta_n)$  is  $\hat{\mathbb{Q}}_n = \mathbb{Q}(\alpha_n)$ .*

**PROOF.** In  $S_n$ , all  $n$ -cycles are conjugate. Since the centralizer of an  $n$ -cycle is exactly the powers of the  $n$ -cycle,  $\sigma_\infty$  isn't conjugate to  $(12)\sigma_\infty(12)$  in  $A_n$ . Thus, the conjugacy class of  $\sigma_\infty$  in  $S_n$  breaks into two conjugacy classes in  $A_n$ . With  $k$  in the statement, we show  $\sigma_\infty^k$  and  $\sigma_\infty$  aren't conjugate in  $A_n$ .

Note:  $\sigma_\infty^k$  maps  $i \mapsto i+k \pmod n$ ,  $i = 1, \dots, n$ . Multiplication by  $k$  gives a permutation  $\tau_k$  of the integers modulo  $n$ . Then,  $\tau_k \sigma_\infty \tau_k^{-1}$  equals  $\sigma_\infty^k$ :

$$\tau_k \sigma_\infty \tau_k^{-1}(ki) = \tau_k \sigma_\infty(i) = \tau_k(i+1) = ki + k.$$

We characterize those  $k$  with  $\tau_k$  not in  $A_n$ . Recall:  $(\mathbb{Z}/n)^* = \prod_{i=1}^t (\mathbb{Z}/p_i^{u_i})^*$ . So, it suffices to check if  $\tau_k \in A_n$  for  $k = \mathbf{k}_i = (1, \dots, 1, k_i, 1, \dots, 1)$ ; the only non-identity entry is  $k_i$ , a generator of the cyclic group  $(\mathbb{Z}/p_i^{u_i})^*$ , in the  $i$ -th position. Consider what happens with  $k$  equal  $(k_1, 1, \dots, 1)$ .

First, take the case  $t = 1$ ,  $u_1 = u$  and  $k_1 = k$ . Consider the cycle structure of  $\tau_k$  on the integers modulo  $p^u$ . Multiplication by  $k$  on integers of  $\mathbb{Z}/p^u$  exactly divisible by  $p^i$ ,  $i < u$ , gives one orbit of length  $p^{u-i} - p^{u-i-1}$ . For each  $i$  between

0 and  $u - 1$ , this cycle is of even length—not in  $A_n$ . (The orbit for  $i = u$  is of length 1.) Thus, the permutation is a product of  $u$  elements not in  $A_n$  (and it fixes exactly one integer). The total permutation from multiplication by  $k$  is in  $A_n$  if and only if  $u$  is even.

For the general case, write  $\mathbb{Z}/n$  as  $\mathbb{Z}/p_1^{u_1} \times \mathbb{Z}/n'$ . Multiplication by  $k$  is the identity on the second coordinate. Thus, it stabilizes each coset  $\mathbb{Z}/p_1^{u_1} \times k'$  with  $k' \in \mathbb{Z}/n'$ . In particular,  $\tau_k$  is the product of  $n'$  elements coming from the first case above. Thus,  $\tau_k \in A_n$  if and only if  $u_1$  is even. The converse comes by noting it suffices to check the elements  $\mathbf{k}_i$  above.

Finally, we identify the field  $\hat{\mathbb{Q}}_n$ . Identify the kernel of  $\mu : (\mathbb{Z}/n)^* \rightarrow \mathbb{Z}/2$  by  $k \in (\mathbb{Z}/n)^*$  maps to  $\tau_k \pmod{A_n}$ . In the above notation,  $\mathbf{k}_i$  goes to 1 if and only if  $i \in J$ . The unique quadratic extension of  $\mathbb{Q}$  inside  $\mathbb{Q}(\zeta_{p_j})$  is  $\mathbb{Q}\left(\sqrt{(-1)^{(p_j-1)/2}p_j}\right)$ . Conclude by noting the kernel of  $\mu$  is of index 2 in  $(\mathbb{Z}/n)^*$  and it fixes  $\alpha_n$ .  $\square$

We generalize the Irrational Cycle Lemma (ICL) for Ex. 4.4. For  $\sigma \in A_n$  of order  $m$ , define:

$$M_\sigma = \{k \in (\mathbb{Z}/m)^* \mid \sigma^k \text{ is conjugate to } \sigma \text{ in } A_n\}.$$

We say  $M_\sigma$  is nontrivial if the conjugacy class of  $\sigma$  in  $A_n$  isn't rational. That is, if  $M_\sigma$  is a proper subgroup of  $\mathbb{Z}/m$ .

Write  $m$  as  $\prod_{i=1}^s q_i^{v_i}$  with the  $q_i$ s distinct primes and the  $v_i$ s positive. Denote the maximal power of  $q_i$  dividing  $m_j$  by  $v_{i,j}$  and the vector  $(v_{i,1}, \dots, v_{i,t})$  by  $\mathbf{v}_i$ . Finally, let  $\mu : \mathbb{Z}^t \rightarrow \mathbb{Z}/2$  by  $(a_1, \dots, a_t) \mapsto \sum_{j=1}^t a_j \pmod{2}$ .

**IRRATIONAL CYCLE ADDENDUM.** Suppose  $n > 4$ . Denote the conjugacy class of  $\sigma \in S_n$  by  $C_\sigma$ . Display the disjoint cycle form of  $\sigma$  as  $(m_1) \cdots (m_t)$  as in (†) of Prop. 2.1. The following are equivalent.

- (\*\_1)  $C_\sigma$  breaks into two conjugacy classes in  $A_n$ .
- (\*\_2) The centralizer of  $\sigma$  in  $S_n$  lies entirely in  $A_n$ .
- (\*\_3) (†) of Prop. 2.1 holds ( $m_i \neq m_j$  for  $i \neq j$ ), and all the  $m_i$ s are odd.

Further,  $M_\sigma$  is nontrivial if and only if  $\mu(\mathbf{v}_i)$  is nonzero for some  $i$  between 1 and  $t$ . Let  $J$  be the integers from 1 to  $t$  with  $\mu(\mathbf{v}_i)$  nonzero. Denote  $\sqrt{\prod_{j \in J} (-1)^{(p_j-1)/2} p_j}$  by  $\alpha_\sigma$ . The fixed field in  $\mathbb{Q}(\zeta_m)$  of  $M_\sigma$  is  $\hat{\mathbb{Q}}_\sigma = \mathbb{Q}(\alpha_\sigma)$ .

**PROOF.** Equivalence of (\*<sub>1</sub>) and (\*<sub>2</sub>) is at the beginning of the proof of ICL. Now assume (\*<sub>2</sub>) holds. Suppose an  $m_i$  is even. Then, the cycle in  $\sigma$  corresponding to  $m_i$  commutes with  $\sigma$ . Since  $m_i$  is even, the cycle is not in  $A_n$ , contrary to (\*<sub>2</sub>). Suppose two of the  $m_i$ s, say  $m_1$  and  $m_2$ , are equal. Then, conjugate the  $m_1$ -cycle of  $\sigma$  to the  $m_2$ -cycle using a product  $\tau$  of  $m_1$  disjoint 2-cycles. Do this while leaving integers not in the support of these cycles fixed. Then,  $\tau$  commutes with  $\sigma$ . Since  $m_1$  is odd,  $\tau$  isn't in  $A_n$ . If (\*<sub>3</sub>) holds, (†) implies the disjoint



cycles of  $\sigma$  generate its centralizer. These cycles are of odd length. So, they are in  $A_n$ . Now we characterize when  $M_\sigma$  is nontrivial.

Let  $k$  be a generator of  $(\mathbb{Z}/q_i^{v_i})^*$ . As in ICL,  $k$  acts by multiplication on  $\bigoplus_{j=1}^t \mathbb{Z}/q_i^{v_i, j}$ . Identify  $k$  with a permutation  $\tau_k \in S_{V_i}$ , with  $V_i = \bigoplus_{j=1}^t q_i^{v_i, j}$ . The rest follows from ICL, if we show  $\tau_k$  is in  $A_n$  if and only if  $\mu(\mathbf{v}_i)$  is 0. For that, let  $\tau_k(j)$  be the corresponding permutation of  $\mathbb{Z}/q_i^{v_i, j}$ . From ICL, the  $j$ -th coordinate of  $\mathbf{v}_i$  is zero mod 2 if and only if  $\tau_k(j)$  is in  $A_n$ . Since  $\tau_k$  is the product of the  $\tau_k(j)$  s, it is in  $A_n$  exactly if  $\mu(\mathbf{v}_i)$  is 0. We are done.  $\square$

**PROPOSITION 2.2.** *Let  $n \geq 5$  be an odd integer. For  $x_1, x_2 \in \mathbb{Q}$  distinct, there exists a unique polynomial  $f \in \mathbb{Q}[y]$  (up to linear change of  $y$ ) with the following properties. Its branch points are  $x_1, x_2$  and  $x_3 = \infty$ . The corresponding branch cycles have  $\sigma_1$  a 3-cycle,  $\sigma_2$  an  $n-2$ -cycle and  $\sigma_3$  an  $n$ -cycle. Also,  $\Omega_f \cap \bar{\mathbb{Q}}$  is the field  $\hat{\mathbb{Q}}_n$  from the Irrational Cycle Lemma. If  $n$  is a nonsquare, the extension  $\mathbb{Q}(y)/\mathbb{Q}(x)$  with  $f(y) = x$  gives an  $(A_n, S_n)$  realization. If  $n$  is a square, then  $\mathbb{Q}(y)/\mathbb{Q}(x)$  gives an  $(A_n, A_n)$  realization.*

**PROOF OF EXISTENCE.** We give counterexamples to the Cohen question and Chowla-Zassenhaus conjecture (from the introduction; see Finite Field App. 3.2). To do this, produce examples  $f \in \mathbb{Q}[y]$  of the polynomials of Prop. 2.2. Take  $f$  to be any antiderivative in  $\mathbb{Q}[y]$  of  $g(y) = (y-a)^2 y^{n-3}$  with  $a \in \mathbb{Q}$ ,  $a \neq 0$ . Branch cycles for  $f$  over the finite branch points are a 3-cycle and an  $n-2$ -cycle. If  $G_f$  is  $A_n$ , apply Prop. 2.1 and the Irrational Cycle Lemma to conclude  $f$  gives an  $(A_n, S_n)$  realization when  $n$  is a nonsquare.

Since  $G_f$  contains a 3-cycle, if we show it is primitive we are done. Suppose not. It contains an  $n-2$ -cycle. Thus, any block of imprimitivity not supported entirely in the integers of the  $n-2$ -cycle must contain only two integers. The length, however, of this block divides  $n$ , contrary to  $n$  being odd. So, it is  $A_n$ , and the proof of existence of  $f$  is complete.  $\square$

The proof of the remainder of Prop. 2.2 is in §3. The proof of Prop. 2.1 produces automatic nontriviality of the constants of the Galois closure under the weaker assumptions of the next proposition. The easier half of [Fr1, Th. 5.1] is more general in allowing any field of definition and including information from all branch points. Let  $\{x_i, x_{i_2}, \dots, x_{i_k}\}$  be the orbit of  $x_i = x_{i_1}$  under  $G_{\mathbb{Q}}$ . Let  $e_i = e$  be the order of the elements in  $C_i$ , the conjugacy class in  $G$  attached to  $x_i$ . We define the *multiplier* of  $C_i$ :

$$M_i = \{m \in (\mathbb{Z}/e)^* \mid \bigcup_{j=1}^k C_{i_j}^m = \bigcup_{j=1}^k C_{i_j}\}.$$

Let  $\hat{\mathbb{Q}}_{L,i}$  be the fixed field in  $\mathbb{Q}(\zeta_e)$  of  $M_i$ . Use notation from Prop. 2.1.

**PROPOSITION 2.3.** *For each  $i = 1, \dots, r$ ,  $\hat{\mathbb{Q}}_L \supset \hat{\mathbb{Q}}_{L,i}$ .*

**REMARK 2.4.** *General extension of constants.* [FrV, Prop. 3] gives a fuller

story than Prop. 2.1 or Prop. 2.3 on extension of constants. Indeed, consider any pair  $(G, \hat{G})$  of transitive subgroups of  $S_n$ . Assume  $G \triangleleft \hat{G}$ , and the following:

- (2.1)  $G$  has no center; and
- (2.2) the centralizer of  $G$  in  $\hat{G}$  is trivial.

Then, there is a finite extension  $F$  of  $\mathbb{Q}$  and  $L/F(x)$  regular with  $G(\hat{L}/F(x)) = \hat{G}$  and  $G(\hat{L}/\hat{F}_L(x)) = G$ . In particular,  $[\hat{F}_L : F] = (\hat{G} : G)$ . Thus, extension of constants can be large even when each conjugacy class  $C_i$ ,  $i = 1, \dots, r$ , is rational in  $G$ . Note: Given (2.1), (2.2) is necessary so  $\hat{G}$  can be a Galois closure group. Explanation: This is a statement about the Galois closure process for an extension  $L/F(x)$  and not pure group theory. It is equivalent to the following. Consider elements  $\tau \in G(\hat{F}_L/F)$  that are images from  $\hat{G} = G(\hat{L}/F(x))$  of a  $\hat{\tau}$  for which conjugation on  $G$  by  $\hat{\tau}$  equals conjugation by  $\gamma \in G = G(\hat{L}/\hat{F}_L(x))$ . Since  $L/F(x)$  is regular, we may assume  $\hat{\tau}$  is fixed on  $L$ . As  $G$  has no center, given  $\hat{\tau}$ ,  $\gamma$  is unique. Such  $\tau$  form a subgroup  $H$  of  $G(\hat{F}_L/F)$ : (2.2) says  $H$  is trivial [Fr1, Prop. 2]. The argument there uses Weil's cocycle condition.

That is, the centralizer  $C_{\hat{G}}(G)$  of  $G$  in  $\hat{G}$  is a normal subgroup, disjoint from  $G$ . So, its fixed field in  $\hat{L}$  is Galois and contains  $L$ .  $\square$

Prop. 2.2 shows there are  $(A_n, S_n)$  realizations over  $\mathbb{Q}$  (for  $n$  odd and not a square) by taking the monodromy group of a polynomial over  $\mathbb{Q}$ . Remark 2.4 notes existence of general  $(G, \hat{G})$  realizations, except we may not achieve  $\mathbb{Q}$  as the field  $F$  of the realization. Recently we learned how to bound the genus (and number of branch points) of the function field  $L/F(x)$  giving the realization effectively. This also gives a bound on the degree of  $F$  over  $\mathbb{Q}$ .

### §3. Rigidity and completion of Prop. 2.2

This section discusses a *rigidity* criterion. It applies to complete the proof of Prop. 2.2. Finite Field Applic. 3.2 shows these  $(A_n, S_n)$  realizations from polynomials over  $\mathbb{Q}$  also give counterexamples to the Chowla-Zassenhaus conjecture. In §4 we look at other  $(A_n, S_n)$  realizations by polynomials. With a result of Müller, we show all counterexamples to Cohen's question are of odd degree and have  $A_n$  as geometric monodromy group.

[Fr1, Th. 5.1] gives a partial converse to the Branch Cycle Argument. It uses moduli spaces to consider extensions  $L/\mathbb{Q}(x)$  with a given pair  $(G, \hat{G})$  as arithmetic and geometric monodromy groups (§1). If  $[L : \mathbb{Q}(x)] = n$ , both  $G$  and  $\hat{G}$  are naturally subgroups of  $S_n$  with  $G$  normal in  $\hat{G}$ . For applications, start with  $G$  and conjugacy classes  $\mathbf{C} = (C_1, \dots, C_r)$  of generators  $(\sigma_1, \dots, \sigma_r) \in G^r$ .

We say we have a  $(G, H, \mathbf{C})$  realization over  $\mathbb{Q}$  if there is  $L/\mathbb{Q}(x)$  of degree  $n$  with these properties. The geometric (resp., arithmetic) monodromy group of  $L/\mathbb{Q}(x)$  is  $G$  (resp.,  $H$ ). Also, the geometric Galois closure  $\mathbb{Q}\hat{L}/\mathbb{Q}(x)$  has conjugacy class data  $\mathbf{C}$  in  $G$ . Given  $(G, \mathbf{C})$ , the Branch Cycle Argument shows

there is a natural group containing all possible groups  $H$ :

$$\hat{G}^{\mathbf{C}} = \{\beta \in S_n \mid \exists \tau \in S_r, m \in (\mathbb{Z}/N_{\mathbf{C}})^* \text{ with } \beta C_i \beta^{-1} = C_{\tau(i)}^m, i = 1, \dots, r\}.$$

Let  $H$  be a group between  $G$  and  $\hat{G}^{\mathbf{C}}$ . As before the Branch Cycle Argument, denote the conjugacy classes in  $H$  corresponding to  $\mathbf{C}$  by  $\mathbf{C}^H$ . Assume:

- (iii) <sub>$H$</sub>   $\mathbf{C}^H$  is a rational union of conjugacy classes in  $H$ ; and
- (iv)  $G$  has no center (so from (2.2), no element of  $H \setminus G$  centralizes  $G$ ).

The converse to the Branch Cycle Argument associates to  $(G, H, \mathbf{C})$  an algebraic set  $\mathcal{H}(G, H, \mathbf{C})$ . This has a natural unramified covering map to the space  $\mathbb{P}^r \setminus D_r$  of unordered distinct  $r$ -tuples of elements of  $\mathbb{P}^1$ . ([**FrV**] gives details.) The definition of  $\mathcal{H}(G, H, \mathbf{C})$  includes conjugation by  $H$  in the equivalence on  $r$ -tuples of branch cycles attached to  $\mathbf{C}$ . This is as in Riemann's Existence Theorem. From (iii) <sub>$H$</sub> ,  $\mathbb{Q}$  is a field of definition of  $\mathcal{H}(G, H, \mathbf{C})$  and its map to  $\mathbb{P}^r \setminus D_r$ : (iii) <sub>$H$</sub>  is necessary and sufficient for this.

Further, suppose  $G \leq H \leq H' \leq \hat{G}^{\mathbf{C}}$ . Then, there is a (finite) map

$$\Psi_{H, H'} : \mathcal{H}(G, H, \mathbf{C}) \rightarrow \mathcal{H}(G, H', \mathbf{C}).$$

If (iii) <sub>$H$</sub>  and (iii) <sub>$H'$</sub>  hold,  $\mathbb{Q}$  is also a field of definition for  $\Psi_{H, H'}$ . The next statement considers points  $\mathbf{p} \in \mathcal{H}(G, G, \mathbf{C})$ . Take  $V$  an absolutely irreducible component of  $\mathcal{H}(G, G, \mathbf{C})$  containing  $\mathbf{p}$ . Automatically—because  $\mathcal{H}(G, G, \mathbf{C})$  is a manifold— $\mathbb{Q}(\mathbf{p})$ , the field generated by the  $\mathbf{p}$  coordinates, contains the field of definition of  $V$ . Also,  $G(1)$  denotes the stabilizer in  $G \leq S_n$  of the integer 1.

CONVERSE OF BRANCH CYCLE ARGUMENT: [**Fr1**], [**FrV**]. Besides (iv), assume the embedding of  $G$  in  $S_n$  satisfies one of these:

- (v) it is the regular representation of  $G$ ; or
- (vi) the normalizer of  $G(1)$  in  $G$  is just  $G(1)$ .

Here is a diophantine condition equivalent to existence of a  $(G, H, \mathbf{C})$  realization,  $L/\mathbb{Q}(x)$  of degree  $n$ , over  $\mathbb{Q}$ . There is a point  $\mathbf{p} \in \mathcal{H}(G, G, \mathbf{C})$  whose image in  $\mathcal{H}(G, H, \mathbf{C})$  has coordinates in  $\mathbb{Q}$  and  $[\mathbb{Q}(\mathbf{p}) : \mathbb{Q}] = (H : G)$ . (Since the  $\mathcal{H}$ s are moduli spaces, this applies with any field  $K$  replacing  $\mathbb{Q}$ .)

The spaces  $\mathcal{H}$  are manifolds. Thus, they can't have rational points unless they have absolutely irreducible components over  $\mathbb{Q}$ . We now discuss a case of rigidity, a little more general than [**Se**, §7.3]. Any variant on rigidity not using braid group action, including this one, applies rarely unless  $r = 3$ . When  $r = 3$ , an  $\mathcal{H}$  is either  $(\mathbb{P}^1)^3$  with the fat diagonal removed, or a quotient of it by a subgroup of  $S_3$ . Trivially, these have a dense set of rational points. Ex. 4.7 gives practical ingredients for showing a space  $\mathcal{H}(G, H, \mathbf{C})$  is unirational when  $r = 4$ .

Take  $(C_1, C_2, C_3) = \mathbf{C}$  to be three conjugacy classes from  $G$ . Let  $\Sigma(\mathbf{C}^H)$  be the collection of  $\sigma = (\sigma_1, \sigma_2, \sigma_3) \in G^3$  where (i) and (ii) hold (§1) and  $\sigma_i \in C_i^H$ ,

$i = 1, 2, 3$ . Here  $h \in H$  acts on  $\Sigma(\mathbf{C}^H)$  by conjugation:

$$h\sigma h^{-1} = (h\sigma_1 h^{-1}, h\sigma_2 h^{-1}, h\sigma_3 h^{-1}).$$

**RIGIDITY CONDITION.** Assume  $(G, H, \mathbf{C})$  satisfies (iii)<sub>H</sub> and (iv). Then,  $(G, H, \mathbf{C})$ -rigidity holds if  $H$  is transitive on  $\Sigma(\mathbf{C}^H)$ . For  $r > 3$ , [Fr1, Th. 5.1] and [FrV] generalize transitivity of  $G$  with *braid transitivity*. This is transitivity of the combined action of the Artin braid group and  $H$  on the set analogous to  $\Sigma(\mathbf{C}^H)$  (see Ex. 4.7).

Turn the definition of  $\hat{G}^{\mathbf{C}}$  upside down to produce the group of a valuable cyclotomic field. Consider  $H$  with  $G \leq H \leq \hat{G}^{\mathbf{C}}$ . Recall  $N_{\mathbf{C}}$  and define:

$$M_H = \{m \in (\mathbb{Z}/N_{\mathbf{C}})^* \mid \exists \tau \in S_r, \exists \beta \in H \text{ with } \beta C_i \beta^{-1} = C_{\tau(i)}^m, i = 1, \dots, r\}.$$

**RIDIGITY RESULTS 3.1.** Assume  $(G, G, \mathbf{C})$ -Rigidity and (v) hold. Then, there is a regular extension  $\hat{L}/\mathbb{Q}(x)$  with Galois group  $G$ . More generally, suppose  $(G, H, \mathbf{C})$ -Rigidity and either (v) or (vi) hold. Then, there is an extension  $L/\mathbb{Q}(x)$  giving a  $(G, H', \mathbf{C})$  realization over  $\mathbb{Q}$  with  $G \leq H' \leq H$ . Further,  $\hat{L} \cap \mathbb{Q} = \hat{\mathbb{Q}}$  contains the fixed field in  $\mathbb{Q}(\zeta_{N_{\mathbf{C}}})$  of  $M_H$ .

Suppose  $(G, G, \mathbf{C})$ -rigidity and (vi) hold. Replace the representation giving (vi) with the regular representation to give (v). Given the conclusion of the Rigidity Results, take the fixed field of  $G(1)$  in the resulting extension. Thus, recover existence of the degree  $n$  extension giving the prescribed Galois closure. Conclude: The first statement of the Rigidity Results is equivalent to the statement with (vi) replacing (v).

**PROOF THAT PROPOSITION 2.2 ILLUSTRATES RIGIDITY.** After Prop. 2.2 we constructed polynomial counterexamples to Cohen's question. The simple ramification properties of these polynomials made them easy to work with. Here, however, we redo that argument, illustrating rigidity. This gives something new when  $n$  is a square.

Let  $n > 3$  be an odd integer. Suppose  $\mathbf{C}^{S_n}$  are the conjugacy classes, in  $S_n$ , of the triple  $(\sigma_1, \sigma_2, \sigma_3) \in A_n^3$  with  $\sigma_1 = (123)$ ,  $\sigma_2 = (145 \dots n)$  and  $\sigma_3 = (12 \dots n)^{-1}$ . Our previous argument showed such elements generate  $A_n$ . We show any other triple from  $\Sigma(\mathbf{C}^{S_n})$  is conjugate to this under  $S_n$ .

With no loss take such a triple to be  $\tau = (\tau_1, \tau_2, \tau_3)$  with  $\tau_3 = \sigma_3$ . Conjugating by a power of  $\sigma_3$  assures the common integer in the 3-cycles  $\tau_1$  and  $\tau_2$  is one. Product condition (i) now detects the  $\tau$ s equal to the  $\sigma$ s.

When  $n$  is a nonsquare, conclude the following from Rigidity Results 3.1. There is a degree  $n$  cover unique (up to equivalence),  $\phi: X \rightarrow \mathbb{P}^1$ , having these branch cycles, defined over  $\mathbb{Q}$  with  $x_1, x_2$  and  $\infty$  as branch points. It realizes the monodromy group pair  $(A_n, S_n)$ . With  $H = S_n$ , the Irrational Cycle Lemma

says the subgroup  $M_H$  of  $(\mathbb{Z}/n)^*$  equals  $M_n$ . Thus, it produces  $L/\mathbb{Q}(x)$  with  $\hat{\mathbb{Q}}_L = \hat{\mathbb{Q}}_n$ . The Riemann-Hurwitz formula gives its genus as  $g$  with

$$2(n + g - 1) = 2 + n - 3 + n - 1 = 2(n - 1).$$

So,  $g = 0$  and the point over  $\infty$  totally ramifies. A polynomial map gives this.

Now let  $n > 5$  be an odd square. The Irrational Cycle Lemma shows both conjugacy classes of  $n$ -cycles in  $A_n$  are rational. Therefore, so are all the classes of  $\mathbf{C}$ . The argument above, with  $H = A_n$  replacing  $H = S_n$  shows the hypotheses of the Rigidity Results 3.1 hold. Thus, we get an  $(A_n, A_n)$  realization over  $\mathbb{Q}$ . I've never seen these alternating group realizations in the literature.  $\square$

We use the examples of Prop. 2.2 (and §4) to answer questions over finite fields. These require analogs of the Chebotarev density theorem. See the examples of [FrJ, §19.6] and references there for details and other examples. Consider  $f \in F[y]$ . The geometric monodromy group of  $f : \mathbb{C} \cup \{\infty\} \rightarrow \mathbb{C} \cup \{\infty\}$  contains a uniquely defined conjugacy class of  $n$ -cycles from ramification over  $\infty$  (proof of Prop. 2.1). Denote this class by  $C_\infty$ . We often choose it as the last conjugacy class  $C_r$  in a branch cycle description.

We may apply the Branch Cycle Argument to any tamely ramified cover over any perfect field  $F$ . To illustrate the adjustments let  $F \subset \mathbb{C}$ . Consider

$$M_{F,n} = G(F(\zeta_n)/F) = G(\mathbb{Q}(\zeta_n)/F \cap \mathbb{Q}(\zeta_n))$$

as a subgroup of  $(\mathbb{Z}/n)^*$ . Apply the Branch Cycle Argument (over  $F$ ) to a regular field extension  $L/F(x)$ , totally ramified over infinity. (Notation for  $\hat{L}$ ,  $\hat{G}$  and  $\hat{F}_L$  is in §1.) It says  $\sigma_\infty^k$  is conjugate to  $\sigma_\infty$  in  $\hat{G}$  for all  $k \in M_{F,n}$ . Also, if  $\sigma_\infty^k$  and  $\sigma_\infty$  are not conjugate in  $G$ , then  $k$  has nontrivial image in  $G(\hat{F}_L \cap F(\zeta_n)/F)$ . Each  $\tau \in \hat{G}/G$  defines a coset of  $G$  in  $\hat{G}$ . Call this  $\tau G$ .

**FINITE FIELD APPLICATION 3.2.** *Let  $F$  be a number field with ring of integers  $O_F$ . Consider  $f(y) \in F[y]$ . Suppose  $F(y)/F(x)$ , with  $f(y) = x$ , gives a  $(G, \hat{G})$  realization over  $F$ . Assume, further, these properties of  $\sigma_\infty \in C_\infty$ .*

(3.1a) *There exists  $(k, n)$  with  $\sigma_\infty^k$  not conjugate to  $\sigma_\infty$  in  $G$ .*

(3.1b) *There exists  $\tau \in \hat{G}/G$  with  $\tau G$  containing no  $n$ -cycle.*

*Then, for infinitely many prime ideals  $\mathcal{P}$  of  $O_F$ , no  $b \in O_F/\mathcal{P} = \mathbb{F}_{\mathcal{P}}$  has either of the following properties.*

(3.2a)  *$f(x) - b$  factors completely over  $\mathbb{F}_{\mathcal{P}}$ .*

(3.2b)  *$f(x) - b$  is irreducible over  $\mathbb{F}_{\mathcal{P}}$ .*

*In particular, for  $f$  of Prop. 2.2 (and Ex. 4.3), and infinitely many primes  $p$ , there is no  $b \in \mathbb{Z}/p$  for which either (3.2a) or (3.2b) holds.*

**PROOF.** Let  $\Omega_f$  be the splitting field of  $f(y) - x$  over  $F$ . Similarly, let  $\Omega_{f,\mathcal{P}}$  be the splitting field of  $f(y) - x$  over  $\mathbb{F}_{\mathcal{P}}$ . Choose  $\tau$  as in the statement of this

application. Here is the result of the Chebotarev analog in [Fr8, Prop. 2]. For infinitely many  $\mathcal{P}$ ,  $G(\Omega_{f,\mathcal{P}}/\mathbb{F}_{\mathcal{P}}(x))$  is isomorphic to the subgroup of  $\hat{G}$  generated by  $G$  and  $\tau$ . Further, we may assume

$$\Omega_{f,\mathcal{P}} \cap \bar{\mathbb{F}}_{\mathcal{P}}(x) = \hat{\mathbb{F}}_{\mathcal{P}}$$

has its Frobenius generator over  $\mathbb{F}_{\mathcal{P}}$  equal to  $\tau$ . For such  $\mathcal{P}$ , we show there is no  $b \in \mathbb{F}_{\mathcal{P}}$  with either of the properties (3.2a) or (3.2b).

Suppose, to the contrary, there is such a  $b$ . The non-regular Chebotarev analog (as in [Fr8, loc. sit.] or [FrJ, Prop. 5.16]) says the following when  $|\mathbb{F}_{\mathcal{P}}|$  is suitably large. There is a non-branch point  $b$  (for the cover given by  $f$ ) for which  $f(y) - b$  splits completely if and only if  $\tau$  is the identity. Since  $\tau \neq 1$ , this proves (3.2a) can't hold for  $b$  unless it is a branch point. Now assume  $b$  is in the branch locus. Lift the Frobenius generator of  $\hat{\mathbb{F}}_{\mathcal{P}}/\mathbb{F}_{\mathcal{P}}$  to the decomposition group  $D_{\mathcal{P}}$  of a place of  $\Omega_{f,\mathcal{P}}$  over the place  $x \mapsto b$  of  $\mathbb{F}_{\mathcal{P}}(x)$ . All such lifts  $\tau'$  of  $\tau$  lie in a coset of the inertia group  $I_{\mathcal{P}}$  of  $\mathcal{P}$ . The curve cover by  $f$  is nonsingular. So, what  $\tau$  does to the zeros of  $f(x) - b$  determines the Frobenius on the residue class field of the cover over  $b$ . Since we assume complete splitting,  $\tau'$  must be an element of the inertia group. Here, however, the inertia group is in  $G$ , contrary to our assumption about  $\tau$ . Showing (3.2b) can't hold is similar, except the conclusion comes from all  $n$ -cycles being in  $G$ .  $\square$

#### §4. Classifying which $C$ in $A_n$ give $(A_n, S_n)$ realizations

The constants of  $\Omega_f$  for  $f \in \mathbb{Q}[x]$  have limited options. To see this we need a classification of the geometric monodromy groups of such polynomials. Müller [M] gives what we want.

**Q-POLYNOMIAL MONODROMY THEOREM 4.1.** *Suppose  $f \in \mathbb{Q}[x]$  is indecomposable and  $G$  is its geometric monodromy group. Then,  $G$  is either  $S_n$ ,  $A_n$ , cyclic, dihedral,  $\mathrm{PGL}_2(5)$ ,  $\mathrm{PGL}_2(8)$ , or  $\mathrm{PGL}_2(9)$ . The latter have representations of degree 6, 9 and 10 respectively.*

**HISTORICAL REMARKS 4.2.** *Polynomials over a number field different from  $\mathbb{Q}$ .* Müller also gives a complete classification of the geometric monodromy groups of polynomials over  $\mathbb{C}$ . Here, too, there are only sporadic examples, other than  $A_n$ ,  $S_n$ , cyclic and dihedral groups. Nevertheless, the sporadic examples are interesting. For Theorem 4.1, Müller uses the beginnings of the subject in [Fr4], more than a decade before the classification of finite simple groups. The Branch Cycle argument alone eliminated a geometrically viable class of groups as geometric monodromy groups from Theorem 4.1. Before we knew for certain their identities, we labeled the  $G$  in this list by the following properties.

(4.1a)  $G$  has two faithful, doubly transitive representations  $T_1, T_2 : G \rightarrow S_n$ .

- (4.1b)  $T_1$  and  $T_2$  are inequivalent permutation representations, but equivalent as ordinary complex group representations.
- (4.1c) There exists  $\sigma_\infty \in G$  with  $T_1(\sigma_\infty)$  and  $T_2(\sigma_\infty)$  both  $n$ -cycles.

Projective linear groups acting on projective space of 2 or more dimensions were key examples. The sporadic examples of Theorem 4.1 act on projective 1-space. Following the classification, with help from Feit and Kantor, [Fr7] fulfilled an outline from [Fr6] to show there are exactly six polynomial degrees from this list: 7, 11, 13, 15, 21 and 31. This is about half of the sporadic examples in [M]. Ex. 4.7 contains the degree 7 case.  $\square$

We give four examples to test  $(A_n, S_n)$  realization over  $\mathbb{Q}$ . The first is generic for satisfying the necessary hypotheses. Since these polynomials give covers with more than three branch points, it shows how polynomials are simpler than the general applications of the theory. The second considers when  $n$  is a square. The examples of this degree from Prop. 2.2 did not give  $(A_n, S_n)$  realizations; we still don't have any. The third example is similar to Prop. 2.2, except for one point: The transitivity condition in the rigidity hypothesis doesn't hold. As a consequence, it doesn't give  $(A_n, S_n)$  realizations over  $\mathbb{Q}$ . Of interest: It isn't for the failure of the *rational union* conjugacy class hypothesis. This is the simplest example I know of its failure. The fourth, and most challenging, example considers polynomials with all branch cycles, of finite branch points, products of two disjoint 2-cycles.

**EXAMPLE 4.3.** *Generic 3-cycle case and variants when all branch cycles are cycles in  $A_n$ .* Suppose a polynomial of odd, non-square degree  $n > 3$  has the maximal number of branch cycles, all 3-cycles. The Riemann-Hurwitz formula (conclusion of Prop. 2.2 in §3), shows this number is  $r - 1$  where  $2(n - 1) = n - 1 + 2(r - 1)$ . That is, there are  $(n - 1)/2$  such finite branch points. Suppose monic  $f \in \mathbb{Q}[y]$  gives an  $(A_n, S_n)$  realization over  $\mathbb{Q}$  with all its branch cycles 3-cycles. Then  $\frac{df}{dy} = ng(y)^2$  where  $g \in \mathbb{Q}[y]$  is monic and has *distinct* roots. (If they weren't distinct, the multiplicity of the branch points would be higher than 3.) Further, the image of the roots of  $g$  under  $f$  are distinct. (Otherwise, there would be more than two disjoint cycles of length greater than 1 in some branch cycle.) The branch cycle argument with the Irrational Cycle Lemma implies  $f$  gives an  $(A_n, S_n)$  realization over  $\mathbb{Q}$ . All that remains is to produce the polynomials  $f$ . This, however, is easy.

Monic, degree  $(n-1)/2$ , polynomials form an affine space  $V_{(n-1)/2} = \mathbb{A}^{(n-1)/2}$ . Square any representing polynomial  $g$  and form an antiderivative. Denote this  $\int g^2 dx$ . Except that it is in  $\mathbb{Q}$ , we don't care about the choice of constant. The general  $\mathbb{Q}$  point of  $V_{(n-1)/2}$  represents a polynomial  $g(y)$  with distinct roots. Further, for such a general polynomial, these roots have distinct images under  $\int g^2 dx$ . All such examples come from this process.

We generalize the previous paragraphs. Let  $\mathbf{C} = (C_1, C_2, \dots, C_{r-1}, C_r)$  with

$C_r$  the conjugacy class of an  $n$ -cycle, and  $C_i$  the conjugacy class of  $k_i$ -cycles,  $1 < k_i < n-1$ ,  $i = 1, \dots, r-1$ . The Riemann-Hurwitz formula shows there are polynomials having such branch cycles if and only if

$$(4.2) \quad \sum_{i=1}^{r-1} k_i - 1 = n - 1.$$

If  $\sigma_i \in C_i$ ,  $i = 1, \dots, r-1$ , and these  $\sigma_i$ s generate a transitive group, Lemma 4.6 shows it is automatic their product is an  $n$ -cycle. As above, find  $f \in \mathbb{Q}[y]$  with this type of branching. The derivative of  $f$  has the form

$$(y - a_1)^{k_1-1} (y - a_2)^{k_2-1} \dots (y - a_{r-1})^{k_{r-1}-1}$$

with  $a_i \in \mathbb{Q}$  and  $f(a_1), \dots, f(a_{r-1})$  distinct. An open subset of affine  $\mathbb{A}^{r-1}$ -space represents polynomials with appropriate  $a_1, \dots, a_{r-1}$ . A Zariski open subset of the  $\mathbb{Q}$  points gives the polynomials we want.  $\square$

EXAMPLE 4.4.  $A_n$  when  $n$  is an odd square. Recall the failure of Prop. 2.2 to give  $(A_n, S_n)$  realizations for  $n$  a square. This doesn't, however, mean there are no  $(A_n, S_n)$  realizations over  $\mathbb{Q}$  for this  $n$ . I'll illustrate complications with  $n = 9$  using the Irrational Cycle Addendum. According to it, the only other conjugacy classes in  $A_n$  that aren't rational have cycle type  $(1)(3)(5)$ . Let  $\sigma$  be an element of this type. A 9-cycle and  $\sigma$  generate a primitive group:  $\sigma^3$  is a 5-cycle, and the group contains a 3-cycle,  $\sigma^5$ . So it is  $A_n$ . For example,

$$(\bullet_1) \quad ((2\ 3\ 4)(5\ 6\ 7\ 8\ 9), (1\ 2\ 5), (1\ 2\ \dots\ 9)^{-1})$$

are branch cycles of a cover from  $f \in \mathbb{C}[y]$ .

Check if the hypotheses of Rigidity Results 3.1 apply to give an  $(A_n, S_n)$  realization. Choose  $(\sigma_1, \sigma_2, \sigma_3)$  where  $\sigma_1$  has the cycle type of  $\sigma$ ,  $\sigma_2$  is a 3-cycle and  $\sigma_3$  is a 9-cycle. Conjugate by an element of  $S_9$  to assume  $\sigma_3 = (1\ 2\ \dots\ 9)^{-1}$  and the 1-cycle of  $\sigma_1$  is 1. We have normalized, so the Rigidity Results hold if and only if there is exactly one such 3-tuple. Alas, there are exactly 2:  $(\bullet_1)$  and

$$(\bullet_2) \quad ((7\ 8\ 9)(2\ 3\ 4\ 5\ 6), (1\ 2\ 7), (1\ 2\ \dots\ 9)^{-1}).$$

Finally, Prop. 2.1 explains why no polynomials over  $\mathbb{Q}$  have these branch cycles. If they exist, the Irrational Cycle Addendum says extension of constants would be  $\mathbb{Q}(\sqrt{-3 \cdot 5})$ . On the other hand, from total ramification over  $\infty$ , the extension of constants must be in  $\mathbb{Q}(\sqrt{-3})$ . These two fields are different, so the extension of constants is trivial. This contradicts Prop. 2.1 for the conjugacy class of  $\sigma_2$ . Still, there may be other ways to get an  $(A_9, S_9)$  realization by polynomials over  $\mathbb{Q}$  for  $n = 9$ . These, however, would have all conjugacy classes rational. For example, the  $(2)(2)$  polynomials of degree 9 in Ex. 4.7 might give such an example.



Suppose we want to use a conjugacy class  $C$  that isn't rational to force an  $(A_n, S_n)$  realization (for  $n = w^2$  an odd square) over  $\mathbb{Q}$ . To avoid the problem above, we must assure  $\mathbb{Q}(\alpha_\sigma)$ ,  $\sigma \in C$ , is a subfield of  $\mathbb{Q}(\zeta_n)$ . The argument above shows you can't do this for  $n = 25$ . You can, however, find  $m_i$ s that work for  $n = (3 \cdot 5)^2$ . Take  $C$  a conjugacy class of elements of form

$$(7 \cdot 3)(7 \cdot 5)(13^2) = (m_1)(m_2)(m_3).$$

The  $m_i$ s are distinct odd integers that sum to 225. The field  $\mathbb{Q}(\alpha_\sigma)$  in the Irrational Cycle Addendum is  $\mathbb{Q}(\sqrt{-3 \cdot 5})$  because the vectors for 7 and 13 map to 0 under  $\mu$ .

Assume there is a monic polynomial  $f \in \mathbb{Q}$  with its cover having the appropriate branch cycle description. The other branch cycle above a finite point must be a 3-cycle or a product of two disjoint 2-cycles. Let's try the former. All points above the finite branch point for  $\sigma$  must be rational. Suppose  $a_i$  corresponds to the  $m_i$ -cycles,  $i = 1, 2, 3$ . With no loss take  $a_3 = 0$ . Then,

$$\frac{df}{dy} = 225(y - a_1)^{7 \cdot 3 - 1}(y - a_2)^{7 \cdot 5 - 1}y^{13^2 - 1}(y - b)^2; \text{ and } f(a_1) = f(a_2) = f(0).$$

*Mathematica* showed us there are no rational solutions for  $a_1 \neq a_2$  and  $b$  (as in Ex. 4.5). Thus, this choice of  $m_i$ s for  $n = 225$  doesn't produce an  $(A_{25^2}, S_{25^2})$  realization by polynomials over  $\mathbb{Q}$ .

So, we need another idea, for there are many such situations to check as  $n$  increases. In fact, the main result of [RT] says the following. For  $n > 24$  and  $p < n - 2$  a prime, there are distinct odd integers  $l_1, \dots, l_s$  with  $n = p + \sum_{j=1}^s l_j^2$ . Take  $p$  to be a prime dividing  $n$ . Apply the Irrational Cycle Addendum. Suppose  $f \in \mathbb{Q}[y]$ , of degree  $n$ , has a branch cycle of form  $(p)(l_1^2) \cdots (l_s^2)$ . Then, the extension of constants must be  $\mathbb{Q}(\sqrt{(-1)^{(p-1)/2} p})$ . As  $p|n$ , this is in  $\mathbb{Q}(\zeta_n)$ . We know no general criterion to eliminate this case. ([RT] informs us, [JK] contains a version of our Irrational Cycle Addendum.)  $\square$

EXAMPLE 4.5. *A three branch point non-rigid  $A_n$  cover.* Follow notation of Prop. 2.2 with  $n \geq 5$ , odd and squarefree. Let  $C$  be the conjugacy classes of the triple  $(\sigma_1, \sigma_2, \sigma_3) \in A_n^3$  with  $\sigma_1 = (12)(34)$ ,  $\sigma_2 = (13567 \dots n)$  and  $\sigma_3 = (12 \dots n)^{-1}$ . Check easily the geometric monodromy group is  $A_n$ .

As in Prop. 2.2, give representatives for conjugation of  $S_n$  on  $\Sigma(C^{S_n})$ :

$$\sigma_i = ((12)(i \ i+1), (13 \dots i \ i+2 \ i+3 \dots n), \sigma_3), \quad i = 3, \dots, (n+1)/2.$$

This means for any possible pair of points,  $x_1, x_2 \in \mathbb{Q}$ , there are  $(n-3)/2$  inequivalent polynomial covers with  $x_1$  and  $x_2$  as their finite branch points. Given any such cover,  $f : \mathbb{P}_y^1 \rightarrow \mathbb{P}_x^1$ , compose  $f$  on the right with a linear map  $\lambda(x) = ux + v$  where  $\lambda(0) = x_1$  and  $\lambda(1) = x_2$ . Since  $x_1, x_2 \in \mathbb{Q}$ , so are  $u, v \in \mathbb{Q}$ . Thus, the nature of the covers doesn't depend on the branch points. This doesn't

work unless there are two finite branch points and these are in  $\mathbb{Q}$ . That happens here because the conjugacy classes are distinct in  $S_n$ .

We investigate if some representing polynomial  $f(y)$  for these covers is in  $\mathbb{Q}[y]$ . Assume it is. Take its derivative to be  $g(y) = (y-a)(y-b)y^{n-3} \in \mathbb{Q}[y]$ . Conclude  $a, b$  are either in  $\mathbb{Q}$  or they are conjugate over  $\mathbb{Q}$ . Further, our hypotheses give two other conditions:

$$(4.3) \quad f(x) = y^n/n - (a+b)y^{n-1}/(n-1) + aby^{n-2}/(n-2) + d; \text{ and } f(a) = f(b).$$

Note:  $d \in \mathbb{Q}$  is arbitrary. The last half of (4.3) gives a degree  $n$  equation in  $b/a = \alpha$ . Simplify to

$$(4.4) \quad (n-2)(\alpha^n - 1) = n(\alpha^{n-1} - \alpha).$$

The solution  $\alpha = 1$  implies  $a = b$ . Remove this: it is contrary to the first element of  $\sigma_i$  being a product of two disjoint 2-cycles. Indeed, a check of the first and second derivatives of (4.4) shows  $\alpha = 1$  is a solution of multiplicity 3.

Synthetically divide to get a polynomial with no roots equal 1:  $(\alpha-1)^2$  divides

$$(4.5) \quad h_n(\alpha) = (n-2)\alpha^{n-1} - 2(\alpha + \cdots + \alpha^{n-2}) + (n-2).$$

For  $n = 5$ ,  $\alpha$ s different from 1 satisfy  $3\alpha^2 + 4\alpha + 3 = 0$ . The two complex conjugate roots are in  $\mathbb{Q}(\sqrt{-5})$ . For this case, there is a polynomial over  $\mathbb{Q}$ .

For general (odd)  $n$ , there is a polynomial over  $\mathbb{Q}$  exactly when  $h_n(\alpha)/(\alpha-1)^2$  has a degree 2 factor over  $\mathbb{Q}$ . We suspect there is none for odd  $n > 5$ . Still, we don't see how to prove this. For example,

$$(4.6) \quad h_7(\alpha)/(\alpha-1)^2 = 5\alpha^4 + 8\alpha^3 + 9\alpha^2 + 8\alpha + 5.$$

*Mathematica* said this is irreducible. Moreover, it says  $h_n(\alpha)/(\alpha-1)^2$  over  $\mathbb{Q}$  is irreducible for all odd  $n$  I tried, up to  $n = 31$ .  $\square$

Now consider the generic situation containing the phenomenon of Ex. 4.5. This concludes the paper, leaving several practical mysteries for further progress on the classification of  $(A_n, S_n)$  realizations over  $\mathbb{Q}$  by polynomials. Lemma 4.6 discusses groups having generators with each a product of two disjoint 2-cycles. Especially, it analyzes the case these generators are branch cycles for finite branch points of a polynomial cover. [Fr6-7] discuss the history of *Davenport polynomials*. Lemma 4.6 includes the degree 7 examples with  $\text{PSL}_3(\mathbb{F}_2)$  as monodromy group. Recall two combinatorial definitions. The *index*  $\text{ind}(\sigma)$  of  $\sigma \in S_n$  of cycle type  $(m_1) \cdots (m_t)$  (include length 1 cycles) is  $n - t$ . Here is how the  $i$ -th *braid* operation  $Q_i$  acts on an  $r$ -tuple:

$$(4.7) \quad (\sigma)Q_i = (\sigma_1, \dots, \sigma_{i-1}, \sigma_i \sigma_{i+1} \sigma_i^{-1}, \sigma_i, \sigma_{i+2}, \dots, \sigma_r), \quad i = 1, \dots, r-1.$$

LEMMA 4.6. Suppose  $\sigma \in S_n^r$  is a branch cycle description of a polynomial cover;  $\sigma_r$  is the  $n$ -cycle. Then, for  $1 \leq i < j \leq r-1$ ,

$$(4.8a) \quad \text{ind}(\sigma_i \sigma_j) = \text{ind}(\sigma_i) + \text{ind}(\sigma_j).$$

If  $\tau_1, \dots, \tau_{r-1} \in S_n$  generate a transitive group and  $\sum_{j=1}^{r-1} \text{ind}(\tau_j) \leq n-1$ , then,

$$(4.8b) \quad \sum_{j=1}^{r-1} \text{ind}(\tau_j) = n-1, \text{ and } \tau_1 \cdots \tau_{r-1} \text{ is an } n\text{-cycle.}$$

Now, suppose  $n > 3$  is an odd integer. Further assume:

(4.9a)  $\sigma \in S_n^r$  is a branch cycle description of a polynomial cover;

(4.9b)  $\sigma_r$  is an  $n$ -cycle; and

(4.9c)  $\sigma_i$  is a product of two disjoint 2-cycles,  $i = 1, \dots, r-1$ .

Then,  $r-1 = (n-1)/2$  and the geometric monodromy group  $G$  of the cover is  $A_n$  if and only if  $G$  contains a 3-cycle. For  $n > 7$ ,  $G$  is  $A_n$ . For  $n = 5$ ,  $G = D_5$ , the dihedral group. For  $n = 7$  it is either  $\text{PSL}_3(\mathbb{F}_2)$  or  $A_7$ ; both appear.

PROOF. There are five parts. Three are statements on indices. Two compute the braid action on branch cycles for polynomial covers with group  $\text{PSL}_3(\mathbb{F}_2)$ . There are two orbits. Part D of Ex. 4.7 explains conclusions from this.

*Part A: Proof of statement (4.8b).* Consider  $\tau_1, \dots, \tau_{r-1}$  satisfying the hypotheses prior to (4.8b). Let  $\tau_r = (\tau_1 \cdots \tau_{r-1})^{-1}$ . Since  $\tau_1, \dots, \tau_{r-1}$  generate a transitive group, applying the Riemann-Hurwitz formula to  $\tau_1, \dots, \tau_r$  gives the following. There is an integer  $g \geq 0$  such that

$$(4.10) \quad 2(n+g-1) = \sum_{i=1}^{r-1} \text{ind}(\tau_i) + \text{ind}(\tau_r) \leq n-1 + \text{ind}(\tau_r) \leq 2(n-1).$$

Thus,  $g = 0$  and equality holds through (4.10):  $\text{ind}(\tau_r) = n-1$ , so  $\tau_r$  is an  $n$ -cycle. Conclude further:  $\tau_1, \dots, \tau_r$  is a description of the branch cycles of a polynomial cover.

*Part B: Proof of statement (4.8a).* Start with a  $\sigma$  from the first sentence of the lemma. Characterization:  $\sigma_r$  is an  $n$ -cycle and the genus is 0. The Riemann-Hurwitz formula says (4.2) holds where  $k_i$  is the index of  $\sigma_i$ . So,

$$(4.11) \quad \text{ind}(\sigma_1) + \text{ind}(\sigma_2) = n-1 - \sum_{i=3}^{r-1} \text{ind}(\sigma_i).$$

Now replace  $\text{ind}(\sigma_1) + \text{ind}(\sigma_2)$  in (4.11) with  $\text{ind}(\sigma_1 \sigma_2)$ . Suppose we prove

$$(4.12) \quad \text{ind}(\sigma_1) + \text{ind}(\sigma_2) \geq \text{ind}(\sigma_1 \sigma_2).$$

Then, apply Part A to  $(\sigma_1 \cdot \sigma_2, \sigma_3, \dots, \sigma_{r-1})$  to conclude equality of the left and right sides of (4.12). The index, however, of  $\sigma$  is also the fewest 2-cycles whose

product equals  $\sigma$ . Multiply the smallest product for  $\sigma_1$  and for  $\sigma_2$  to give a product of 2-cycles for  $\sigma_1\sigma_2$ , showing (4.12). This proves (4.8a) for  $i = 1, j = 2$ .

To prove (4.8a) for general  $i < j \leq r-1$ , apply the braid

$$Q = Q_{i-1}^{-1} Q_{i-2}^{-1} \cdots Q_1^{-1} Q_{j-1}^{-1} \cdots Q_2^{-1}$$

to  $\sigma$  to get  $\sigma'$  satisfying the hypotheses before (4.8a). The former  $\sigma_i$  and  $\sigma_j$  are now  $\sigma'_1$  and  $\sigma'_2$ .

*Part C:*  $\sigma_i, i = 1, \dots, r-1$ , is a product of two disjoint 2-cycles. The value of  $r$  follows from the Riemann-Hurwitz formula:  $2(n-1) = 2(r-1) + (n-1)$ , since each finite branch cycle adds 2 to the right hand side. Let  $G$  be the group the  $\sigma$  generate. Primitivity is easy to prove as in the first part of the proof of Prop. 2.2. The group must be  $A_n$  if  $n > 7$ , from Müller's classification for all polynomials. Involutions in  $\text{PSL}_{k+1}$  acting on points of  $\mathbb{P}^k$ ,  $k \geq 2$ , can't be products of two 2-cycles unless  $k = 2$  and  $n = 7$  is the number of points. Details start in Parts D and E. The case  $n = 5$  is clear: involutions  $\sigma_1$  and  $\sigma_2$  must generate the dihedral group of order 10.

*Part D: Start of the case  $n = 7$ .* Order branch cycles in all cases so  $\sigma_4 = (12 \dots 7)^{-1}$ . Here is an example where the branch cycles generate  $A_7$ :

$$(4.13) \quad \sigma = ((12)(34), (13)(57), (15)(67), \sigma_4).$$

Here  $\sigma_1\sigma_3 = (125)(34)(67)$ . Thus, its square is a 3-cycle and the group is  $A_7$ .

Now, we display branch cycles for polynomials over  $\mathbb{C}$  having monodromy group  $\text{PSL}_3(\mathbb{F}_2)$ , acting on the seven points of  $\mathbb{P}^2(\mathbb{F}_2)$ , projective 2-space over  $\mathbb{F}_2$ . There are two families of these. These correspond, as in (4.1a)–(4.1c), to the equivalent, but not permutation equivalent representations of  $\text{PSL}_3(\mathbb{F}_2) = G$  on lines and planes. Let  $T_1 : G \rightarrow S_7$  be a representation of this group on the 7 points. Let  $\bar{T}_1 : G \rightarrow \text{GL}_7(\mathbb{Q})$  be the associated linear representation.

There exists a matrix  $M \in \text{GL}_7(\mathbb{Q})$ , such that  $M^{-1} \circ \bar{T}_1 \circ M = \bar{T}_2$  has the following property. It is a permutation representation of  $G$  giving the action of  $G$  on the lines of the projective space. It arises from a second permutation representation of  $G$ . No permutation matrix represents  $M$ , so these representations are not permutation equivalent. Ex. 4.7 explains why these families have no members over  $\mathbb{Q}$ , as in Historical Remarks 4.2. There are also polynomials with group  $A_n$  where each of the 3 finite branch cycles is a product of two disjoint 2-cycles. Ex. 4.7 discusses these in detail.

In both representations  $T_1$  and  $T_2$ ,  $\sigma_4 = (12 \dots 7)^{-1}$ . Polynomial notation can give a better picture of the relation between the representations. Take  $g$  the polynomial produced by branch cycles for the representation  $T_2$ , and  $h$  the corresponding polynomial for branch cycles in the representation  $T_1$ . The zeros  $z_1, \dots, z_7$  of  $g(z) - x$  (representing lines of  $\mathbb{P}^2(\mathbb{Z}/2)$ ) are related to the zeros  $y_1, \dots, y_7$  of  $h(y) - x$  (representing points of  $\mathbb{P}^2(\mathbb{Z}/2)$ ) by the formula  $z_1 =$

$y_1 + y_{\alpha_2} + y_{\alpha_3}$ . That is, the splitting fields  $\Omega_h$  and  $\Omega_g$  are equal as extensions of  $\mathbb{C}(x)$ . Here,  $\{1, \alpha_2, \alpha_3\}$  is a difference set modulo 7. This means, the pairs of nonzero differences run over all elements of  $\mathbb{F}_7$  (in our case, each appearing once). There are two (translation inequivalent) difference sets modulo 7,  $\{1, 2, 4\}$  and its negative. Each involution in  $\text{PSL}_3(\mathbb{F}_2) = G$  comes from a reflection in a line, so each will fix all points of some line. We now do the case where the translates of the difference set  $\{1, 2, 4\}$  consist of sets of points constituting lines in the projective space.

Directly compute the possibilities for  $\sigma_1, \sigma_2, \sigma_3$  from this. Conjugation of each by some power of  $\sigma_4$  must fix all elements of  $\{1, 2, 4\}$ .

*Part E:  $\text{PSL}_3(\mathbb{F}_2)$  branch cycles.* Label finite branch cycles  $(\sigma_1, \sigma_2, \sigma_3)$  for a polynomial  $h$  as  $Y_1, \dots, Y_7$ . There are exactly 7 up to conjugation by  $S_7$ .

$$\begin{aligned} Y_1 &: ((3\ 5)(6\ 7), ((4\ 5)(6\ 2), (3\ 6)(1\ 2))); & Y_2 &: ((3\ 5)(6\ 7), (3\ 6)(1\ 2), (3\ 1)(4\ 5)); \\ Y_3 &: ((3\ 5)(6\ 7), (1\ 6)(2\ 3), (4\ 5)(6\ 2)); & Y_4 &: ((3\ 5)(6\ 7), (1\ 3)(4\ 5), (2\ 3)(1\ 6)); \\ Y_5 &: ((3\ 7)(5\ 6), (1\ 3)(4\ 5), (2\ 3)(4\ 7)); & Y_6 &: ((3\ 7)(5\ 6), (2\ 3)(4\ 7), (1\ 2)(7\ 5)); \\ Y_7 &: ((3\ 7)(5\ 6), ((1\ 2)(7\ 5), (1\ 3)(4\ 5)). \end{aligned}$$

Now compute the effect of the braid operators  $Q_1$  and  $Q_2$  on  $Y_1, \dots, Y_7$ . Apply standard notation in  $S_7$  by having them act on  $1, \dots, 7$ . (This isn't the action through the representations  $T_1$  and  $T_2$ .)

$$(4.14) \quad Q_1 = (3\ 5\ 1)(4\ 7\ 6\ 2), \text{ and } Q_2 = (1\ 3\ 4\ 2)(5\ 7\ 6) \text{ (see Part B of Ex. 4.7).}$$

Observe:  $Q_1$  and  $Q_2$  are transitive on the  $Y$ s. This shows the collection of polynomials with these descriptions of branch cycles forms a connected space  $\mathcal{H}(G, \mathbb{C})$ . The next calculation assures the variety (one of those in §3) is *unirational* (see Part D of Ex. 4.7). In particular, it has many rational points over the field of its definition. Analogous examples from [DFr], [Fr6-7], [Fr9] and [MM] show the rationnel behind this calculation. From  $Q_1$  and  $Q_2$ , produce  $a_{12}, a_{13}$  and  $(a_{12}a_{13})^{-1}$  which have product 1 and generate a transitive subgroup of  $S_7$ :

$$(4.15a) \quad a_{12} = Q_1^{-2} = (1\ 3\ 5)(2\ 7)(4\ 6);$$

$$(4.15b) \quad a_{13} = Q_1 Q_2^{-2} Q_1^{-1} = (3\ 4\ 7)(1\ 6)(2\ 5); \text{ and}$$

$$(4.15c) \quad (a_{12}a_{13})^{-1} = (7\ 6\ 5)(1\ 4)(2\ 3).$$

Riemann's Existence Theorem 1.1 says these are branch cycles for a 3-branch point, degree 7 cover  $\psi : \mathcal{W} \rightarrow \mathbb{P}^1$ . The geometric monodromy group of this cover is  $A_7$ , though it isn't a polynomial cover. By Riemann-Hurwitz, the genus  $g(\mathcal{W})$  of  $\mathcal{W}$  is 0:  $2(7 + g - 1) = 3 \cdot 4$ . Since the degree of  $\psi$  is 7, there is an odd degree divisor on  $\mathcal{W}$  defined over the field  $K = \mathbb{Q}(\sqrt{-7})$  of definition of the cover. Part D of Ex. 4.7 explains the meaning of this curve. A genus 0 curve having an odd degree divisor over  $K$  is isomorphic to  $\mathbb{P}^1$  over  $K$ . Thus, the function field of  $\mathcal{H}(G, \mathbb{C})$  is a subfield of  $K(x_2, x_3, w)$ . Coordinates  $x_2$  and  $x_3$  represent two of

the branch points of the general cover in the family;  $w$  is a variable for a copy of projective 1-space.  $\square$

EXAMPLE 4.7. (2)(2) *polynomials*. Following the first part of Ex. 4.3,  $n > 5$  is odd, nonsquare and there are  $(n - 1)/2 = r - 1$  branch cycles corresponding to finite branch points. Here, however, instead of 3-cycles, each branch cycle is a product of two disjoint 2-cycles. That is,  $\mathbf{C} = (C_1, \dots, C_{r-1}, C_r)$  with each of  $C_1, \dots, C_{r-1}$  the conjugacy class of (1 2)(3 4). Here are conclusions from Lemma 4.6. Elements from this conjugacy class will have product an  $n$ -cycle if and only if they generate a transitive group. If  $n > 7$ , such elements generate  $A_n$ . Suppose a polynomial  $f \in \bar{\mathbb{Q}}[y]$  gives a cover with its finite branch cycles products of two disjoint 2-cycles. Call  $f$  a (2)(2) polynomial. It is automatic from Prop. 2.1 that a (2)(2) polynomial over  $\mathbb{Q}$  produces an  $(A_n, S_n)$  realization (for  $n$  odd and nonsquare).

Now we investigate if there are (2)(2) polynomials  $f \in \mathbb{Q}[y]$ . With no loss, assume the derivative of  $f$  is

$$(4.16a) \quad g(y) = \prod_{i=1}^{(n-1)/2} (y - a_i)(y - a'_i) \text{ where}$$

$$(4.16b) \quad f(a_i) = f(a'_i) \text{ and } f(a_i) \neq f(a_j), 1 \leq i < j \leq (n - 1)/2.$$

This is a complicated set of equations. See Synopsis 4.9 for  $n > 7$ . The remainder completes the work of Lemma 4.6 on the case  $n = 7$  in four parts. The first three do the case where the geometric monodromy group is  $A_7$ . The last summarizes the description of the collection satisfying (4.16). We follow the work of Parts D-E of the proof of Lemma 4.6.

*Part A: Branch cycles for (2)(2) polynomials.* As in Part D of Lemma 4.6, order branch cycles in all cases so  $\sigma_4 = (1 2 \dots 7)^{-1}$ . For relevant  $\sigma$ , there are three possibilities for the cycle types of  $\sigma_1 \cdot \sigma_2$ :

$$(4.17) \quad U_1 : (5); U_2 : (3)(2)(2); U_3 : (4)(2); U_4 : (3)(3).$$

From Lemma 4.6 it is automatic  $\sigma$  giving  $U_1$  or  $U_2$  has group  $A_7$ . The example of (4.13) has types  $U_1, U_2, U_3$  appearing in paired products from the 3-tuple. We list all possibilities, up to conjugation, having the cycle types of (4.17). These will be in the form  $(\sigma_1 \sigma_2, \sigma_3)$  after coalescing  $\sigma_1$  and  $\sigma_2$ . Then, for each, we list corresponding pairs  $(\sigma_1, \sigma_2)$ . Part of the calculation determines the conjugating power of  $\sigma_4$  on  $\sigma$  to give the following normalizations.

(4.18a) For  $U_1$ , choose  $(\sigma_1 \cdot \sigma_2, \sigma_3)$  to be one of the two representations that appear for  $n = 7$  in Ex. 4.5.

(4.18b) For  $U_2$ , 1 appears in the 3-cycle of  $\sigma_1 \cdot \sigma_2$ , but not in  $\sigma_3$ .

(4.18c) For  $U_3$  and  $U_4$ , 1 does not appear in  $\sigma_1 \cdot \sigma_2$ .

Coalescing  $Y_2, Y_4, Y_6$  and  $Y_7$  in Lemma 4.6, Part D, gives one  $U_3$  example,  $U_3[3] : (2\ 3\ 4\ 7)(5\ 6), (1\ 2)(5\ 7)$ . Coalescing similar branch cycles for the negative of the difference set  $\{1, 2, 4\}$  gives another,  $U_3[4] : (2\ 5\ 6\ 7)(3\ 4), (1\ 2)(5\ 3)$ . Neither of these give  $A_7$  as Galois group; so remove them. Here are the remaining normalized  $(\sigma_1\sigma_2, \sigma_3)$  pairs:

$$\begin{aligned}
(4.19a) \quad U_1[1] &: (1\ 3\ 4\ 5\ 6), (1\ 7)(2\ 3); & U_1[2] &: (1\ 2\ 4\ 5\ 6), (1\ 7)(4\ 3) \\
(4.19b) \quad U_2[1] &: (1\ 4\ 7)(2\ 3)(5\ 6), (2\ 4)(7\ 5); & U_2[2] &: (7\ 1\ 2)(6\ 3)(4\ 5), (3\ 7)(4\ 6) \\
(4.19c) \quad U_3[1] &: (2\ 3\ 6\ 7)(4\ 5), (1\ 2)(4\ 6); & U_3[2] &: (6\ 3\ 4\ 5)(2\ 7), (1\ 2)(3\ 7) \\
(4.19d) \quad U_4[1] &: (4\ 5\ 6)(2\ 3\ 7), (1\ 2)(7\ 4); & U_4[2] &: (3\ 4\ 5)(2\ 6\ 7), (1\ 2)(6\ 3).
\end{aligned}$$

Excluding  $U_4[1]$  and  $U_4[2]$ , any  $\sigma$  that coalesces to one of these will have monodromy group  $A_7$ . For each  $U_i$  we need a scheme to label the  $\sigma$ s that coalesce to these. Here is an example.

(4.20a)  $U_1[i; j]$  replaces the 5-cycle with the product of  $((2)(2), (2)(2))$  with  $j$  in the 5-cycle missing from the support of 2-cycles in the first coordinate.

In (4.20a),  $U_1[1; 6]$  replaces  $(1\ 3\ 4\ 5\ 6)$  with  $((5\ 1)(3\ 4), (5\ 3)(1\ 6))$ .

(4.20b)  $U_2[i; j, \alpha]$  replaces  $(j\ k, l)\alpha\alpha'$  with  $((j\ k)\alpha, (j\ l)\alpha')$ .

(4.20c)  $U_3[i; (i_1\ i_3)^1]$  (resp.,  $U_3[i; (i_1\ i_3)^2]$ ) replaces  $(i_1\ i_2\ i_3\ i_4)\alpha$  with

$$((i_1\ i_3)\alpha, (i_2\ i_3)(i_1\ i_4)) \text{ (resp., } ((i_1\ i_2)(i_3\ i_4), (i_1\ i_3)\alpha).$$

(4.20d)  $U_4[i; k_1, l_1]$  replaces  $(k_1\ k_2\ k_3)(l_1\ l_2\ l_3)$  by  $((k_1\ k_2)(l_1\ l_2), (k_1\ k_3)(l_1\ l_3))$ .

Exclude three (4.20d) cases that appear in Part D of Lemma 4.6:  $U_4[2; 5, 6]$ ,  $U_4[2; 3, 7]$  and  $U_4[2; 2, 4]$ . Similarly, exclude three cases that come from the other difference set in Part D:  $U_4[1; 4, 3]$ ,  $U_4[1; 5, 7]$  and  $U_4[1; 6, 2]$ . Note: The order of the last two integers in the  $U_4$  descriptions is irrelevant, but we must put them in *some* order. Condense notation by writing  $U_i[????]$  as  $i_{[????]}$ .

*Part B: Two orbits of  $(2)(2)$  polynomials with monodromy group  $A_7$ .* As in Part E of Lemma 4.6, compute the action of  $Q_1$  and  $Q_2$  on the list of (4.20). Two illustrations show how to program the calculation.

$$\begin{aligned}
(4.21a) \quad (2_{[1;4,(2\ 3)]})Q_1 &= ((4\ 7)(2\ 3), (4\ 1)(5\ 6), (2\ 4)(7\ 5))Q_1 \\
&= ((7\ 1)(4\ 5), (6\ 4)(2\ 7), (2\ 4)(7\ 5)) = 2_{[1;7,(5\ 6)]}.
\end{aligned}$$

Once you have a list of the possible 3-tuples, the action of  $Q_1$  is easy. The action of  $Q_2$  requires one tricky identification step:

$$\begin{aligned}
(4.21b) \quad (2_{[1;4,(2\ 3)]})Q_2 &= ((4\ 7)(2\ 3), (2\ 1)(7\ 6), (4\ 1)(5\ 6)) \\
&\cong ((7\ 3)(6\ 5), (4\ 5)(3\ 2), (1\ 2)(7\ 4)) = 4_{[1;5,3]}.
\end{aligned}$$

The place of  $\cong$  is where we normalize by a uniform translation of all integers in the middle triple. To figure the correct translation, multiply the 1st and 2nd entries of the middle triple (here, (47)(23) and (21)(76)). From this, compare with the list of (4.20); and produce the label easily after translation. The final permutations:

$$\begin{aligned}
Q_1 = & (1_{[1;6]} 1_{[1;3]} 1_{[1;5]} 1_{[1;1]} 1_{[1;4]}) (1_{[2;6]} 1_{[2;2]} 1_{[2;5]} 1_{[2;1]} 1_{[2;4]}) \\
& (2_{[1;4,(23)]} 2_{[1;7,(56)]} 2_{[1;1,(23)]} 2_{[1;4,(56)]} 2_{[1;7,(23)]} 2_{[1;1,(56)]}) \\
& (2_{[2;2,(36)]} 2_{[2;7,(45)]} 2_{[2;1,(36)]} 2_{[2;2,(45)]} 2_{[2;7,(36)]} 2_{[2;1,(45)]}) \\
& (3_{[1;(26)^1]} 3_{[1;(26)^2]} 3_{[1;(37)^1]} 3_{[1;(37)^2]}) \\
& (3_{[2;(46)^1]} 3_{[2;(46)^2]} 3_{[2;(35)^1]} 3_{[2;(35)^2]}) \\
& (4_{[1;4,2]} 4_{[1;5,3]} 4_{[1;6,7]}) (4_{[1;4,7]} 4_{[1;5,2]} 4_{[1;6,3]}) \\
& (4_{[2;3,2]} 4_{[2;4,6]} 4_{[2;5,7]}) (4_{[2;3,6]} 4_{[2;4,7]} 4_{[2;5,2]}); \text{ and} \\
Q_2 = & (1_{[1;6]} 2_{[1;4,(23)]} 4_{[1;5,3]}) (1_{[1;3]} 4_{[2;3,2]} 2_{[1;1,(56)]}) \\
& (1_{[1;5]} 4_{[1;6,7]} 4_{[2;5,7]} 1_{[1;4]} 3_{[2;(35)^1]} 3_{[2;(46)^1]}) \\
& (1_{[1;1]} 2_{[1;4,(56)]} 3_{[2;(46)^2]} 2_{[1;1,(23)]}) (1_{[2;2]} 2_{[2;7,(36)]} 3_{[1;(37)^1]}) \\
& (1_{[2;6]} 2_{[2;2,(36)]} 1_{[2;4]} 4_{[2;5,2]} 3_{[1;(37)^2]} 4_{[1;6,3]}) \\
& (1_{[2;5]} 4_{[1;4,7]} 2_{[2;2,(45)]} 4_{[2;4,7]}) (1_{[2;1]} 3_{[1;(26)^1]} 2_{[2;1,(36)]}) \\
& (2_{[1;7,(56)]} 4_{[2;4,6]} 4_{[1;4,2]} 2_{[1;7,(23)]} 3_{[2;(35)^2]}) \\
& (2_{[2;7,(45)]} 2_{[2;1,(45)]} 4_{[1;5,2]} 3_{[1;(26)^2]} 4_{[2;3,6]}).
\end{aligned}$$

The permutations  $Q_1$  and  $Q_2$  generate a group,  $\mathcal{G}$ . Alone,  $Q_1$  is transitive on each of the sets  $U_1[1], U_1[2], U_2[1], U_2[2], U_3[1]$ , and  $U_3[2]$ . Further,  $Q_2$  connects  $U_1[1]$  to  $U_2[1]$  and  $U_3[2]$ , and to the elements of the 1st and 3rd cycles of  $U_4$ s appearing in  $Q_1$ . This gives one orbit, for a transitive representation  $\mathcal{T}_1 : \mathcal{G} \rightarrow S_{21}$ . The remaining symbols fall in a second orbit of  $\mathcal{G}$ , giving the representation  $\mathcal{T}_2 : \mathcal{G} \rightarrow S_{21}$ . The image groups  $\mathcal{T}_i(\mathcal{G})$  are  $A_{21}$ ,  $i = 1, 2$ . The images of  $Q_i$  under both representations are conjugate in  $A_{21}$ ,  $i = 1, 2$ .

**TWO ORBITS RESULT.** *The above process gives two distinct connected families,  $\mathcal{H}_1$  and  $\mathcal{H}_2$ , of (2)(2) polynomial covers of degree 7. Each has monodromy group  $A_7$ . Further, take any set of three distinct points in  $\bar{\mathbb{Q}}$ . There are 21 distinct polynomial covers  $f : \mathbb{P}_y^1 \rightarrow \mathbb{P}_x^1$  (up to equivalence by linear change of the  $y$ -variable) in each family having those three points as branch points.*

*Part C: Properties of  $\mathcal{H}_1$  and  $\mathcal{H}_2$ .* Consider  $\mathcal{T}_1(Q_1)$  and  $\mathcal{T}_1(Q_2)$ , the permutations the braids give on the first orbit. As in Part E of Lemma 4.6, compute the elements  $a_{ij}$ . Simplify the subscripting notation by dropping the surrounding  $[\ ]$  and also be dropping reference to which of the  $U_j$  pairs the symbols belong. So



abbreviated, the following table gives the action of  $Q_1$  and  $Q_2$  on the  $\mathcal{T}_1$  symbols.

$$\begin{aligned}
Q_1 = & (1_6 1_3 1_5 1_1 1_4) \\
& (2_{4,(23)} 2_{7,(56)} 2_{1,(23)} 2_{4,(56)} 2_{7,(23)} 2_{1,(56)}) \\
& (3_{(46)^1} 3_{(46)^2} 3_{(35)^1} 3_{(35)^2}) \\
& (4_{4,2} 4_{5,3} 4_{6,7})(4_{3,2} 4_{4,6} 4_{5,7}); \text{ and} \\
Q_2 = & (1_6 2_{4,(23)} 4_{5,3})(1_3 4_{3,2} 2_{1,(56)}) \\
& (1_5 4_{6,7} 4_{5,7} 1_4 3_{(35)^1} 3_{(46)^1}) \\
& (1_1 2_{4,(56)} 3_{(46)^2} 2_{1,(23)})(2_{7,(56)} 4_{4,6} 4_{4,2} 2_{7,(23)} 3_{(35)^2}).
\end{aligned}$$

This allows the genus computation as previously.

(4.22a)

$$\begin{aligned}
a_{12} = Q_1^{-2} = & (1_6 1_1 1_3 1_4 1_5)(2_{4,(23)} 2_{7,(23)} 2_{1,(23)}) \\
& (2_{7,(56)} 2_{1,(56)} 2_{4,(56)})(3_{(46)^1} 3_{(35)^1})(3_{(46)^2} 3_{(35)^2}) \\
& (4_{4,2} 4_{5,3} 4_{6,7})(4_{3,2} 4_{4,6} 4_{5,7});
\end{aligned}$$

(4.22b)

$$\begin{aligned}
a_{13} = Q_1 Q_2^{-2} Q_1^{-1} = & (1_6 4_{5,7} 2_{7,(23)})(1_5 3_{(46)^1})(1_3 3_{(46)^2} 4_{4,6}) \\
& (1_1 4_{5,3} 3_{(35)^2})(1_4 2_{1,(56)} 4_{4,2})(2_{7,(56)} 2_{1,(23)}) \\
& (2_{4,(23)} 2_{4,(56)} 4_{3,2} 3_{(35)^1} 4_{6,7}); \text{ and}
\end{aligned}$$

(4.22c)

$$\begin{aligned}
(a_{12} a_{13})^{-1} = & (1_6 4_{5,3} 2_{4,(23)})(1_5 4_{5,7} 3_{(35)^1})(1_4 3_{(46)^1} 4_{6,7}) \\
& (1_3 2_{1,(56)} 4_{3,2})(1_1 3_{(46)^2})(2_{7,(23)} 2_{7,(56)}) \\
& (2_{7,(23)} 2_{7,(56)} 4_{4,2} 3_{(35)^2} 4_{4,6}).
\end{aligned}$$

As in Lemma 4.6, (4.22) is the branch cycles of a three branch point cover  $\mathcal{Z} \rightarrow \mathbb{P}^1$  of degree 21. Unlike (4.15), where the genus of  $\mathcal{Y}$  was 0, Riemann-Hurwitz gives the genus  $g(\mathcal{Z})$  of  $\mathcal{Z}$  as 1:  $2(21 + g(\mathcal{Z}) - 1) = 3 \cdot (21 - 7)$ .

*Part D: The locus of (4.16) and the genus 1 curve  $\mathcal{Z}$ .* There are four absolutely irreducible components of the locus of (4.16) when  $n = 7$ . Two of these are varieties whose function fields are the function fields of  $\mathcal{H}_1$  and  $\mathcal{H}_2$  with some rational parameters adjoined. These each parametrize a family of polynomials of degree 7 with geometric monodromy group  $A_7$ . If we can find members of either of these families over  $\mathbb{Q}$ , they give us  $(A_7, S_7)$  realizations by polynomials over  $\mathbb{Q}$ . We accomplish this if we can answer the following questions affirmatively. From [Fr1, Th. 5.1] or [FrV],  $\mathcal{H}_1$  and  $\mathcal{H}_2$  have a minimal field of definition  $K$  with  $[K : \mathbb{Q}] \leq 2$ .

**DISJOINT 2-CYCLE STATEMENT 4.8.** *If  $[K : \mathbb{Q}] = 2$ , then  $\mathcal{H}_1$  and  $\mathcal{H}_2$  are conjugate and there is no hope of getting an  $(A_7, S_7)$  realization from (2)(2) polynomials over  $\mathbb{Q}$ . If  $K = \mathbb{Q}$ , both  $\mathcal{H}_1$  and  $\mathcal{H}_2$  are unirational over  $\mathbb{Q}$  and*

they contain dense sets of  $\mathbb{Q}$  points. Each such  $\mathbb{Q}$  point provides a unique (2)(2) polynomial over  $\mathbb{Q}$ , producing an  $(A_7, S_7)$  realization.

PROOF. We have already given references for everything here, except the unirationality statement. We explain its proof and meaning. [Fr9] does an easier, but similar example where the analog there of  $\mathcal{Z}$  also has genus 1.

Let  $x_1^*, x_2^*, x_3^*$  be algebraically independent indeterminates over  $\mathbb{Q}$ , representing the finite branch points of a (2)(2) polynomial cover. The space  $\mathcal{H}_1$  is a cover of the space  $\mathbb{A}_0^3 = \mathbb{A}^3 \setminus D_3$  of unordered distinct triples that  $\mathbf{x}^* = (x_1^*, x_2^*, x_3^*)$  represent. That is, coordinates for  $\mathbb{A}^3$  are symmetric functions in the  $x_i^*$  s. The  $Q_i$  s come from generators of the fundamental group  $B_2$  of  $\mathbb{A}_0^3$ .

Transitive permutation representations of a fundamental group produce connected unramified covers of the space. The representations  $\mathcal{T}_1$  and  $\mathcal{T}_2$  are transitive, and the spaces  $\mathcal{H}_1$  and  $\mathcal{H}_2$  are the result of applying this theory [Fr1, §4]. The points of these spaces give coordinates for the coefficients of (2)(2) polynomials having  $A_7$  as monodromy group. From [Fr1, Th. 5.1], members of this family are in  $\mathbb{Q}$  if and only if  $\mathcal{H}^1$  or  $\mathcal{H}^2$  has a rational point. These manifolds can't have  $\mathbb{Q}$  points unless they have  $\mathbb{Q}$  as a field of definition. This happens if and only if  $\mathcal{H}_1$  and  $\mathcal{H}_2$  are not conjugate under the absolute Galois group of  $\mathbb{Q}$ . Now we describe the role of  $\mathcal{Z}$ .

The space  $\mathbb{A}^3 \setminus \Delta_3 = \mathbb{A}_{\mathbf{z}}^3$  of ordered triples of  $(x_1^*, x_2^*, x_3^*)$  naturally maps to  $\mathbb{A}_0^3$ . Choose  $x_2^*$  and  $x_3^*$  generically. Then, we may take the cover  $\phi : \mathcal{Z} \rightarrow \mathbb{P}_{x_1^*}^1$  arising from the branch cycles of (4.22) to ramify over  $x_2^*, x_3^*, \infty$ . The space  $\mathcal{Z}$  consists of the points of  $\mathcal{H}^1$  representing (2)(2) covers having finite branch points at  $x_2^*, x_3^*$  (and some 3rd point whose coordinate is a value of  $x_1^*$ ). Our computation determines that  $\mathcal{Z}$  is a genus 1 curve over  $K(x_2^*, x_3^*)$  with a degree 21 map to  $\mathbb{P}_{x_1^*}^1$ . Regarding  $x_2^*$  and  $x_3^*$  as variables, this gives a birational map generically finite-to-one,

$$(4.23) \quad \mathcal{Z} \times \mathbb{P}_{x_2^*}^1 \times \mathbb{P}_{x_3^*}^1 \rightarrow \mathcal{H}_1$$

sending  $(\mathbf{h}, x_2^*, x_3^*)$  to  $\mathbf{h} \in \mathcal{H}_1$ .

Here is the key observation. Let  $\lambda(x_1^*)$  be the affine function over  $K(x_2^*, x_3^*)$  that maps  $\infty$  to  $\infty$  and switches  $x_2^*$  and  $x_3^*$ . Form  $\lambda \circ \phi = \phi'$ . Then,

$$(4.24a) \quad \text{there exists an analytic isomorphism } \tau : \mathcal{Z} \rightarrow \mathcal{Z} \text{ for which } \phi' = \phi \circ \tau.$$

Here is the reason (see the  $A_5$  example of [Fr9] for details).

Over any given value of  $x_1^*$  the fibers of  $\phi$  and  $\phi'$  have points that correspond to exactly the same (2)(2) polynomial covers. Note: This is from transitivity of the  $a_{1j}$  s, a stronger property than transitivity of the  $Q_i$  s, on the symbols of the representation  $\mathcal{T}_1$ . Thus, (4.24a) gives us a cover

$$(4.24b) \quad \phi_\tau : \mathcal{Z}/\tau \rightarrow \mathbb{P}^1/\lambda$$

from the respective quotients of  $\mathcal{Z}$  and  $\mathbb{P}_{x_1}^1$ . The map  $\mu : \mathbb{P}^1 \rightarrow \mathbb{P}^1/\lambda$  ramifies. By counting the degrees of the maps,  $\phi$  is the pullback of  $\phi_\tau$  via  $\mu$ , so the natural map  $\mathcal{Z} \rightarrow \mathcal{Z}/\tau$  ramifies. The image of a ramified cover by a genus 1 curve is a genus 0 curve. Conclude:

(4.25)  $\mathcal{Z}/\tau$  is genus 0 and  $\phi_\tau$  has degree 21. The function field  $K(\mathcal{Z}/\tau, x_2^*, x_3^*)$  is pure transcendental over  $K$ , and it contains the function field of  $\mathcal{H}_1$ .

Use the argument at the end of Part E of the proof of Lemma 4.6 to see that degree 21 (odd) implies  $\mathcal{Z}/\tau$  provides one transcendental parameter. Expression (4.25), in particular, implies  $\mathcal{H}_1$  is unirational over  $K$ . This concludes the proof of Statement 4.8.

Compare the families of (2)(2) polynomials with group  $\mathrm{PSL}_3(\mathbb{Z}/2)$  and those with group  $A_7$ . For the former, there is an automorphism, given by a matrix  $M$  that takes the 7-cycle to its inverse. Since, however, no element of  $S_7$  represents this automorphism, the Branch Cycle Argument guarantees no polynomial in this family is in  $\mathbb{Q}[y]$ . Rather, every field of definition of a polynomial in this family contains  $Q(\zeta_7 + \zeta_7^2 + \zeta_7^4) = Q(\sqrt{-7})$ . This is the fixed field of the multiplier of a 7-cycle in  $\mathrm{PSL}_3(\mathbb{Z}/2)$ . For both types of polynomials, there are pure transcendental parameters we may specialize to achieve example polynomials.  $\square$

We purposely avoided braid actions and Hurwitz spaces up to Lemma 4.6 and Ex. 4.7 to keep the exposition elementary. Ex. 4.7, however, shows the benefit of the Hurwitz space approach. This turns the description of those examples into a computation with the Hurwitz monodromy group as in [FrV] and [Fr6-7].

SYNOPSIS OF UNSOLVED PROBLEMS 4.9. *One problem remains from Disjoint (2)(2) cycle Statement 4.8: Is  $K$  equal  $\mathbb{Q}$ . Here are others we consider worthy.*

- (4.26a) *Are the zeros of  $h_n(\alpha)/(\alpha - 1)^2$  all of degree exceeding 2 for odd  $n > 5$ .*  
 (4.26b) *Are there any  $(A_n, S_n)$  realizations by polynomials over  $\mathbb{Q}$  when  $n$  is an arbitrary odd square?*  
 (4.26c) *Are there (2)(2) polynomials over  $\mathbb{Q}$  when  $n > 7$  is odd?*

## REFERENCES

- [CaF] J. Fröhlich, *Local Ramification Theory*, Algebraic Number Theory, Acad. Press, London and New York, 1967, pp. 1-35.  
 [C] S. Cohen, *The distribution of polynomials over finite fields*, Acta. Arith. **17** (1970), 255-271.  
 [ChZ] S. Chowla and H. Zassenhaus, *Some conjectures concerning finite fields*, Norske Vid. Selsk. Forh. (Trondheim) **41** (1968), 34-35.  
 [DFr] P. Debes and M. Fried, *Arithmetic variation of fibers in families: Hurwitz monodromy criteria for rational points on all members of the family*, Crelles J. **409** (1990), 106-137.  
 [Fr1] M. Fried, *Fields of Definition of Function Fields and Hurwitz Families and; Groups as Galois Groups*, Communications in Algebra **5** (1977), 17-82.  
 [Fr2] M. Fried, *Galois groups and complex multiplication*, TAMS **235** (1978), 141-162.

- [Fr3] M. Fried, *Review of Serre's Topics in Galois Theory*, BAMS **30** #1 (1994), 124–135.
- [Fr4] M. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Ill. J. of Math. **17** (1973), 128–146.
- [Fr5] M. Fried, *On a conjecture of Schur*, Mich. Math. Journal **17** (1970), 41–55.
- [Fr6] M. Fried, *Exposition on an Arithmetic-Group Theoretic Connection via Riemann's Existence Theorem*, A.M.S. Publications, Proceedings of Symposia in Pure Math: Santa Cruz Conference on Finite Groups, vol. 37, 1980, pp. 571–601.
- [Fr7] M. Fried, *Rigidity and applications of the classification of simple groups to monodromy, Part II – Applications of connectivity; Davenport and Hilbert-Siegel Problems*, Preprint from 1986.
- [Fr8] M. Fried, *On Hilbert's irreducibility theorem*, J. Num. Th. **6** (1974), 211–232.
- [Fr9] M. Fried, *Arithmetic of 3 and 4 branch point covers: a bridge provided by noncongruence subgroups of  $SL_2(\mathbb{Z})$* , Progress in Math. Birkhauser, vol. 81, 1990, pp. 77–117.
- [FrV] M.D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli space*, Math. Ann. **290** (1991), 771–800.
- [GM] S. Gao and G. Mullen, *Dickson polynomials and irreducible polynomials over finite fields*, J. No. Theory **49** (1994), 118–132.
- [GT] R.M. Guralnick and J.G. Thompson, *Finite groups of genus zero*, J. Alg. **131** (1990), 303–341.
- [JK] G.D. James and A. Kerber, *The representation theory of the symmetric group*, Encyclopedia of Mathematics, vol. 16, Addison-Wesley, Reading, Mass., 1981.
- [MM] G. Malle and B.H. Matzat, *Inverse Galois Theory*, Near completion as of Jan. 1995.
- [Me] J.-F. Mestre, *Extensions régulières de  $\mathbb{Q}(T)$  de groupe de Galois  $\tilde{A}_n$* , J. Alg. **131** (1990), 483–495.
- [M] Peter Müller, *Recent developments in the inverse Galois problem*, Editor: Michael Fried, AMS, Cont. Math. Series, 1995.
- [RT] G. Robinson and J.G. Thompson, *Sums of squares and the fields  $\mathbb{Q}_{A_n}$* , preprint as of October 1994.
- [Se] J.-P. Serre, *Topics in Galois Theory*, ISBN 0-86720-210-6, Bartlett and Jones Publishers, 1992.
- [V] H. Voelklein, *Groups as Galois groups—the rigidity method*.
- [Wi] H. Wielandt, *Finite permutation groups*, Academic Press, 1964.

UC IRVINE, IRVINE, CA 92717, USA

*E-mail address:* mfried@math.uci.edu