Glasgow Mathematical Journal (2023), **65**, pp. 222–255
doi:10.1017/S0017089522000222

Glasgow
Mathematical
Journal

RESEARCH ARTICLE

Automorphism groups of endomorphisms of $\mathbb{P}^1(\bar{\mathbb{F}}_p)$

Julia Cai[1], Benjamin Hutz[2,*], Leo Mayer[3] and Max Weinreich[4]

[1]Department of Mathematics, Yale University, New Haven, CT 06520, USA, [2]Department of Mathematics and Statistics, Saint Louis University, St. Louis, MO 63103, USA, [3]Department of Mathematics, Lawrence University, Appleton, WI 54911, USA, [4]Department of Mathematics, Brown University, Providence, RI 02912, USA
*Corresponding author. E-mail: benjamin.hutz@slu.edu

Received: 18 August 2021; **Revised:** 6 June 2022; **Accepted:** 7 June 2022; **First published online:** 13 July 2022

Keywords: dynamical system, finite field, automorphism

2020 Mathematics Subject Classification: *Primary* - 37P25, 37P05, *Secondary* - 37P45

Abstract
For any algebraically closed field K and any endomorphism f of $\mathbb{P}^1(K)$ of degree at least 2, the automorphisms of f are the Möbius transformations that commute with f, and these form a finite subgroup of $\mathrm{PGL}_2(K)$. In the moduli space of complex dynamical systems, the locus of maps with nontrivial automorphisms has been studied in detail and there are techniques for constructing maps with prescribed automorphism groups that date back to Klein. We study the corresponding questions when K is the algebraic closure $\bar{\mathbb{F}}_p$ of a finite field. We use the classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ to show that every finite subgroup is realizable as an automorphism group. To construct examples, we use methods from modular invariant theory. Then, we calculate the locus of maps over $\bar{\mathbb{F}}_p$ of degree 2 with nontrivial automorphisms, showing how the geometry and possible automorphism groups depend on the prime p.

1. Introduction

Let K be an algebraically closed field. A dynamical system of degree d on the projective line is an endomorphism of $\mathbb{P}^1(K)$ and can be represented in coordinates as a pair of homogeneous polynomials of degree d with coefficients in K and no common factors. We assume throughout that $d \geq 2$. The set of all such dynamical systems is denoted Rat_d. There is a natural conjugation action on Rat_d by automorphisms of $\mathbb{P}^1$, the group PGL_2, given as:

$$f^\alpha = \alpha^{-1} \circ f \circ \alpha \quad \text{for } f \in \mathrm{Rat}_d \text{ and } \alpha \in \mathrm{PGL}_2.$$

The quotient by this action, see Silverman [15], is the *moduli space of dynamical systems of degree d*:

$$\mathcal{M}_d := \mathrm{Rat}_d/\mathrm{PGL}_2.$$

We use square brackets to distinguish between a map f in Rat_d and its conjugacy class $[f]$ in $\mathcal{M}_d$. An *automorphism* (or *symmetry*) of f is an element α of $\mathrm{PGL}_2(K)$ such that

$$f^\alpha = f.$$

The set of such α is a subgroup of $\mathrm{PGL}_2(K)$, called the *automorphism group* of f. We denote it $\mathrm{Aut}(f)$. Since these automorphisms have finite invariant sets of points, such as the periodic points of some fixed period, the automorphism group of a given map must be finite.

Our objects of study are those maps f for which $\mathrm{Aut}(f)$ is nontrivial: that is, those f which have an automorphism besides the identity. As is the case with elliptic curves that have complex multiplication, dynamical systems with nontrivial automorphisms can feature exceptional properties. For instance, a complex dynamical system with icosahedral symmetry was used to solve the quintic through iteration [6].

Max Weinreich was supported by a National Science Foundation Graduate Research Fellowship under Grant No. 2040433.

We will need to know how conjugation affects automorphism groups. Given $\sigma \in \mathrm{PGL}_2$, the conjugation action on $\mathrm{Aut}(f)$ defined by $\alpha \mapsto \alpha^\sigma$ defines a group isomorphism:

$$\mathrm{Aut}(f) \cong \mathrm{Aut}(f^\sigma).$$

The conjugacy class of $\mathrm{Aut}(f)$ in PGL_2 is, thus, a well-defined invariant of $[f]$. When we speak of the automorphism group associated with $[f]$, we understand this group to be well defined only up to conjugacy.

In particular, the locus of rational maps with a nontrivial automorphism group descends to a well-defined subset of $\mathcal{M}_d$. We call this set the *automorphism locus of* $\mathcal{M}_d$, denoted as $\mathcal{A}_d$. Note that conjugation may affect the field of definition of both the map and its automorphism group, and determining the minimal field of definition of a conjugacy class and/or its automorphism group can often be a delicate question, e.g., [4, 14].

In this article, we initiate the study of dynamical systems with nontrivial automorphisms over finite fields and their algebraic closures. Specifically, we address the following pair of questions:

(1) How can we construct examples of dynamical systems over $\bar{\mathbb{F}}_p$ with nontrivial automorphisms, and which automorphism groups can arise?
(2) What is the structure of the automorphism locus $\mathcal{A}_2$ in the moduli space $\mathcal{M}_2(\bar{\mathbb{F}}_p)$?

We fully resolve the realizability problem.

Theorem 1.1. *Every finite subgroup of* $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ *occurs as the automorphism group of some dynamical system.*

We do not place restrictions on the degrees of the maps which realize the automorphism groups. However, in many cases, we prove that the given map has the smallest degree among all maps of degree $d \geq 2$ that realize a given automorphism group. We say such a map is *of minimal degree* for that group. Explicit constructions and details are given in Theorems 1.6 and 1.7.

The methods used previously to construct dynamical systems with nontrivial automorphisms and to study automorphism loci depend on characteristic 0 in fundamental ways, opening the possibility that new phenomena emerge when we change the base field to a finite subfield of $\bar{\mathbb{F}}_p$. We investigate these new phenomena, emphasizing how our methods and results contrast with characteristic 0.

To provide context, we briefly describe some of what is known about $\mathcal{A}_d$ in the complex case. As mentioned earlier, the automorphism group is a finite subgroup of PGL_2, so the classification of such subgroups is important. In characteristic 0, the finite subgroups of PGL_2 were classified classically. For a modern exposition, see [14].

Notation 1.2. *We set notation for referring to various groups.*

- *Let 1 denote the trivial group.*
- *Let C_n denote the cyclic group of n elements, for each $n \geq 2$.*
- *Let D_{2n} denote the dihedral group of 2n elements, for each $n \geq 2$.*
- *Let A_4 denote the tetrahedral group.*
- *Let S_4 denote the octahedral group.*
- *Let A_5 denote the icosahedral group.*

The above are a complete list of finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$, up to conjugacy. The general problem of which subgroups of $\mathrm{PGL}_2(\mathbb{C})$ can be realized as an automorphism group for some $f \in \mathrm{Rat}_d$ relies on tools from the classical invariant theory of finite groups; see [4], as well as partial results found in a number of other places, such as [14].

The problem of determining the locus $\mathcal{A}_d(\mathbb{C})$ has been studied in a number of articles [9, 10, 12, 13, 20]. The automorphism locus $\mathcal{A}_d(\mathbb{C})$ forms a Zariski-closed proper subset of $\mathcal{M}_d(\mathbb{C})$. In fact, for

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

$d > 2$, the automorphism locus coincides with the singular locus of $\mathcal{M}_d(\mathbb{C})$ [12]. The case $d = 2$ stands in contrast: Milnor showed that $\mathcal{M}_2(\mathbb{C})$ is isomorphic as a variety to the affine plane $\mathbb{A}^2(\mathbb{C})$, which is smooth, and that the automorphism locus $\mathcal{A}_2(\mathbb{C})$ is a cuspidal cubic curve [13]. The points of $\mathcal{A}_2(\mathbb{C})$ all have an automorphism group isomorphic to C_2, except at the cusp, where the automorphism group is isomorphic to the symmetric group S_3. The descriptions of $\mathcal{A}_3(\mathbb{C})$ and $\mathcal{A}_4(\mathbb{C})$ are more recent and more complicated [10, 20]. The best results currently available for $\mathcal{A}_d(\mathbb{C})$ with $d \geq 5$ mostly focus on the dimensions of the various components [12].

We first study which automorphism groups are realizable. Among the finite subgroups Γ of PGL_2, which arise as automorphism groups of rational maps? We call this question the *realizability problem* for Γ. If Γ is realizable, so are its conjugates; thus, it suffices to look at one representative per conjugacy class. Our next theorems construct solutions to the realizability problem for every finite subgroup Γ of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$.

We first review what is known in the complex case. Miasnikov, Stout, and Williams [12] give the dimensions of the components of $\mathcal{A}_d(\mathbb{C})$ associated with each finite $\Gamma \subset \mathrm{PGL}_2(\mathbb{C})$. They do not, however, give any explicit realizations or explore arithmetic questions, such as the necessary field of definition. The strongest results in this direction come from de Faria and Hutz [4]. They prove that every finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$ is realizable as a subgroup of the automorphism group infinitely often (allowing the degree of the map to increase). This construction is explicit and relies on the classical invariant theory of finite groups.

In characteristic $p > 0$, much less is known. While the classification of finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is classical, the unpublished version by Faber [7] in modern notation is the most readable. For each prime p, each conjugacy class for each subgroup supplies a case of the realizability problem. We summarize the classification in Proposition 1.5.

Definition 1.3. *A finite subgroup of* $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ *is called p-regular if p does not divide the group order; otherwise, it is called p-irregular.*

Definition 1.4. *For each power q of a prime p, the Borel group* $B(\mathbb{F}_q)$ *is the group of upper triangular matrices in* $\mathrm{PGL}_2(\mathbb{F}_q)$*. A p-semi-elementary group is one that is the semi-direct product of a Sylow p-subgroup of order p and a cyclic subgroup.*

Proposition 1.5 (Faber [7]). *Let p be a prime. Each finite subgroup* Γ *of* $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ *belongs to one of the following isomorphism types:*

- *The identity group 1;*
- *The cyclic group* C_n*, for each* $n \geq 2$*;*
- *The dihedral group* D_{2n}*, for each* $n \geq 2$*;*
- *The tetrahedral group* A_4*;*
- *The icosahedral group* A_5*;*
- *The octahedral group* S_4*;*
- *The group* $\mathrm{PGL}_2(\mathbb{F}_q)$*, for some power q of p;*
- *The group* $\mathrm{PSL}_2(\mathbb{F}_q)$*, for some power q of p;*
- *A p-semi-elementary group conjugate to a subgroup of the Borel group* $B(\mathbb{F}_q)$*, for some power q of p.*

Except for p-semi-elementary groups, each possible isomorphism type occurs as at most one conjugacy class in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$*.*

For each power q of p, each subgroup of $B(\mathbb{F}_q)$ *is of the form:*

$$\{z \mapsto \alpha z + \beta : \alpha \in \mu,\ \beta \in \Lambda\},$$

where μ *is a subgroup of* $\mathbb{F}_q^\times$ *of some order n, and* Λ *is a subgroup of* $\mathbb{F}_q^+$ *such that* $\mu(\Lambda) \subseteq \Lambda$*. A subgroup of* $\mathrm{PGL}_2(\mathbb{F}_q)$ *is p-semi-elementary if and only if it is conjugate to a subgroup of* $B(\mathbb{F}_q)$ *for which* $\Lambda \neq 0$*.*

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

Not every group named in Proposition 1.5 appears for every prime, and for some small primes, there are accidental isomorphisms between some of the possible groups. The precise classification of subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ up to conjugacy is given in the Appendix.

The next two theorems resolve the realizability question for p-irregular and p-regular subgroups, respectively. Together, the theorems show by explicit constructions that every finite subgroup of PGL_2 arises as an automorphism group (Theorem 1.1). For certain groups, we show that our constructions furnish maps which are of minimal degree among all maps with the prescribed automorphism group.

Theorem 1.6. *Let p be a prime and let q be a power of p. Let Γ be a finite p-irregular subgroup of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. Then there exists a rational map $f{:}\mathbb{P}^1(\bar{\mathbb{F}}_p) \to \mathbb{P}^1(\bar{\mathbb{F}}_p)$ with $\mathrm{Aut}(f) = \Gamma$. In particular, such a map f can be constructed for each Γ as follows.*

(1) Let $f(z) = z^q$. Then $\mathrm{Aut}(f) = \mathrm{PGL}_2(\mathbb{F}_q)$, and f is of minimal degree for $\mathrm{PGL}_2(\mathbb{F}_q)$.

(2) Let Γ be a p-semi-elementary subgroup with associated additive group Λ and integer n in the form of Proposition 1.5. Then

$$f(z) = \prod_{\lambda\in\Lambda} (z-\lambda)^{n+1} + z$$

satisfies $\mathrm{Aut}(f) = \Gamma$. In particular, if $\Lambda = \mathbb{F}_q$, then

$$f(z) = (z^q - z)^{n+1} + z.$$

(3) If $p > 2$, then $\mathrm{PSL}_2(\mathbb{F}_q)$ is distinct from $\mathrm{PGL}_2(\mathbb{F}_q)$. In this case, there exists a map f such that

$$\mathrm{Aut}(f) = \mathrm{PSL}_2(\mathbb{F}_q).$$

We construct such an f of degree $\frac{1}{2}(q^3 - 2q^2 + q + 2)$. Consider the two fundamental invariants of $\mathrm{SL}_2(\mathbb{F}_q)$:

$$u = x^q y - xy^q,$$
$$c_1 = \sum_{n=0}^{q} x^{(q-1)(q-n)} y^{(q-1)n}.$$

Also set

$$a = \frac{q(q-3)+4}{2}, \qquad b = \frac{q-1}{2}.$$

Then take f to be the dynamical system that arises from the Doyle–McMullen construction (2.1) applied to $F = c_1^b$ and $G = u^a$; that is,

$$f(x,y) = \left[xc_1^b + \frac{\partial u^a}{\partial y} : yc_1^b - \frac{\partial u^a}{\partial x} \right].$$

This f is of minimal degree for $\mathrm{PSL}_2(\mathbb{F}_q)$.

(4) Let $p = 2$, and let $n \geq 3$ be odd. Then $f(z) = 1/z^{2n-1}$ has $\mathrm{Aut}(f) \cong D_{2n}$.

(5) Let $p = 3$. There is a unique p-irregular subgroup of $\mathrm{PGL}_2(\bar{\mathbb{F}}_3)$ isomorphic to A_5, up to conjugacy. There exists a map f such that $\mathrm{Aut}(f) \cong A_5$. Specifically, there is a representation of A_5 in $\mathrm{PGL}_2(\bar{\mathbb{F}}_3)$ with fundamental invariants:

$$u_1 = x^{10} + iy^{10},$$
$$u_2 = x^{11}y + (i+2)x^6y^6 - ixy^{11},$$

where $i \in \bar{\mathbb{F}}_3$ satisfies $i^2 + 1 = 0$. Let f be the dynamical system arising from the Doyle–McMullen construction (2.1) applied to $F = u_1^2$ and $G = u_1u_2$, that is,

$$f(x,y) = \left[xu_1^2 + \frac{\partial(u_1u_2)}{\partial y} : yu_1^2 - \frac{\partial(u_1u_2)}{\partial x} \right].$$

Then f has degree 21 and is of minimal degree for A_5 in $\mathrm{PGL}_2(\bar{\mathbb{F}}_3)$.

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

Theorem 1.7. *Let p be a prime and q a power of p. Let Γ be a p-regular subgroup of* $\mathrm{PGL}_2(\mathbb{F}_q)$. *Then there exists a rational map $f:\mathbb{P}^1(\bar{\mathbb{F}}_p) \to \mathbb{P}^1(\bar{\mathbb{F}}_p)$ with automorphism group exactly Γ. In particular, such a map f can be constructed for each Γ as follows.*

(1) The map $f(z) = z^2 + z$ has $\mathrm{Aut}(f) = 1$, and $f(z)$ is trivially of minimal degree for $\Gamma = 1$.
(2) Let $n \geq 2$ be relatively prime to p. Then the map $f(z) = \frac{1}{z^{n-1}} + z$ has $\mathrm{Aut}(f) \cong C_n$. Furthermore, this map is of minimal degree for C_n.
(3) Let $p > 2$ be prime and let $n \geq 2$ be coprime to p. The realizability problem for D_{2n} over $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ *is solvable through one of the following constructions:*

- *If $n \not\equiv -1 \mod p$, then the map $f(z) = z^{n+1}$ has exact automorphism group D_{2n}.*
- *If $n \not\equiv 1 \mod p$ and $n > 2$, then the map $f(z) = \frac{1}{z^{n-1}}$ has exact automorphism group D_{2n}. This example is of minimal degree for D_{2n}.*
- *If $n = 2$, then for every $a \in \bar{\mathbb{F}}_p$ not in the exceptional set* $\{-3, -1, 0, 1\}$, *the map*

$$f(z) = z \cdot \frac{z^2 + a}{az^2 + 1}$$

has $\mathrm{Aut}(f) \cong D_4$, *and $f(z)$ is of minimal degree for D_4.*

- *The tetrahedral group A_4 is realizable as an automorphism group of a degree 3 map over $\bar{\mathbb{F}}_p$, for all $p \geq 5$, and 3 is the minimal degree for A_4.*
- *The octahedral group S_4 is realizable as an automorphism group over $\bar{\mathbb{F}}_p$, for all $p \geq 5$.*
- *The icosahedral group A_5 is realizable as an automorphism group over $\bar{\mathbb{F}}_p$, for all $p \geq 7$.*

The invariant theory constructions used in de Faria and Hutz [4] go through in the p-regular case but remain unknown in the modular case (where the characteristic p divides the order of the group). Consequently, the methods used for our realizability results are a combination of adaptations of the invariant theory constructions and *ad hoc* computations. See the discussion at the beginning of Section 2.

For the p-regular case in Theorem 1.7, we take maps in characteristic 0 with the appropriate automorphism group and reduce modulo p; see Section 2.2. The p-irregular case in Theorem 1.6 is more elaborate. The work of Klein [11] and Doyle and McMullen [6] shows that the problem of creating maps over $\mathbb{C}$ with prescribed automorphism group can be framed in terms of classical invariant theory. In the case of characteristic p and a p-irregular group of automorphisms, we use modular invariant theory in place of classical invariant theory. Magma can calculate modular invariants [3]. By generating lots of invariants, we obtained a variety of maps which were candidates for realizing the subgroup in question. Throughout, there is the new difficulty that many maps with some prescribed automorphisms in fact have *extra* automorphisms; that is, the automorphism group is all of $\mathrm{PGL}_2(\mathbb{F}_q)$. We used the automorphism group calculation algorithm of Faber–Manes–Viray [8], which is implemented in Sage [19], to check exactness of the automorphism groups. Examining the computational evidence, we were able to conjecture general forms for solutions and prove them. See Section 2.1.

We next study the locus of maps in $\mathcal{A}_2(\bar{\mathbb{F}}_p)$ with a nontrivial automorphism. For a given point $x \in \mathcal{M}_d$, we freely write $\mathrm{Aut}(x) \cong G$ to mean that any map representing x has automorphism group isomorphic to G. Many subgroups of PGL_2 arise in just one conjugacy class, so such a description often suffices to describe the conjugacy class $\mathrm{Aut}(x)$.

To state the result, we use the explicit isomorphism $\mathcal{M}_2 \to \mathbb{A}^2$ given by $f \mapsto (\sigma_1, \sigma_2)$, where σ_1 and σ_2 are the first two elementary symmetric polynomials evaluated at the multipliers of the fixed points of f. This isomorphism was established over $\mathbb{C}$ by Milnor [13] and extended to an isomorphism of schemes over Spec $\mathbb{Z}$ by Silverman [15, Theorem 5.1].

Theorem 1.8. *The geometry of the automorphism locus $\mathcal{A}_2(\bar{\mathbb{F}}_p)$ depends on the prime p, in the following way.*

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

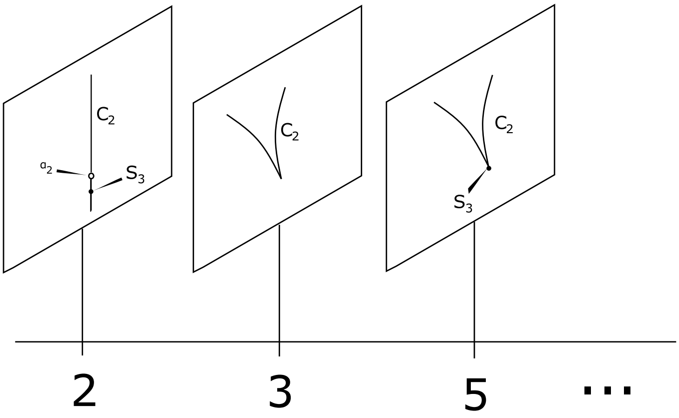

Figure 1. *Geometry of* $\mathcal{A}_2(\bar{\mathbb{F}}_p)$.

(1) $\boxed{p=2}$: *The automorphism locus* $\mathcal{A}_2(\bar{\mathbb{F}}_2)$ *is the line* $\sigma_1 = 0$. *For every point* $x = (\sigma_1, \sigma_2)$ *except* $(0, 0)$ *and* $(0, 1)$, *we have* $\mathrm{Aut}(x) \cong C_2$. *For* $x = (0, 0)$, *we have* $\mathrm{Aut}(x) \cong S_3$. *For* $x = (0, 1)$ *we have that* $\mathrm{Aut}(x)$ *is trivial as a subgroup of* PGL_2 *and isomorphic to* $\alpha_2 \cong \bar{\mathbb{F}}_2[t]/(t^2)$ *as a group scheme.*

(2) $\boxed{p=3}$: *The automorphism locus* $\mathcal{A}_2(\bar{\mathbb{F}}_3)$ *is the cuspidal cubic curve:*

$$2\sigma_1^3 + \sigma_1^2\sigma_2 - \sigma_1^2 - \sigma_2^2 - 2\sigma_1\sigma_2 = 0.$$

Every point x has $\mathrm{Aut}(x) \cong C_2$.

(3) $\boxed{p>3}$: *The automorphism locus* $\mathcal{A}_2(\bar{\mathbb{F}}_p)$ *is the cuspidal cubic curve:*

$$2\sigma_1^3 + \sigma_1^2\sigma_2 - \sigma_1^2 - 4\sigma_2^2 - 8\sigma_1\sigma_2 + 12\sigma_1 + 12\sigma_2 - 36 = 0.$$

Every point x except the cusp has $\mathrm{Aut}(x) \cong C_2$, *and when x is the cusp, we have* $\mathrm{Aut}(x) \cong S_3$.

We imagine this theorem in terms of the informal picture in Figure 1. As p varies, we obtain a family of curves. Automorphism groups that were possible in characteristic 0 can collapse when we reduce modulo certain small primes. This kind of behavior is typical in arithmetic geometry. More intriguing is, that without considering group schemes, the theorem over $\mathbb{C}$ that $\mathcal{A}_d$ is Zariski-closed fails in characteristic p. We can illustrate the phenomenon by the (dehomogenized) one-parameter family in $\mathrm{Rat}_2(\bar{\mathbb{F}}_2)$ defined by:

$$f_c(z) = z^2 + cz, \qquad c \in \bar{\mathbb{F}}_2.$$

We show in Section 4.2 that this family of rational maps forms a line in the moduli space and that the map $z \mapsto z + c - 1$ is an automorphism of f_c. This automorphism is nontrivial, unless $c = 1$, in which case the automorphism degenerates to the identity map. The reader can readily check that $\mathrm{Aut}(f_1)$ is trivial as a subgroup of PGL_2. In Section 4.2, we compute the automorphism group scheme [8] of f_1 and find that it is the well-known group scheme α_2. While the group of α_2 is trivial, its group scheme structure is not.

Question 1.9. As the map f_c varies, so does the nontrivial automorphism it carries. Can we create a moduli space that parametrizes rational maps with a choice of automorphism, and would the analog of $\mathcal{A}_d$ in this moduli space be a Zariski-closed set? (This line of inquiry was suggested to us by Joseph Silverman.)

The structure of the article is as follows. In Section 2, we study the realizability problem and prove Theorems 1.6 and 1.7. This section starts with an introduction to the methods and proceeds through the cases of p-irregular followed by p-regular. In Section 3, we adapt the structure theorem of Doyle and McMullen [6] to the setting of modular invariant theory, and we prove that our example for $\mathrm{PSL}_2(\mathbb{F}_q)$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

is of minimal degree, Theorem 1.6(3). In Section 4, we study the structure of $\mathcal{A}_d \subset \mathcal{M}_d$ and prove Theorem 1.8.

The authors thank the Institute for Computational and Experimental Mathematical Research (ICERM) for hosting the summer Research Experience for Undergraduates (REU) program in 2019, where the majority of this work was completed. We also thank Xander Faber and Joseph Silverman for helpful conversations and an anonymous referee for many helpful and detailed comments.

2. Realizability

In considering the realizability problem, our constructions are best understood in contrast to the resolution of the realizability problem over $\mathbb{C}$, which we sketch. This story spans centuries: it starts with Klein's beautiful lectures on the icosahedron [11], is continued in Doyle and McMullen's work on the quintic [6], and concludes in the recent paper by de Faria and Hutz [4].

If f is a solution for the realizability problem for Γ, then for any $\sigma \in \mathrm{PGL}_2$, the conjugated map $\sigma^{-1} \circ f \circ \sigma$ is a solution for $\sigma^{-1}\Gamma\sigma$. So, to solve the realizability problem in general, we need only consider one representative of each conjugacy class of Γ in PGL_2. The finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ were classified up to conjugacy by Klein [11]; a more modern version can be found in Silverman [14]. The finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ belong to one of the following isomorphism types:

- a cyclic group C_n;
- a dihedral group D_{2n};
- the tetrahedral group A_4;
- the octahedral group S_4;
- the icosahedral group A_5.

Each isomorphism type arises as just one conjugacy class in $\mathrm{PGL}_2(\mathbb{C})$.

Klein's strategy for creating maps with symmetry rested on what is now known as the classical invariant theory of finite groups. Roughly, classical invariant theory is an algorithm which takes as input a $\mathbb{C}$-vector space V and a group representation $\Gamma \hookrightarrow \mathrm{GL}(V)$ and outputs information about the homogeneous elements of the polynomial algebra $\mathbb{C}[V]$ which are fixed by all the transformations in Γ. In other words, classical invariant theory calculates the set of homogeneous $F \in \mathbb{C}[V]$ such that for all $\gamma \in \Gamma$, we have

$$F \circ \gamma = F.$$

The set of such F forms a ring, called the *ring of polynomial invariants*, and is denoted $\mathbb{C}[V]^\Gamma$. A basic method used in classical invariant theory to furnish polynomial invariants is to use the Reynolds operator, which is the projection $\mathbb{C}[V] \to \mathbb{C}[V]^\Gamma$ defined by:

$$F \mapsto \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma} (F \circ \gamma).$$

The first interesting example takes $V = \mathbb{C}^2$ and Γ to be the representation of C_2, that maps the nonidentity element to $\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right]$. Then, $\mathbb{C}[V]^\Gamma$ is the ring of homogeneous symmetric polynomials in two variables.

Klein found, and the reader may directly check, that given a homogeneous polynomial in two variables invariant under the action of Γ, i.e., $G \in \mathbb{C}[V]^\Gamma$, the map $f : \mathbb{P}^1 \to \mathbb{P}^1$ defined in coordinates by

$$[x : y] \mapsto \left[\frac{\partial G}{\partial y} : -\frac{\partial G}{\partial x}\right]$$

satisfies $\Gamma \subseteq \mathrm{Aut}(f)$. Doyle and McMullen derived another more general construction, again using classical invariant theory, which creates maps with automorphism group containing Γ [6]. Specifically, given two invariants F,G with degrees satisfying $\deg(G) = \deg(F) + 2$ (or $F = 0$), the map is given by:

$$[x : y] \mapsto \left[xF + \frac{\partial G}{\partial y} : yF - \frac{\partial G}{\partial x} \right]. \tag{2.1}$$

They also prove analytically that every dynamical system with automorphism group containing Γ arises from their construction. With this machine for creating dynamical systems with symmetries, the only concern is that we might not exactly have $\Gamma = \mathrm{Aut}(f)$. To be sure we have a solution to the realizability problem, we must check against the existence of *extra automorphisms*. De Faria and Hutz [4] used this machinery to solve the realizability problem over $\mathbb{C}$ as well as to produce infinite families where every member of the family has automorphism group containing Γ.

Now we replace the base field $\mathbb{C}$ by $\bar{\mathbb{F}}_p$ and explain how the above story morphs at each step:

- As shown by the classification of Faber [7], there are many more conjugacy classes to test.
- If Γ is p-regular, the same formula for the Reynolds operator works, and much of the classical theory over $\mathbb{C}$ carries over with minor modification. But if Γ is p-irregular, the Reynolds operator is unavailable, and it can be computationally more difficult to locate polynomial invariants. This suggests the basic dichotomy present in modern commutative algebra between *modular invariant theory* (the case where p divides $|\Gamma|$) and its complement *nonmodular invariant theory*. For an excellent reference that emphasizes this dichotomy, see [18]. Our investigation opens a new field of application for modular invariant theory. In particular, any work on the realizability problem in higher dimensions will probably require a deeper description of modular invariants than is presently available.
- The Klein and Doyle–McMullen constructions, which are the bridge from invariant theory to dynamics, may fail for various reasons in characteristic p. For instance, if we attempt the Doyle–McMullen construction with $F(x, y) = 0$, $G(x, y) = x^p + y^p$, we obtain the nonsense map $[0 : 0]$. Evidently, some constraints on degree are necessary. Even so, if the construction actually produces a valid map of degree at least 2, then it is easy to check that $\Gamma \subseteq \mathrm{Aut}(f)$.

  The converse—that all maps with $\Gamma \subseteq \mathrm{Aut}(f)$ arise from the Doyle–McMullen construction—is much harder to see, and some subtleties particular to positive characteristic arise. We build up the theory of this correspondence in Section 3, with our analogue of the Doyle–McMullen correspondence presented as Theorem 3.2.
- Over $\mathbb{C}$, the central task is writing down an example f such that $\Gamma \subseteq \mathrm{Aut}(f)$, and the problem of extra automorphisms has been addressed for a few special cases. Over $\bar{\mathbb{F}}_p$, the problem of extra automorphisms is in some sense the whole point. We will see that the automorphism group of $f(z) = z^q$ is $\mathrm{PGL}_2(\mathbb{F}_q)$, and every finite subgroup Γ of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is contained in $\mathrm{PGL}_2(\mathbb{F}_q)$ for a large enough choice of q. For each prime power q, this gives us a single example f such that $\Gamma \subseteq \mathrm{Aut}(f)$ for every finite subgroup Γ of $\mathrm{PGL}_2(\mathbb{F}_q)$. So, the difficulty arises in how to create maps f with some prescribed symmetries without picking up lots of others.

The following essential proposition, due to Faber, Manes and Viray, links the existence of automorphisms of certain order to the degree of the map.

Proposition 2.1 ([8], Proof of Proposition 2.4). *Let p be a prime, let $n \in \mathbb{N}$, and let $f{:}\mathbb{P}^1 \to \mathbb{P}^1$ be a rational map over $\bar{\mathbb{F}}_p$ admitting an automorphism of order n. Then,*

$$\deg(f) \equiv -1, 0, 1 \mod n. \tag{2.2}$$

If $n = p$, then up to conjugation, we further have $f(z) = \psi(z^p - z) + z$ for some rational map ψ, and

$$\deg(f) \equiv 0, 1 \mod p. \tag{2.3}$$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

2.1. *Realizability of p-irregular subgroups of* $\mathrm{PGL}_2(\mathbb{F}_q)$

2.1.1. *Realizing* $\mathrm{PGL}_2(\mathbb{F}_q)$

We now show that, for any power q of a prime p, the group $\mathrm{PGL}_2(\mathbb{F}_q)$ is realizable over $\mathbb{F}_p$.

Proof of Theorem 1.6 part 1. Let $f(z) = z^q$. For any rational map $g \in \bar{\mathbb{F}}_q(z)$, we have $g(z^q) = g(z)^q$ if and only if g is defined over $\mathbb{F}_q$. Restricting g to be degree 1, we find that $\mathrm{Aut}(f) = \mathrm{PGL}_2(\mathbb{F}_q)$. We further claim that any map with degree at least 2 and with automorphism group $\mathrm{PGL}_2(\mathbb{F}_q)$ has degree at least q. To see this, let g be a such a map. Up to conjugation by an element of $\mathrm{PGL}_2(\mathbb{F}_q)$, we may assume that g has an affine fixed point. Let $a \in \mathbb{F}_q$ be an affine fixed point of g. For every $b \in \mathbb{F}_q$, we have an automorphism $z \mapsto z + b$ of g, so every point of the form $a + b$ where $b \in \mathbb{F}_q$ is fixed by g. Since g has at least q fixed points, we deduce that $\deg g \geq q - 1$. Further, since g has an automorphism of order p, we know that $\deg g \equiv 0$ or $\deg g \equiv 1 \pmod{p}$, by (2.3). We conclude that $\deg g \geq q$. □

Somewhat surprisingly, for any prime power q, the map $\frac{1}{z^q}$ also has automorphism group isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$, because z^q is conjugate to $\frac{1}{z^q}$. In fact, it is a quadratic twist.

Proposition 2.2. *For any prime power q, let ζ_{q+1} be a primitive $(q+1)$-th root of unity, and let $\tau = \begin{pmatrix} 1 & \zeta_{q+1} \\ \zeta_{q+1} & 1 \end{pmatrix}$. Then, $\tau \in \mathrm{PGL}_2(\mathbb{F}_{q^2})$ and conjugation by τ maps $f(z) = z^q$ to $f^\tau(z) = \frac{1}{z^q}$.*

Proof. Checking the conjugation is a simple calculation, and ζ_{q+1} is in a quadratic extension of $\mathbb{F}_q$ because $\mathbb{F}_{q^2}^*$ is cyclic of order $q^2 - 1 = (q-1)(q+1)$. □

It turns out that there are many elements of $\mathrm{PGL}_2(\mathbb{F}_{p^2})$ that conjugate z^q to $\frac{1}{z^q}$. This can be explained by the following result.

Proposition 2.3. *Let $f, g \in \mathrm{Rat}_d$ be in the same conjugacy class. Then the set $\mathrm{Conj}(f, g)$ of all conjugations from f to g is a right coset of $\mathrm{Aut}(f)$.*

Proof. Let $\tau \in \mathrm{Conj}(f, g)$. We must show that $\mathrm{Aut}(f) \circ \tau = \mathrm{Conj}(f, g)$. For the first containment, let $\beta \in \mathrm{Aut}(f)$. Then $f^{\beta\circ\tau} = (f^\beta)^\tau = f^\tau = g$, and so $\beta \circ \tau \in \mathrm{Conj}(f, g)$. □

For the reverse containment, it suffices to show that for all $\tau, \beta \in \mathrm{Conj}(f, g)$, we have $\tau \circ \beta^{-1} \in \mathrm{Aut}(f)$. This holds, since $f^{\tau\circ\beta^{-1}} = (f^\tau)^{\beta^{-1}} = g^{\beta^{-1}} = f$.

2.1.2. *Realizing p-semi-elementary subgroups*

Proof of Theorem 1.6 part (2). Let Γ be a p-semi-elementary subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$. For the purposes of the realizability problem, we can replace Γ by a conjugate. Then by the classification of Faber [7], as presented in Proposition 1.5, we can assume that Γ has the following form:

- The group Γ is a subgroup of the Borel group; that is, all its elements are of the form $z \mapsto az + b$.
- For any integer $n \geq 1$, let μ_n denote the multiplicative group of n-th roots of unity in $\bar{\mathbb{F}}_p$. There is an additive group $\Lambda \subseteq \mathbb{F}_q$ and an integer $n \geq 1$ such that
$$\Gamma = \{z \mapsto az + b : a \in \mu_n, b \in \Lambda\}.$$
- Multiplication by elements of μ_n maps Λ into Λ.

Let

$$f(z) = \prod_{\lambda\in\Lambda} (z - \lambda)^{n+1} + z.$$

Then we claim $\mathrm{Aut}(f) = \Gamma$. Say $\tau \in \Gamma$. Then τ is given by $\tau(z) = az + b$ for some a, b where $b \in \Lambda$ and $a \in \mu_n$. The following sequence of equalities is justified by re-indexing the product twice:

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

$$\begin{aligned}f(\tau(z)) &= \prod_{\lambda\in\Lambda}(az+b-\lambda)^{n+1}+az+b\\ &= \prod_{\lambda\in\Lambda}(az-\lambda)^{n+1}+az+b\\ &= a^{n+1}\prod_{\lambda\in\Lambda}(z-\lambda/a)^{n+1}+az+b\\ &= a\prod_{\lambda\in\Lambda}(z-\lambda/a)^{n+1}+az+b\\ &= a\prod_{\lambda\in\Lambda}(z-\lambda)^{n+1}+az+b\\ &= \tau(f(z)).\end{aligned}$$

Thus, $\Gamma \subseteq \mathrm{Aut}(f)$. Now we prove the reverse containment. Suppose that $\tau \in \mathrm{Aut}(f)$. The fixed points of f are $\Lambda \cup \{\infty\}$. The multiplier at ∞ is 0 because ∞ is a critical point, and the multiplier at each point of Λ is 1 (since $n \geq 1$). Then τ must fix ∞, since it is the only fixed point of f with multiplier 0, so τ is of the form $z \mapsto az + b$. Now we must show that b is in Λ and that a is in μ_n. We consider the equality of polynomials given by $f(\tau(z)) = \tau(f(z))$:

$$f(az+b) = af(z) + b.$$

The leading coefficient on the left side is a^{n+1}, and the leading coefficient on the right is a, so a is an n-th root of unity. Expanding the equality of polynomials,

$$a\prod_{\lambda\in\Lambda}(z+b/a-\lambda/a)^{n+1}+az+b = a\prod_{\lambda\in\Lambda}(z-\lambda)^{n+1}+az+b.$$

Simplifying, we have

$$\prod_{\lambda\in\Lambda}(z+b/a-\lambda/a)^{n+1} = \prod_{\lambda\in\Lambda}(z-\lambda)^{n+1}.$$

Then $z \mapsto az + b$ must map Λ to Λ bijectively. The map $z \mapsto z/a$ is also bijective, so composing, we find that $z \mapsto z + b$ maps Λ to Λ. Therefore, $b \in \Lambda$, completing the proof. □

2.1.3. Realizing $\mathrm{PSL}_2(\mathbb{F}_q)$

We now show how to realize $\mathrm{PSL}_2(\mathbb{F}_q)$, where q is a power of an odd prime p. We assume $p > 2$ to ensure that $\mathrm{PSL}_2(\mathbb{F}_q) \neq \mathrm{PGL}_2(\mathbb{F}_q)$.

Proof of Theorem 1.6 part (3). We begin with the fundamental invariants of $\mathrm{PSL}_2(\mathbb{F}_q)$:

$$\begin{aligned}u &= x^q y - xy^q,\\ c_1 &= \sum_{n=0}^{q} x^{(q-1)(q-n)}y^{(q-1)n},\end{aligned}$$

which have degree $q + 1$ and $q^2 - q$, respectively (see, for instance, [2]).

The Doyle–McMullen construction [6] takes two invariant homogeneous polynomials F and G of some $\Gamma \subseteq \mathrm{PGL}_2$ and outputs a map with $\Gamma \subseteq \mathrm{Aut}(f)$. We generalize this construction to characteristic $p > 0$ in Theorem 3.2. For invariants F and G, the corresponding map on projective space is $f = [xF + G_y : yF - G_x]$, where G_y and G_x are the partial derivatives.

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

Applying this construction to $G = u^a$ and $F = c_1^b$, with a and b as given in the statement of the theorem and using that $a \equiv 1 \mod p$, we obtain the map:

$$f(x,y) = \left[x\left(\sum_{n=0}^{q} x^{(q-1)(q-n)}y^{(q-1)n}\right)^{b} + (x^q y - xy^q)^{a-1}x^q : \right.$$
$$\left. y\left(\sum_{n=0}^{q} x^{(q-1)(q-n)}y^{(q-1)n}\right)^{b} - (x^q y - xy^q)^{a-1}y^q \right].$$

Next, we calculate the fixed points of f:

$$\begin{aligned}
& f(x,y) = [x:y] \\
\iff \quad & y\left(x\left(\sum_{n=0}^{q} x^{(q-1)(q-n)}y^{(q-1)n}\right)^{b} + (x^q y - xy^q)^{a-1}x^q \right) \\
& \quad = x\left(y\left(\sum_{n=0}^{q} x^{(q-1)(q-n)}y^{(q-1)n}\right)^{b} + (x^q y - xy^q)^{a-1}y^q \right) \\
\iff \quad & (x^q y - xy^q)^{a-1}x^q y = (x^q y - xy^q)^{a-1}xy^q \\
\iff \quad & (x^q y - xy^q)^{a-1}(x^q y - xy^q) = (x^q y - xy^q)^a = 0.
\end{aligned}$$

Setting $y = 1$, we see that the fixed points are the roots of $(x^q - x)^a$, or the elements of $\mathbb{F}_q$, each with multiplicity a. Likewise, $y = 0$ is a solution, so infinity is a fixed point with multiplicity a.

We know that $\mathrm{PSL}_2(\mathbb{F}_q) \subseteq \mathrm{Aut}(f)$ by construction. It remains to show equality. Using the assumption $p > 2$, let α be any non-square element of $\mathbb{F}_q$. Then $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$ corresponds to the map $\tau(x,y) = [\alpha x : y]$. We claim that $\tau \notin \mathrm{Aut}(f)$. Indeed, we compute

$$\begin{aligned}
f^{\tau} = & \left[\frac{1}{\alpha}\left(\alpha x\left(\sum_{n=0}^{q} (\alpha x)^{(q-1)(q-n)}y^{(q-1)n}\right)^{b} + ((\alpha x)^q y - (\alpha x)y^q)^{a-1}((\alpha x)^q) \right) : \right. \\
& \left. y\left(\sum_{n=0}^{q} (\alpha x)^{(q-1)(q-n)}y^{(q-1)n})\right)^{b} + ((\alpha x)^q y - (\alpha x)y^q)^{a-1}y^q \right] \\
= & \left[x\left(\sum_{n=0}^{q} x^{(q-1)(q-n)}y^{(q-1)n}\right)^{b} + \alpha^{a-1}(x^q y - xy^q)^{a-1}x^q : \right. \\
& \left. y\left(\sum_{n=0}^{q} x^{(q-1)(q-n)}y^{(q-1)n}\right)^{b} + \alpha^{a-1}(x^q y - xy^q)^{a-1}y^q \right].
\end{aligned}$$

Thus, we see that $f^{\tau} = f \iff \alpha^{a-1} = 1$. Since $a = \frac{q(q-3)+4}{2}$,

$$\begin{aligned}
a - 1 = \frac{q(q-3)+2}{2} &= \frac{(q-1)(q-2)}{2} \\
\implies \alpha^{a-1} &= (\alpha^{\frac{q-1}{2}})^{q-2} = (-1)^{q-2} = -1.
\end{aligned}$$

Therefore, $f^{\tau} \neq f$.

Since f has $q+1$ fixed points, we have $|\mathrm{Aut}(f)| \leq (q+1)q(q-1)$. Further, since $z \mapsto \alpha z$ induces a self-map of $\mathrm{Fix}(f)$ but is not an automorphism of f, the inequality is strict. Since $\mathrm{Aut}(f)$ contains $\mathrm{PSL}_2(\mathbb{F}_q)$, we have

$$\frac{(q+1)q(q-1)}{2} \leq |\mathrm{Aut}(f)| < (q+1)q(q-1). \tag{2.4}$$

Since Aut(f) contains $\mathrm{PSL}_2(\mathbb{F}_q)$, it is a p-irregular group that does not stabilize any subset of $\mathbb{P}^1(\bar{\mathbb{F}}_q)$ of cardinality 1 or 2. By the classification of finite subgroups (see the Appendix), if $p \neq 3$, the only such groups are isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{q'})$ or $\mathrm{PSL}_2(\mathbb{F}_{q'})$ for some power $q' \geq q$ of p, and among these, the only isomorphism type satisfying (2.4) is $\mathrm{PSL}_2(\mathbb{F}_q)$. If $p = 3$, the same argument applies, but we must also rule out the isomorphism type A_5. But the order of A_5 is 60, which does not satisfy (2.4) for any power q of 3.

The final claims to verify are that

$$\deg f = \frac{1}{2}(q^3 - 2q^2 + q + 2), \tag{2.5}$$

and that this f is of minimal degree for $\mathrm{PSL}_2(\mathbb{F}_q)$. In Theorem 3.3, we show that any map f with $\deg f > 1$ and $\mathrm{Aut}(f) \cong \mathrm{PSL}_2(\mathbb{F}_q)$ has degree at least $\frac{1}{2}(q^3 - 2q^2 + q + 2)$. The formula for f shows that $\deg f \leq \frac{1}{2}(q^3 - 2q^2 + q + 2)$. The set of fixed points has cardinality $q+1$, so $\deg f > 1$, proving (2.5). □

Theorem 1.6 part (3) is rather cumbersome, and it is difficult to understand the maps arising from the invariants. In the case where $q = p$, we have the following simplified version.

Theorem 2.4. *Let $p > 2$ be prime, let $m = \frac{1}{2}p^2 - \frac{3}{2}p + 2$, and let $c \neq 0$, and let*

$$\psi(z) = \frac{cz^m}{(z^{p-1}+1)^{\frac{p-1}{2}} + cz^{m-1}}.$$

Then the automorphism group of $f(z) = \psi(z^p - z) + z$ is exactly $\mathrm{PSL}_2(\mathbb{F}_p)$.

Proof. We check that the generators of $\mathrm{PSL}_2(\mathbb{F}_p)$, which are $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$, where α is a quadratic residue in $\mathbb{F}_p$, are all automorphisms of f. We also need to show that $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ is not an automorphism of f when α is a non-residue.

For $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, we compute

$$f(z+1) - 1 = \psi((z+1)^p - (z+1)) + (z+1) - 1 = \psi(z^p - z) + z = f.$$

We next check maps of the form $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$. This is an automorphism if and only if $f(\alpha z) = \alpha f(z)$. This holds if and only if

$$0 = f(\alpha z) - \alpha f(z) = \alpha\psi(z^p - z) - \psi(\alpha(z^p - z)). \tag{2.6}$$

Making the substitution $w = z^p - z$, we see equation (2.6) holds if and only if

$$\begin{aligned} 0 = \alpha\psi(w) - \psi(\alpha w) &= \frac{\alpha c w^m}{(w^{p-1}+1)^{\frac{p-1}{2}} + cw^{m-1}} - \frac{c\alpha^m w^m}{(\alpha^{p-1}w^{p-1}+1)^{\frac{p-1}{2}} + c\alpha^{m-1}w^{m-1}} \\ &= (c\alpha w^m)\left(\frac{1}{(w^{p-1}+1)^{\frac{p-1}{2}} + cw^{m-1}} - \frac{\alpha^{m-1}}{(\alpha^{p-1}w^{p-1}+1)^{\frac{p-1}{2}} + c\alpha^{m-1}w^{m-1}}\right). \end{aligned}$$

Keeping in mind that $\alpha^{p-1} = 1$, this is equivalent to

$$\begin{aligned} 0 &= (\alpha^{p-1}w^{p-1}+1)^{\frac{p-1}{2}} + c\alpha^{m-1}w^{m-1} - \alpha^{m-1}(w^{p-1}+1)^{\frac{p-1}{2}} - \alpha^{m-1}cw^{m-1} \\ &= (1-\alpha^{m-1})(w^{p-1}+1)^{\frac{p-1}{2}}. \end{aligned}$$

Thus, $\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ is an automorphism of f if and only if $\alpha^{m-1} = 1$. We have

$$\alpha^{m-1} = \alpha^{\frac{(p-1)(p-2)}{2}}$$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

and the order of α is $\mathbb{F}_p$ must be a divisor of $p-1$. So $\alpha^{m-1}=1$ if and only if $\alpha^{\frac{p-1}{2}}=1$, which, by Euler's criterion, is equivalent to α being a quadratic residue.

It remains to check that $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is an automorphism. To simplify the computations, we introduce the variables $x=z^p-z$, $y=z^{p+1}$. We need $\frac{-1}{f(z)}-f(\frac{-1}{z})=0$. We have

$$\frac{-1}{f(z)}-f\left(\frac{-1}{z}\right)=\frac{-1}{\psi(z^p-z)+z}-\psi\left(-\frac{1}{z^p}+\frac{1}{z}\right)+\frac{1}{z}=\frac{-1}{\psi(x)+z}-\psi\left(\frac{x}{y}\right)+\frac{1}{z},$$

which vanishes if and only if

$$z(\psi(x)+z)\psi\left(\frac{x}{y}\right)-\psi(x)=0.$$

Now

$$\begin{aligned}
&z(\psi(x)+z)\psi\left(\frac{x}{y}\right)-\psi(x)\\
&\quad=z\left(\frac{cx^m}{(x^{p-1}+1)^{\frac{p-1}{2}}+cx^{m-1}}+z\right)\left(\frac{c(\frac{x}{y})^m}{((\frac{x}{y})^{p-1}+1)^{\frac{p-1}{2}}+c(\frac{x}{y})^{m-1}}\right)-\frac{cx^m}{(x^{p-1}+1)^{\frac{p-1}{2}}+cx^{m-1}}\\
&\quad=z\left(\frac{cx^m}{(x^{p-1}+1)^{\frac{p-1}{2}}+cx^{m-1}}+z\right)\left(\frac{cx^m}{y^m((\frac{x}{y})^{p-1}+1)^{\frac{p-1}{2}}+cyx^{m-1}}\right)-\frac{cx^m}{(x^{p-1}+1)^{\frac{p-1}{2}}+cx^{m-1}},
\end{aligned}$$

which vanishes precisely with

$$\begin{aligned}
&cx^m\left[cx^mz+z^2\left((x^{p-1}+1)^{\frac{p-1}{2}}+cx^{m-1}\right)-y^m\left(\left(\frac{x}{y}\right)^{p-1}+1\right)^{\frac{p-1}{2}}-cyx^{m-1}\right]\\
&\qquad=cx^m\left[cx^{m-1}(zx+z^2-y)+z^2\left((x^{p-1}+1)^{\frac{p-1}{2}}\right)-y^{\frac{-p+3}{2}}(x^{p-1}+y^{p-1})^{\frac{p-1}{2}}\right]. \qquad (2.7)
\end{aligned}$$

Now we use the following two identities:

$$\begin{gathered}
y=zx+z^2\\
x^{p-1}+y^{p-1}=z^{p-1}(x^{p-1}+1).
\end{gathered}$$

The first identity is trivial, and the second follows from the expansion:

$$x^{p-1}\equiv z^{p(p-1)}+z^{(p-1)(p-1)}+z^{(p-2)(p-1)}+z^{(p-3)(p-1)}+\cdots+z^{p-1} \pmod{p},$$

using that $\binom{p-1}{k}\equiv(-1)^k \pmod{p}$ for $1\leq k\leq p-1$. With these identities, (2.7) becomes

$$\begin{aligned}
&cx^m\left[z^2\left((x^{p-1}+1)^{\frac{p-1}{2}}\right)-y^{\frac{-p+3}{2}}z^{\frac{(p-1)^2}{2}}(x^{p-1}+1)^{\frac{p-1}{2}}\right]\\
&\quad=cx^m(x^{p-1}+1)^{\frac{p-1}{2}}\left[z^2-z^{\frac{(p+1)(-p+3)}{2}+\frac{(p-1)^2}{2}}\right]\\
&\quad=cx^m(x^{p-1}+1)^{\frac{p-1}{2}}\left[z^2-z^2\right]=0.
\end{aligned}$$

Thus, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ is indeed an automorphism.

We have so far shown

$$\mathrm{PSL}_2(\mathbb{F}_p)\subseteq\mathrm{Aut}(f)\subsetneq\mathrm{PGL}_2(\mathbb{F}_q).$$

To show that $\mathrm{Aut}(f)$ is not equal to any group strictly containing $\mathrm{PSL}_2(\mathbb{F}_p)$, we argue as in the proof of Theorem 1.6 part 3. The map f has $p+1$ fixed points, as can be seen from the equation:

$$f(z)=\psi(z^p-z)+z=z.$$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

There are $(p+1)p(p-1)$ elements of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ for which $\mathrm{Fix}(f)$ is an invariant set, and we showed that at least one of these elements is not an automorphism of f. The argument about group orders in the proof of Theorem 1.6 part 3 then shows that $\mathrm{Aut}(f) = \mathrm{PSL}_2(\mathbb{F}_p)$. □

From the earlier discussion of maps of the form $\psi(z^p - z) + z$, we can easily determine the multiplier spectrum of the above map, which shows that varying c results in a one-dimensional family of maps realizing $\mathrm{PSL}_2(\mathbb{F}_p)$ in the moduli space.

2.1.4. p-irregular dihedral groups

We now prove that any p-irregular dihedral group D_{2n} is realizable. These groups occur only when $p = 2$ and $n \geq 3$ is odd.

Proof of Theorem 1.6 part 4. Let

$$f(z) = \frac{1}{z^{2n-1}}.$$

We claim that $\mathrm{Aut}(f) \cong D_{2n}$. By direct computation, the automorphism group of f includes $z \mapsto 1/z$ and $z \mapsto \zeta_n z$, and these transformations generate a dihedral group of order $2n$. We now show that there are no extra automorphisms by showing that $f(z)$ has at most $2n$ automorphisms. First, notice that

$$\mathrm{Fix}(f) = \{z \in \bar{\mathbb{F}}_2 : z^{2n} = 1\},$$

which has cardinality n. Second, we claim that the set of points with a unique preimage is $\{0, \infty\}$. It is clear that $f^{-1}(0) = \infty$ and $f^{-1}(\infty) = 0$. Now let $c \neq 0, \infty$. The affine preimages of c are the values of z such that $f(z) = c$, or equivalently

$$cz^{2n-1} = 1.$$

Since $c \neq 0$, this polynomial is of degree $2n - 1$ and is separable because $2n - 1$ is odd, so the roots are distinct. Each automorphism of f is determined by where it sends 0, 1, and ∞. There are at most two possible images for 0, and n possible images for 1, so there are at most $2n$ automorphisms of f. □

2.1.5. The icosahedral subgroup of $\mathrm{PGL}_2(\bar{\mathbb{F}}_3)$.

The final construction needed for Theorem 1.6 is the case of the icosahedral subgroup A_5 in $\mathrm{PGL}_2(\bar{\mathbb{F}}_3)$. This is a finite calculation that is part of the dynamical systems library in Sage [19].

Proof of Theorem 1.6 part (5). Let f be the dynamical system in the theorem statement. Using the algorithm in Sage to compute automorphism groups of dynamical systems, we computed that $\mathrm{Aut}(f) \cong A_5$ [19]. We also compute in Sage that the resultant of f is nonzero, so $\deg f = 21$. We prove the claim that f is of minimal degree for A_5 in Theorem 3.4. □

***2.2. Realizability of p-regular finite subgroups of* $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$**

In this section, we construct solutions to the realizability problem for every p-regular finite subgroup Γ of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. Each group that appears is trivial, cyclic, dihedral, tetrahedral, octahedral, or icosahedral, and each isomorphism type appears as a single conjugacy class; see the Appendix for the classification.

2.2.1. The trivial group

We now prove Theorem 1.7 part (1), which says that the trivial group 1 is realizable.

Proof of Theorem 1.7 part (1). Let $f(z) = z^2 + z$. By direct calculation, we have $\mathrm{Fix}(f) = \{0, \infty\}$. The multiplier at 0 is 1, and the multiplier at ∞ is 0. Thus any automorphism of f must fix 0 and ∞, so

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

the only possible automorphisms are of the form $z \mapsto \alpha z$, where $\alpha \neq 0$. Given such an automorphism, $f(\alpha z) = \alpha f(z)$ implies $\alpha^2 = \alpha$, so $\alpha = 1$. Thus, $\mathrm{Aut}(f) = 1$. □

Remark 2.5. *This is a special case of the argument used to realize p-semi-elementary groups in Theorem 1.6 part (2), taking the multiplicative group $\mu_n = 1$ and the additive group $\Lambda = 0$. In Section 4, we further show that a generic degree-2 map f has no nontrivial automorphisms.*

2.2.2. Cyclic groups

In this section, we prove Theorem 1.7 part (2), that every p-regular cyclic group C_n arises as the exact automorphism group of a self-map of $\mathbb{P}^1(\bar{\mathbb{F}}_p)$. The p-regularity condition means that n is coprime with p.

Silverman [14] shows that, in characteristic 0, a map f has $C_n \subseteq \mathrm{Aut}(f)$ if and only if f is of the form $f(z) = z\psi(z^n)$ for some rational function ψ. The argument is valid as long as primitive n-th roots of unity exist, which is true in characteristic p when $\gcd(p, n) = 1$.

Proof of Theorem 1.7 part 2. Let n be coprime with p, and let $f(z) = \frac{1}{z^{n-1}} + z$.

First, notice that the map $z \mapsto \zeta_n z$ is an order n automorphism. For the other containment, notice that ∞ is the unique fixed point of f. The unique non-fixed preimage of ∞ is 0. Any automorphism of f, therefore, must fix ∞ and 0 and so is of the form $\alpha(z) = az$ for some constant a. We compute $f^\alpha = \frac{1}{a^n z^{n-1}} + z$, so to get an automorphism, we must have that a is an n-th root of unity.

It remains to show that no map of smaller degree has C_n as its automorphism group. By Silverman [14], if a map f has an order n automorphism with n coprime to p, it must be of the form $z\psi(z^n)$ for some rational map ψ. If ψ is a constant map, then f has degree 1; otherwise, the minimal possible degree is $n-1$ when $\psi(z) = \frac{a}{z}$ with $a \neq 0$. In this case, $f(z) = \frac{a}{z^{n-1}}$ has the extra automorphism $z \mapsto \frac{1}{z}$. Thus, there are no maps of degree $n-1$ with C_n as their exact automorphism group, and n is the minimal degree. □

Remark 2.6. *Let p be a prime and let $n \geq 2$ be coprime to p. Then the map $f(z) = z^{n+1} + z$ also has* $\mathrm{Aut}(f) \cong C_n$. *This f(z) appears when applying the construction used to prove Theorem 1.6 part (2) to the multiplicative group μ_n of n-th roots of unity and the additive group $\Lambda = 0$. However, f(z) is not of minimal degree for C_n.*

2.2.3. Dihedral groups

In this section, we prove Theorem 1.7 part (3) that every p-regular dihedral group D_{2n} arises as the exact automorphism group of a self-map of $\mathbb{P}^1(\bar{\mathbb{F}}_p)$. The p-regularity condition here means that $p > 2$ and that n is coprime to p.

Silverman described maps with automorphism group containing a dihedral group D_{2n}; see [14] or [16, Exercise 4.37]. In characteristic 0, these are exactly the maps of the form:

$$f(z) = z \cdot \frac{F(z^n)}{z^{dn} F(z^{-n})},$$

where F is any polynomial and d is its degree. Using the form above, one can write down various families of maps with at least dihedral symmetry and then check against extra automorphisms. For instance, in characteristic 0, the realizability problem for D_{2n} can be solved by z^{n+1}, which corresponds to the choice $F(z) = z$. But in characteristic p, this f sometimes acquires extra automorphisms. The task for us is to find families of solutions that each work for most choices of p and n, so that taken together, all choices of p and n are accounted for.

Proof of Theorem 1.7 part (3). In each case to be addressed, the maps $\alpha(z) = 1/z$ and $\beta(z) = \zeta_n z$ are automorphisms of f that generate a dihedral group D_{2n}. To prove exactness, we argue that in each case, f has at most $2n$ automorphisms.

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

(1) We assume $n \not\equiv -1 \pmod{p}$ and $f(z) = z^{n+1}$. A simple calculation shows that α and β are automorphisms, so that $D_{2n} \subseteq \mathrm{Aut}(f)$. Any automorphism must permute sets of fixed points of the same multiplier. Examining the equation $f(z) = z$, we calculate that the fixed points are 0 and ∞, and all the n-th roots of unity. Of these, the fixed points 0 and ∞ have multiplier 0, and the n-th roots of unity have multiplier $n + 1$, which is nonzero by the hypothesis on n. We conclude that every automorphism permutes $\{0, \infty\}$ and permutes $\{\zeta_n{}^k : k = 0, 1, ..., n-1\}$.

An automorphism can be completely described by specifying the images of three points. So we may bound the number of automorphisms by considering the possible images of 0, ∞, and 1. There are at most n choices for where to send 1. There are at most two choices for where to send 0, and that choice also determines the image of ∞. So there are at most $2n$ automorphisms of f.

(2) We assume $n \not\equiv 1 \pmod{p}$, $n > 2$, and $f(z) = \frac{1}{z^{n-1}}$. A simple calculation checks that α and β are automorphisms, so $D_{2n} \subseteq \mathrm{Aut}(f)$. We again prove that $\{\zeta_n{}^k : k = 0, ..., n-1\}$ and $\{0, \infty\}$ are invariant sets for every automorphism; then the argument in the first case proves the bound. The first set is Fix(f), so it is invariant. To prove invariance of $\{0, \infty\}$, we show that it is the set of all points with a unique preimage. A direct check shows that this set contains 0 and ∞, so we need only check that no other points are in the set. Suppose $c \notin \{0, \infty\}$. Then the preimages of c are the roots of $z^{n-1} - \frac{1}{c}$.

Since $n \not\equiv 1 \mod p$ by hypothesis, this polynomial is separable, so it has distinct roots. Then, using the hypothesis $n > 2$, distinct roots implies at least two roots, so c does not have a unique preimage. Since D_{2n} has an element of order n, by Proposition 2.1, the lowest-degree map that could realize it is $n - 1$, which is what we have.

(3) We assume $n = 2$ and $f(z) = z \cdot \frac{z^2+a}{az^2+1}$ where a is not in the exceptional set $\{-3, -1, 0, 1\}$. First, we observe that f has automorphisms $\alpha(z) = 1/z$ and $\beta(z) = -z$, which generate a dihedral group $D_4 \cong C_2 \times C_2$ since $p > 2$. The conditions on a ensure that f has degree 3. Then, we just need to show that f has at most four automorphisms. We can do this by finding two invariant sets of cardinality 2. We calculate the fixed points of f and sort them by multiplier. The fixed points are 0, ∞, 1, and -1. The first two of these have multiplier a and the last two have multiplier $(3 - a)/(a + 1)$. The conditions on a guarantee that these two multipliers are distinct. Finally, this map f(z) is of minimal degree for D_4, since by Theorem 1.8, there are no degree 2 maps with automorphism group D_4.

These cases account for all valid choices of p and n. □

2.2.4. *Platonic solid groups*

The problem of finding maps with platonic solid symmetry in characteristic 0 has been studied in detail by Klein [11], Doyle and McMullen [6], and de Faria and Hutz [4]. Using their examples, we experimentally found that various self-maps of $\mathbb{P}^1(\bar{\mathbb{Q}})$ with platonic solid symmetries could usually be reduced modulo p to produce maps of $\mathbb{P}^1(\bar{\mathbb{F}}_p)$ without picking up extra automorphisms. We turn this observation into a proof of the remainder of Theorem 1.7 by carrying out the following strategy.

(1) Exhibit a faithful representation of Γ in $\mathrm{PGL}_2(\bar{\mathbb{Q}})$ where each entry of each matrix in Γ is an algebraic integer. Then by reducing the entries of each matrix modulo p, we get entries in $\bar{\mathbb{F}}_p$, and, in fact, we get a new representation of Γ in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. We denote the image of Γ by Γ_p. We seek representations of Γ such that the resulting representation in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is faithful for almost all p.

(2) Choose a map f over $\bar{\mathbb{Q}}$ that has exact automorphism group Γ and reduce it modulo p to obtain a map f_p. The automorphism group of f_p certainly contains Γ_p but may have picked up additional elements as well.

(3) Show that for most primes, the reduced map f_p has degree at least two and no automorphisms besides those in Γ_p.

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

(4) For any primes that have not been accounted for yet, make another choice of f and repeat the process.

As it turns out, most choices of f seem to work for most primes p, so this strategy does not take long to terminate. The third step above is the most interesting, and our methods differ somewhat for the three platonic solid groups.

Proof of Theorem 1.7 part (5). The octahedral group S_4 has $24 = 2^3 \cdot 3$ elements, and we study only p-regular groups in this section, so this case only concerns primes $p > 3$.

The octahedral group has a representation over $\bar{\mathbb{Q}}$ given by:

$$\Gamma = \left\langle S = \begin{bmatrix} i & i \\ 1 & -1 \end{bmatrix}, T = \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix}, U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\rangle,$$

where i is a primitive fourth root of unity. Now we check whether reduction is injective. When $p > 2$, the image of i is still a primitive fourth root of unity. The subgroup Γ' generated by S, T^2, and U is tetrahedral. Reduction is injective on Γ' since the elements $U, T^2, UT^2, U^2, S^2, S^3, US$ remain distinct, which means the image has cardinality at least 7. Then, the first isomorphism theorem of group theory shows that the homomorphism is injective. And reduction does not map T into the image of Γ', so the image of Γ has at least 13 elements, so reduction is injective on Γ.

The paper by de Faria and Hutz [4] gives examples of maps with exact automorphism group Γ. We first try reducing

$$f(z) = \frac{-z^5 + 5z}{5z^4 - 1}.$$

The resultant is $-2^{12} \cdot 3^4$, so the reduced map f_p has degree 5 for all $p > 3$.

This gives us maps for every $p > 3$ with automorphism group containing Γ_p, but we need to check for extra automorphisms. Suppose f has an extra automorphism. By the classification of subgroups (see the Appendix), all the finite subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ strictly containing S_4 are p-irregular, so any extra automorphism implies the existence of an automorphism of order p. Then by equation (2.3), we know $\deg f \equiv 0, 1 \pmod{p}$, so $p \leq \deg f + 1 = 6$. So we have exactly Γ_p except possibly when $p = 5$. In that case, we need to try another f since $f_5(z) = z^5$ has automorphism group $\mathrm{PGL}_2(\mathbb{F}_5) \neq \Gamma_5$.

To account for the case $p = 5$, we try another choice:

$$f(z) = \frac{-7z^4 - 1}{z^7 + 7z^3}.$$

We compute the resultant $-2^{16} \cdot 3^4$ and find that 5 is not a factor, so the reduced map is degree 7. And the prime 5 passes the test of equation (2.2), and, since we are working with a single prime, we compute directly in Sage [19] that the automorphism group is S_4. □

Proof of Theorem 1.7 part (6). The icosahedral group A_5 has $60 = 2^2 \cdot 3 \cdot 5$ elements, so this case only concerns primes $p \geq 7$. We need a choice of representation Γ of A_5 in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. We first consider the representation over $\bar{\mathbb{Q}}$ that was used by Klein [11]; denoting a chosen primitive fifth root of unity by ζ, the matrix generators are

$$S = \begin{bmatrix} \zeta^3 & 0 \\ 0 & \zeta^2 \end{bmatrix}, \quad T = \begin{bmatrix} \zeta - \zeta^4 & -\zeta^2 + \zeta^3 \\ -\zeta^2 + \zeta^3 & \zeta - \zeta^4 \end{bmatrix}.$$

Next, we verify that the reduction mod p homomorphism is injective. Since A_5 is simple, the possibilities for the kernel are the trivial group and all of A_5, and the kernel does not contain S as long as $p \neq 5$, so the kernel in our case is trivial.

The Appendix shows that, if a map has automorphism group strictly larger than A_5, then its automorphism group is p-irregular, so the same method as the previous section applies.

Doyle and McMullen provide examples of maps with exact automorphism group A_5 over $\bar{\mathbb{Q}}$ [6]. We try

$$f(z) = \frac{z^{11} + 66z^6 - 11z}{-11z^{10} - 66z^5 + 1}.$$

The resultant is divisible only by 2, 3, and 5, so the reduced map is degree 11 for all $p > 5$. Equation (2.2) shows that the only primes for which we may pick up extra automorphisms are $p = 2, 3, 5, 11$. In fact, when $p = 11$, our example reduces to z^{11}, which has exact automorphism group $\mathrm{PGL}_2(\mathbb{F}_{11})$.

So for the case $p = 11$, we try a different map. We check

$$f(z) = \frac{-57z^{15} + 247z^{10} + 171z^5 + 1}{-z^{19} + 171z^{14} - 247z^9 - 57z^4}.$$

We confirm that 11 does not divide the resultant, so the map is degree 15 after reduction; then (2.2) shows that f_{11} has p-regular automorphism group, and we compute $\mathrm{Aut}(f_{11}) \cong A_5$. □

Remark 2.7. *When $p = 3$, there is a subgroup of $\mathrm{PGL}_2(\bar{\mathbb{F}}_3)$ isomorphic to A_5, but it is p-irregular. In Section 2.1.5, we checked that A_5 is realizable when $p = 3$ directly, rather than by reducing a map over $\bar{\mathbb{Q}}$ modulo 3.*

The tetrahedral group A_4 is a bit more difficult to analyze than the previous cases because the representations of A_4 in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ are subrepresentations of S_4, which is also p-regular. There is also an additional curiosity in that the maps that invariant theory furnishes over $\bar{\mathbb{Q}}$ are not defined over $\mathbb{Q}$, for the particular representation we work with. This does not affect our calculation, but it is interesting.

Proof of Theorem 1.7 part (4). Since $|A_4| = 12$, we work with $p \geq 5$. Let Γ be the $\bar{\mathbb{Q}}$-representation of A_4 with matrix generators:

$$\left\{ \begin{bmatrix} i & i \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\},$$

where i is a primitive fourth root of unity. In the proof of Theorem 1.7 part (5), we showed that the reduction map is injective for this representation.

De Faria and Hutz [4] provides examples of maps over $\bar{\mathbb{Q}}$ with exact automorphism group Γ. We first try

$$f(z) = \frac{\sqrt{-3}z^2 - 1}{z^3 + \sqrt{-3}z}.$$

The resultant has just 2 as a prime factor, so for $p > 2$ the degree is still 3 after reduction.

Next, we check against extra automorphisms. The argument of Faber [7, Proposition 4.14, 4.17] shows that each tetrahedral subgroup Γ of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is uniquely contained in an octahedral group. The cited argument starts with a particular choice of Γ and calculates the copy of S_4; since the argument uses a different choice of Γ than we do, we are using the fact that every tetrahedral subgroup is conjugate in $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$.

In our case, the octahedral group is, as described previously, generated by Γ together with

$$\begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix}.$$

We check directly that this matrix is not an automorphism of f, even after reduction, by starting from the equation $f(iz) = if(z)$ and simplifying. The calculation is omitted.

Because the automorphism group of f is not isomorphic to S_4, if there were remaining automorphisms, then the automorphism group would be p-irregular. The test of equation (2.2) shows that f_p has p-regular automorphism group except possibly when $p = 2, 3$, and these primes are not present in this case.

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

To prove that f is of minimal degree, we need only rule out the possibility that a degree 2 map has automorphism group A_4. This follows from (2.2), since A_4 contains an element of order 4. □

3. Theoretical tools for discovering examples

In Theorems 1.7 and 1.6, we showed through explicit constructions that, for any prime power q, every subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$ arises as the automorphism group of a dynamical system. For instance, we calculated that $\mathrm{PSL}_2(\mathbb{F}_q)$ is the automorphism group of a certain dynamical system of degree at most $\frac{1}{2}(q^3 - 2q^2 + q + 2)$. In this section, we develop the theoretical tools that explain how we arrived at these constructions. We present the motivating theorems, then develop the proofs in stages.

Our work is modeled on the theory over $\mathbb{C}$. In work on the quintic, Doyle and McMullen [6] proved a version of the following structure theorem for rational maps of $\mathbb{P}^1(\mathbb{C})$ with automorphisms. The theorem statement requires definitions from invariant theory, which we defer to Section 3.1.

Theorem 3.1 (Doyle and McMullen [6, Theorem 5.2]). *Suppose that Γ is a subgroup of $\mathrm{PGL}_2(\mathbb{C})$. Let $\hat{\Gamma}$ be the preimage of Γ in $\mathrm{SL}_2(\mathbb{C})$. Then every rational map f such that $\deg(f) \geq 2$ and $\Gamma \subseteq \mathrm{Aut}(f)$ arises in the form:*

$$[x:y] \mapsto \left[xF + \frac{\partial G}{\partial y} : yF - \frac{\partial G}{\partial x}\right],$$

where F and G are homogeneous, relatively invariant polynomials for the same character of $\hat{\Gamma}$, such that $F = 0$ or $\deg(F) + 1 = \deg(G) - 1 = \deg(f)$.

The proof idea is that there are ways of going back and forth (not quite bijectively) between the following sets:

- Rational maps of $\mathbb{P}^1(\mathbb{C})$ such that $\Gamma \subseteq \mathrm{Aut}(f)$;
- Homogeneous invariant polynomial differential 1-forms in x, y over $\mathbb{C}$;
- Pairs (F, G) of homogeneous invariant polynomials in $\mathbb{C}[x, y]$ such that $F = 0$ or $\deg(F) + 2 = \deg(G)$.

In characteristic p, both the proofs and the results require modification, mainly because not all polynomials have antiderivatives. We prove the following variation.

Theorem 3.2. *Let p be a prime, and let q be a power of p.*

(1) Suppose that $p > 2$ and Γ is a p-irregular subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$. Let $\hat{\Gamma}$ be the preimage of Γ in $\mathrm{SL}_2(\mathbb{F}_{q^2})$. Then every rational map f such that $\deg(f) \geq 2$ and $\Gamma \subseteq \mathrm{Aut}(f)$ arises in the form:

$$[x:y] \mapsto \left[xF + \frac{\partial G}{\partial y} : yF - \frac{\partial G}{\partial x}\right], \tag{3.1}$$

where F and G are homogeneous, relatively invariant polynomials over $\bar{\mathbb{F}}_p$ for the same character of $\hat{\Gamma}$, such that $\deg(F) + 1 = \deg(G) - 1 = \deg(f)$.

(2) Let $p \geq 2$. Let F and G be homogeneous, relatively invariant polynomials over $\bar{\mathbb{F}}_p$ for the same character of $\Gamma \subseteq \mathrm{SL}_2(\mathbb{F}_q)$. Let $\bar{\Gamma}$ be the image of Γ in $\mathrm{PSL}_2(\mathbb{F}_q)$. If the expressions $xF + \frac{\partial G}{\partial y}$ and $yF - \frac{\partial G}{\partial x}$ are nontrivial homogeneous polynomials of the same degree, then the corresponding rational map f of the form (3.1) has $\bar{\Gamma} \subseteq \mathrm{Aut}(f)$.

One of the difficulties in applying Theorem 3.2 to the realizability problem is that the resulting map f may only satisfy $\Gamma \subseteq \mathrm{Aut}(f)$, while we are looking for equality. In trying to realize $\mathrm{PSL}_2(\mathbb{F}_q)$, for

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

many choices of invariants, the machinery of Theorem 3.2 resulted in a map with automorphism group $\mathrm{PGL}_2(\mathbb{F}_q)$. We observed that the degree of the minimal example of exact $\mathrm{PSL}_2(\mathbb{F}_q)$ automorphism group was a cubic polynomial in q. We formulate this observation as Theorem 3.3, with the tools for the proof coming from Propositions 3.5 and 3.6.

Theorem 3.3. *Let $p > 2$ and let q be a power of p. The degree of a rational map with automorphism group $\mathrm{PSL}_2(\mathbb{F}_q)$ must be at least*

$$\frac{1}{2}\left(q^3 - 2q^2 + q + 2\right).$$

We omit the case $p = 2$ because then $\mathrm{PSL}_2(\mathbb{F}_q)$ and $\mathrm{PGL}_2(\mathbb{F}_q)$ coincide.

A second application of Theorem 3.2 is to the problem of realizing A_5 over $\bar{\mathbb{F}}_3$. Over $\mathbb{C}$, the minimal degree of a map with exact automorphism group A_5 is 11. The example over $\bar{\mathbb{F}}_3$ described in Theorem 1.6 part 5 has degree 21. This turns out to be the minimal degree for A_5 when $p = 3$.

Theorem 3.4. *A rational map over $\bar{\mathbb{F}}_3$ with automorphism group A_5 has degree at least 21.*

3.1. Preliminaries from invariant theory

Let k be a field. Let V be a two-dimensional vector space over k. Let H be a subgroup of $\mathrm{GL}_2(k)$. Let $P[V]$ be the algebra of polynomial functions on V, that is, the symmetric algebra of the dual space V^*. Then H acts on $P[V]$ by *pullback*:

$$H \times P[V] \to P[V],$$

$$(h, F) \mapsto F \circ h.$$

We write $h^*F = F \circ h$. The elements of $P[V]$ fixed by this action form a subring of $P[V]$, denoted $P[V]^H$, called the *ring of (polynomial) invariants*.

Let χ be a character of H, that is, a homomorphism $H \mapsto k^*$. The set

$$\{F \in P[V] : \forall h \in H, h^*F = \chi(h)F\}$$

forms a $P[V]$-submodule of $P[V]$ called the *module of relative (polynomial) invariants*, denoted $P[V]^H_\chi$.

We make the analogous definitions for formal differential forms, following Smith [18]. Let $\Lambda[V]$ be the exterior algebra on the dual space V^*. Let $E[V] = P[V] \otimes \Lambda[V]$. The algebra $E[V]$ is called the *polynomial tensor exterior algebra*. We think of its elements as formal differential forms defined only with polynomials.

We recall the basic properties of $E[V]$, for convenience choosing a basis v, w of V.

(1) The basis v, w of V induces a basis x, y of $P[V]$ and algebra generators dx, dy of $\Lambda[V]$. The exterior algebra $\Lambda[V]$ is spanned as a k-vector space by $1, dx, dy, dx \wedge dy$. The polynomial algebra $P[V]$ is infinite-dimensional as a k-vector space and is spanned by monomials in x, y.

(2) There is a k-linear map $d\colon E[V] \to E[V]$ called the *exterior derivative*. It is defined as follows. We set

$$d(dx) = d(dy) = 0,$$

$$d(x) = dx,$$

$$d(y) = dy.$$

Then, we extend d to all of $E[V]$ by linearity and the Leibniz rule:

$$d(\theta_1\theta_2) = (d\theta_1)\theta_2 + \theta_1(d\theta_2).$$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

In particular, for any $f \in P[V]$, we have

$$df = \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy.$$

Forms in the kernel of d are *closed*, and forms in the image of d are *exact*. For any $\omega \in E[V]$, we have $d(d\omega) = 0$, so exact forms are closed.

(3) A group H of linear self-maps of V induces a pullback action on $E[V]$, as we now explain. Elements of $E[V]$ are sections of the bundle of differential forms on V, where V is viewed as a variety. Let TV be the tangent bundle on V. Let D denote the standard Jacobian matrix derivative. Then any algebraic map $h{:}V \to V$ induces a pushforward map $h_* : TV \to TV$. It is defined as follows: given a tangent vector δ to a point $v \in V$, the pushforward $h_*\delta$ is the tangent vector $(Dh)(\delta)$ to $h(v)$. Since V is a vector space, we may canonically identify the tangent spaces $(TV)_v$ and $(TV)_{h(v)}$ with V. In our setting, the self-map h is linear rather than just algebraic, so it is equal to its own Jacobian with this identification. Thus,

$$h_*\delta = h(\delta).$$

The pullback of a form $\theta \in E[V]$ by an algebraic map $h\colon\ V \to V$ is defined by:

$$h^*\theta = \theta \circ h_*.$$

Thus, any group H of linear self-maps of V induces an action on $E[V]$. It follows from the definition that h^* respects the algebra structure of $E[V]$ and that h^* commutes with the exterior derivative d.

A form $\omega \in E[V]$ is called *relatively invariant* for H (with respect to a character χ) if for all $h \in H$, we have

$$h^*\omega = \chi(h)\omega.$$

If χ is the trivial character, then ω is also called an *absolute* invariant.

The set of relatively invariant forms for H with character χ form the *module of relatively invariant (formal differential) forms*, denoted $E[V]^H_\chi$.

There are a number of natural gradings to consider on $E[V]$. Our convention for the grading is as follows. After choosing generators x, y for $P[V]$ and the corresponding basis dx, dy for the 1-forms in the exterior algebra, we assert that x and y have degree 1 and that dx and dy have degree 0; then we extend multiplicatively. In particular, a homogeneous 1-form is one where dx and dy have coefficients which are homogeneous polynomials of the same degree. (Our convention is that 0 is of every degree.)

3.2. From rational maps to 1-forms and back

We follow [6, Section 5.III]. Viewing V as a variety, each tangent space of V is canonically isomorphic to V. Thus, given any polynomial map:

$$\Phi{:}\mathbb{A}^2 \to \mathbb{A}^2,$$
$$\Phi(x, y) = (\Phi_1(x, y), \Phi_2(x, y)),$$

we can associate a vector field X_Φ on V; it sends (x,y) to the point in $(TV)_{(x,y)}$ corresponding to $\Phi(x, y)$. For any linear map $h\colon\ V \to V$, we may consider the pushforward h_*X_Φ and the conjugate map Φ^h. It follows immediately from the definition of X_Φ that in fact,

$$h_*X_\Phi = X_{\Phi^h}.$$

Throughout, let $\omega = dx \wedge dy$. Let ω_Φ be the 1-form defined by contraction of ω by the vector field X_Φ; that is,

$$\omega_\Phi(\,\cdot\,) = \omega(X_\Phi, \cdot).$$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

In coordinates,

$$\omega_\Phi = \Phi_2 dx - \Phi_1 dy.$$

It follows from the definition of ω_Φ, or its expression in coordinates, that for any invertible linear map $h\colon V \to V$, we have

$$h^*\omega_\Phi = \omega_{\Phi^h}.$$

In particular, we have $\Phi = \Phi^h$ if and only if $h^*\omega_\Phi = \omega_\Phi$.

We can use this connection to translate data about the automorphism group of f into invariant theory, as follows.

Let $\Gamma \subseteq \mathrm{PGL}_2(k)$. Let $\hat\Gamma$ be a subgroup of $\mathrm{GL}_2(k)$ that is mapped to $\mathrm{PGL}_2(k)$ by projectivization. Let f be a rational map. If $\gamma \in \Gamma$ is an automorphism of f, then $f^\gamma = f$. Let Φ be any lift of f to a polynomial function on $\mathbb{A}^2$. Specifically, Φ is a pair of homogeneous polynomials that define the same endomorphism of $\mathbb{P}^1$ as f. Let M be any preimage of γ in $\hat\Gamma$. Since $f = f^\gamma$, there exists some value $\chi(M) \in k^*$ such that $\Phi^M = \chi(M)\Phi$. In fact, $\chi(M)$ is independent of the choice of lift Φ. The rule $M \mapsto \chi(M)$ defines a character $\chi\colon\hat\Gamma \to k^*$. We have

$$M^*\omega_\Phi = \omega_{\Phi^M} = \omega_{\chi(M)\Phi} = \chi(M)\omega_\Phi.$$

So, if f has automorphism group containing Γ, then for any lift Φ of f, the 1-form ω_Φ is a relative invariant of $\hat\Gamma$ with respect to some character.

Conversely, to a nonzero homogeneous 1-form $\omega = f_1 dx + f_2 dy$, we can associate the rational map $r(\omega) := [-f_2 : f_1]$. If ω is relatively invariant for a subgroup H of GL_2, then the elements of the image $\bar H$ of H in PGL_2 are automorphisms of $r(\omega)$. We have established the following proposition.

Proposition 3.5. *Let $\Gamma \subseteq \mathrm{PGL}_2(k)$ and let $\hat\Gamma$ be a subgroup of $\mathrm{GL}_2(k)$ that maps to Γ by projectivization. Let f be a rational map of $\mathbb{P}^1$.*

(1) If f has automorphism group containing Γ, then for any lift Φ of f, the 1-form ω_Φ is a relative invariant of $\hat\Gamma$ with respect to some character.

(2) If ω_Φ is a relative invariant of a group H, then $\bar H \subseteq \mathrm{Aut}(f)$.

Some remarks are as follows:

(1) These associations, from rational maps to nonzero homogeneous 1-forms and back, are almost inverse, but not quite. There is no well-defined association $f \mapsto \omega_\Phi$, except up to scaling. Even so, we can say $r(\omega_\Phi) = f$.

(2) We have $\deg(\omega_\Phi) = \deg(f)$. But because of the possibility of a common factor, the most we can say about $r(\omega)$ is that $\deg(r(\omega)) \le \deg(\omega)$. Equality occurs if and only if ω has no nonzero homogeneous polynomial of positive degree as a factor.

3.3. From 1-forms to polynomials and back

The next proposition links invariant 1-forms to pairs of invariant polynomials. We defer the proof to the end of this subsection.

Proposition 3.6. *Let $\lambda = ydx - xdy$.*

(1) Let k be a field of characteristic p. Let η be a homogeneous 1-form of degree n, where

$$n \not\equiv -1 \pmod{p}. \tag{3.2}$$

Then there exist homogeneous polynomials F and G, possibly 0, such that

$$\eta = F\lambda + dG,$$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

where dG is the 1-form $dG = \frac{\partial G}{\partial x}dx + \frac{\partial G}{\partial y}dy$. Writing $\eta = \eta_1 dx + \eta_2 dy$, explicit formulas for F and G are

$$F = \frac{1}{n+1}\left(\frac{\partial \eta_1}{\partial y} + \frac{\partial \eta_2}{\partial x}\right),$$
$$G = \frac{1}{n+1}(x\eta_1 + y\eta_2).$$

(2) *Suppose H is a subgroup of $\mathrm{SL}_2(k)$. If η is a relative invariant for H with character χ, then the above F and G may further be chosen to be relative invariants of H for character χ.*

(3) *Suppose H is a subgroup of $\mathrm{SL}_2(k)$. If F and G are homogeneous invariant polynomials of H with character χ such that $F\lambda + dG$ is homogeneous, then $F\lambda + dG$ is also a relative invariant for χ.*

Remark 3.7. *To show that the degree hypothesis (3.2) is needed, consider the example $\eta = y^{p-1}dx$. If we assume $\eta = F\lambda + dG$ for some F, G, then we get the equations:*

$$y^{p-1} = yF + \frac{\partial G}{\partial x},$$
$$0 = -xF + \frac{\partial G}{\partial y}.$$

An appropriate linear combination of the above equations gives

$$xy^{p-1} = x\frac{\partial G}{\partial x} + y\frac{\partial G}{\partial y} = (\deg G)G = 0,$$

which is false.

The restriction on degree makes this proposition more subtle than its characteristic 0 counterpart. But in our application (Theorem 3.2), the degree hypothesis is automatically satisfied in the p-irregular case. Thus, Proposition 3.6 is a rare example of modular invariant theory being less complicated than nonmodular invariant theory.

Remark 3.8. *There are creative ways of evading the degree hypothesis (3.2). For instance, say $p > 2$ and η is a relative invariant for H with character χ with degree n, where*

$$n \equiv -1 \pmod{p}.$$

There is an absolutely invariant homogeneous polynomial of $\mathrm{GL}_2(\mathbb{F}_q)$ of degree $q^2 - 1$, which we denote u (see, for instance, Smith [18, Chapter 8]). Then $u\eta$ is a relative invariant for H with character χ with degree $-2 \mod p$. Thus, η can be written in the form $(F\lambda + dG)/u$, where F and G are in degrees $n + q^2 - 2$ and $n + q^2$, respectively. Thus, the structure of the module of relative invariants still affects the existence of rational maps in these degrees.

Before we embark on the proof, we first need a version of the Poincaré Lemma of exterior algebra that is appropriate for fields of characteristic p.

Lemma 3.9. *Say η is a homogeneous, closed 1-form on a two-dimensional vector space over a field of characteristic p. Suppose also that η has degree n such that*

$$n \not\equiv -1 \pmod{p}.$$

Then η is exact.

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

Proof. Express η in a basis as $\eta_1 dx + \eta_2 dy$. Since η is closed, we may obtain from the equation $d\eta = 0$ that

$$\frac{\partial \eta_1}{\partial y} = \frac{\partial \eta_2}{\partial x}.$$

Then we compute explicitly

$$\begin{aligned} d(x\eta_1 + y\eta_2) &= \eta_1 dx + x d\eta_1 + \eta_2 dy + y d\eta_2 \\ &= \eta + x d\eta_1 + y d\eta_2 \\ &= \eta + x\frac{\partial \eta_1}{\partial x}dx + x\frac{\partial \eta_1}{\partial y}dy + y\frac{\partial \eta_2}{\partial x}dx + y\frac{\partial \eta_2}{\partial y}dy \\ &= \eta + x\frac{\partial \eta_1}{\partial x}dx + y\frac{\partial \eta_1}{\partial y}dx + x\frac{\partial \eta_2}{\partial x}dy + y\frac{\partial \eta_2}{\partial y}dy && \text{(using closedness)} \\ &= \eta + n\eta = (n+1)\eta. && \text{(using homogeneity).} \end{aligned}$$

By assumption, we may divide by $n + 1$, so we have the explicit formula:

$$\eta = d\left(\frac{1}{n+1}(x\eta_1 + y\eta_2)\right). \tag{3.3}$$

□

We are ready to prove Proposition 3.6.

Proof of Proposition 3.6. Throughout, set $\omega = dx \wedge dy$. Notice that ω is absolutely invariant with respect to $\mathrm{SL}_2(k)$.

(1) One may just check that the given formulas for F and G suffice. We now explain how to derive the formulas. First, we show that there is a homogeneous polynomial F of degree $n-1$ such that $d\eta = d(F\lambda)$. We have

$$d\eta = \left(-\frac{\partial \eta_1}{\partial y} + \frac{\partial \eta_2}{\partial x}\right)\omega.$$

For convenience, let

$$j = \left(-\frac{\partial \eta_1}{\partial y} + \frac{\partial \eta_2}{\partial x}\right).$$

Thus,

$$d\eta = j\omega.$$

For any homogeneous polynomial F, we have by the Leibniz rule that

$$\begin{aligned} d(F\lambda) &= (dF)\lambda + F(d\lambda) \\ &= \left(\frac{\partial F}{\partial x}dx + \frac{\partial F}{\partial y}dy\right)(-ydx + xdy) + F\omega \\ &= \left(\frac{\partial F}{\partial x}x + \frac{\partial F}{\partial y}y\right)\omega + 2F\omega \\ &= (2 + \deg F)F\omega. \end{aligned}$$

Thus, the desired F must satisfy

$$F = \frac{j}{2 + \deg F},$$

so we see that F must be of degree $n-1$ and we take

$$F = \frac{j}{n+1}.$$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

With this choice of F, we know that the 1-form $\eta - F\lambda$ is closed, hence exact by Lemma 3.9. Thus, there exists a 0-form G such that $dG = \eta - F\lambda$. Applying (3.3), we obtain the stated formula for G.

(2) Let $h \in H$. Let j be as in the proof of (1). We compute the pullback $h^*(d\eta)$ two ways. On the one hand,

$$\begin{aligned} h^*(d\eta) &= h^*(j\omega) \\ &= (h^*j)(h^*\omega) && (h^* \text{ respects multiplication}) \\ &= (h^*j)\omega. && (\omega \text{ is absolutely invariant}). \end{aligned}$$

On the other hand,

$$\begin{aligned} h^*(d\eta) &= d(h^*\eta) && (d \text{ and } h^* \text{ commute}) \\ &= d(\chi(h)\eta) && (\eta \text{ is relatively invariant}) \\ &= \chi(h)d\eta \\ &= \chi(h)j\omega. \end{aligned}$$

Thus, $h^*j = \chi(h)j$, so j is relatively invariant. Since $F = j/(n+1)$, we conclude that F is relatively invariant.

Now we show that G is relatively invariant, that is, that $\chi(\gamma)G = \gamma^*G$. Since η and F are relatively invariant, and λ is absolutely invariant, we have

$$\begin{aligned} h^*(dG) &= h^*(\eta - F\lambda) \\ &= h^*\eta - (h^*F)(h^*\lambda) \\ &= \chi(h)\eta - \chi(h)F\lambda \\ &= \chi(h)(dG). \end{aligned}$$

So dG is relatively invariant. This implies that $\chi(h)G - h^*G$ is a homogeneous closed 0-form of degree $n+1$. The only nonzero closed 0-forms are elements of the polynomial ring $k[x^p, y^p]$. By the assumption that $n \not\equiv -1 \mod p$, we may conclude that $\chi(h)G - h^*G = 0$, so G is relatively invariant.

(3) Let $h \in H$. We compute

$$\begin{aligned} h^*(F\lambda + dG) &= (h^*F)(h^*\lambda) + h^*(dG) \\ &= \chi(h)Fh^*\lambda + h^*(dG) \\ &= \chi(h)F\lambda + h^*(dG) \\ &= \chi(h)F\lambda + d(h^*G) \\ &= \chi(h)F\lambda + d(\chi(h)G) \\ &= \chi(h)(F\lambda + dG). \end{aligned}$$

□

3.4. Proofs

We conclude this section by proving Theorems 3.2, 3.3, and 3.4.

Proof of Theorem 3.2

(1) Let f be a map as described in the theorem statement. Choose any lift Φ of f. Then $\deg(\omega_\Phi) = \deg(f)$. By equation (2.2), we know $\deg(\omega_\Phi) \equiv -1, 0, 1 \mod p$. Since $p > 2$ by assumption, the form ω_Φ meets the degree hypothesis of Proposition 3.6 (1). Since ω_Φ is the form associated with a rational map via 3.5, it is relatively invariant for $\hat{\Gamma}$ with respect to some character, so the invariance hypothesis of Proposition 3.6 (2) is also met. To meet the hypothesis that $\hat{\Gamma}$ is

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

a subgroup of $\mathrm{SL}_2(k)$, we take k to be $\mathbb{F}_{q^2}$ and view Γ as a subgroup of $\mathrm{PSL}_2(\mathbb{F}_{q^2})$. Thus, we can write $\omega_\Phi = F\lambda + dG$ for relative invariant homogeneous polynomials F and G for the same character. Then, again by Proposition 3.5, we have

$$f = r(\omega_\Phi) = r(F\lambda + dG).$$

The theorem statement is just this equation written in coordinates.

(2) Let $\omega = F\lambda + dG$. The conditions on F and G ensure that ω is homogeneous and nonzero. By Proposition 3.6 (3), ω is relatively invariant for Γ. Then $r(\omega)$ has the claimed automorphisms, by the discussion immediately preceding Proposition 3.5. □

Proof of Theorem 3.3. Assume that f has automorphism group $\mathrm{PSL}_2(\mathbb{F}_q)$. Write $d = \deg(f)$. Let ω be a 1-form associated with f via Proposition 3.5. By the proof of Proposition 3.6, there exist relatively invariant homogeneous polynomials F and G of $\mathrm{SL}_2(\mathbb{F}_q)$ such that $\omega = F\lambda + dG$. We also know $\deg F + 1 = \deg G - 1 = d$ (or $F = 0$). Surely $G \neq 0$ because otherwise there would be a homogeneous factor, causing f to be degree 1, which we reject.

For $q > 2$, the only character of $\mathrm{SL}_2(\mathbb{F}_q)$ is the trivial character. To see this, we invoke a well-known fact from group theory (see Dickson [5]): the abelianization of $\mathrm{SL}_2(\mathbb{F}_q)$ is trivial as long as $q \geq 4$. Every character factors through the abelianization, so every character is trivial. For $q = 3$, the group $\mathrm{PSL}_2(\mathbb{F}_3)$ is isomorphic to the alternating group A_4. There are only two 3-regular conjugacy classes in A_4, so there are two modular characters. These are the trivial character and a degree 3 character (the reduction of the ordinary degree 3 character). Since we are only interested in linear characters for invariants, we need only consider the trivial character in the $q = 3$ case.

Now we ask for which values of d there exist homogeneous invariant polynomials in degrees $d - 1$ and $d + 1$. We cite a standard theorem in modular invariant theory, see Smith [18, Theorem 8.1.8]: the ring of invariants $\mathbb{F}_q[x, y]^{\mathrm{SL}_2(\mathbb{F}_q)}$ is generated as an $\mathbb{F}_q$-algebra by the fundamental invariants:

$$u_1 = x^q y - xy^q$$

and

$$u_2 = \sum_{n=0}^{q} x^{(q-1)(q-n)} y^{(q-1)n} = \frac{x^{q^2} y - xy^{q^2}}{x^q y - xy^q}.$$

The set of degrees of nontrivial polynomial invariants is, thus, the numerical semigroup generated by $q + 1$ and $q(q - 1)$. It is also known that u_1 and u_2 are algebraically independent; that is, the ring of invariants above is actually a polynomial ring. So we can write F and G as polynomials in u_1 and u_2, in a unique way.

Next, we show that certain simple families of F and G give rise to 1-forms which are relatively invariant for a character of $\mathrm{GL}_2(\mathbb{F}_q)$. By Proposition 3.5, such 1-forms give rise to rational maps with automorphism group $\mathrm{PGL}_2(\mathbb{F}_q)$. Therefore, the only way to get a map with exact automorphism group $\mathrm{PSL}_2(\mathbb{F}_q)$ is to avoid these families.

The determinant, denoted by det, is a character of $\mathrm{GL}_2(\mathbb{F}_q)$. The polynomial u_1 and the 1-form λ are, by direct calculation, relative invariants for det. The polynomial u_2 is an absolute invariant of $\mathrm{GL}_2(\mathbb{F}_q)$. This causes many simple expressions of the form $F\lambda + dG$ to be relative invariants for some power of det.

Each pair of F and G falls into at least one of the following cases:

(1) $F = 0$.
(2) $F \neq 0$ and F and G are monomials in u_1 and u_2.
(3) At least one of F and G is not a monomial in u_1 and u_2.

Now we see which elements of these cases are admissible, in the sense that $F\lambda + dG$ is not a relative invariant for any power of det.

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

(1) Say $F=0$. If G is a pure polynomial in u_1, it is of the form $c{u_1}^k$, so it is a relative invariant of $\mathrm{GL}_2(\mathbb{F}_q)$ for $\det^k$. If G is a pure polynomial in u_2, it is an absolute invariant of $\mathrm{GL}_2(\mathbb{F}_q)$. So G must contain a binomial, which reduces us to the last case.

(2) Write $F=\alpha {u_1}^{a_1}{u_2}^{a_2}, G=\beta {u_1}^{b_1}{u_2}^{b_2}$, where $\alpha, \beta \in \mathbb{F}_q^*$. Then, $F\lambda$ is relatively invariant for $\det^{a_1+1}$ and G is relatively invariant for $\det^{b_1}$. The sum of relative invariants for the same character is again a relative invariant, so $\det^{a_1+1} \neq \det^{b_2}$. Since $\det^{q-1}$ is trivial by cyclicity of k^*, we conclude

$$a_1+1 \not\equiv b_1 \mod (q-1).$$

This property is preserved by multiplying or factoring out a monomial simultaneously from F and G. Thus, we reduce to one of the following cases: $F={u_1}^{a_1}$ and $G={u_2}^{b_2}$, or $F={u_2}^{a_2}$ and $G={u_1}^{b_1}$.

In the first case, a_1 and b_2 are positive solutions to

$$a_1(q+1)+2=b_2(q^2-q).$$

Finding minimal solutions for such equations is a basic Diophantine problem. Reducing modulo $q(q-1)/2$, we find $a_1 \equiv q-2$. We earlier found that $a_2+1 \not\equiv b_1 \mod (q-1)$, and $b_1=0$, so we cannot have $a_1=q-2$. Looking at the next positive solution for a_1 gives

$$a_1 \geq \frac{1}{2}q(q-1)+q-2.$$

Then the degree of f in this case is at least $\left(\frac{1}{2}q(q-1)+q-2\right)(q+1)+1$.

In the second case, a_2 and b_1 are positive solutions to

$$a_2(q^2-q)+2=b_1(q+1).$$

The minimal solution occurs when

$$b_1 \geq \frac{1}{2}(q^2-q)-q+2.$$

Then

$$\deg(f) \geq \frac{1}{2}(q^3-2q^2+q+2).$$

(3) The lowest degree homogeneous polynomial in u_1 and u_2 that is not a monomial occurs in degree:

$$\operatorname{lcm}(\deg(u_1), \deg(u_2)) = \frac{1}{2}q(q-1)(q+1).$$

Thus, if F or G contains a binomial, $\deg(f) \geq \frac{1}{2}q(q-1)(q+1)-1$.

Recalling that $q \geq 3$, the bound

$$\deg(f) \geq \frac{1}{2}(q^3-2q^2+q+2)$$

holds across all the cases. □

Proof of Theorem 3.4. Assume that f has automorphism group $A_5 \subseteq \mathrm{PGL}_2(\bar{\mathbb{F}}_3)$. We claim that $\deg f \geq 21$. Let ζ be a primitive fifth root of unity in $\bar{\mathbb{F}}_3$. By a conjugacy, we may assume that the subgroup A_5 is generated by the matrices:

$$\begin{bmatrix} \zeta & 0 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 1-\zeta-\zeta^{-1} \\ 1 & -1 \end{bmatrix}.$$

Let $\hat{A}_5$ be the inverse image of A_5 in $\mathrm{SL}_2(\bar{\mathbb{F}}_3)$. We note that the only character of $\hat{A}_5$ is the trivial character. To see this, notice that $\hat{A}_5$ is isomorphic to $\mathrm{SL}_2(\bar{\mathbb{F}}_5)$, so the abelianization of $\hat{A}_5$ is trivial. By the lack of

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

nontrivial characters and Theorem 3.2, there exist homogeneous polynomials F and G over $\bar{\mathbb{F}}_3$ that are absolutely invariant for $\hat{A}_5$, such that either $F=0$ or $\deg(F)+1=\deg(G)-1=\deg f$, and

$$f=\left[xF+\frac{\partial G}{\partial y}:yF-\frac{\partial G}{\partial x}\right].$$

In Magma [3], we compute the fundamental invariants of $\hat{A}_5$. Let $i\in\bar{\mathbb{F}}_3$ satisfy $i^2+1=0$; then the fundamental invariants are

$$u_1=x^{10}+iy^{10},$$
$$u_2=x^{11}y+(i+2)x^6y^6-ixy^{11}.$$

We now rule out some low-degree possibilities for F and G. We let c_1 and c_2 denote arbitrary nonzero constants in $\bar{\mathbb{F}}_3$.

- If $F=0$ and $G=c_1u_1$, then by direct computation, the map f has extra automorphisms.
- If $F=0$ and $G=c_2u_2$, then there is a common factor in the formula for f, so $\deg f<\deg(G)-1$.
- If $F=c_1u_1$ and $G=c_2u_2$, then there is a common factor in the formula for f.
- If $F=0$ and $G=c_1u_1^2$, then there is a common factor in the formula for f.

The above cases rule out all the possibilities for G such that $\deg G\leq 21$, proving the theorem. □

4. Moduli space $\mathcal{M}_2$ and its symmetry locus

We are interested in determining the automorphism locus $\mathcal{A}_2(\bar{\mathbb{F}}_p)\subset\mathcal{M}_2(\bar{\mathbb{F}}_p)$. It is known that $\mathcal{M}_2\cong\mathbb{A}^2$ via the explicit isomorphism $f\mapsto(\sigma_1,\sigma_2)$, where σ_1 and σ_2 are the first two elementary symmetric polynomials evaluated on the multipliers of the fixed points [17]. Any automorphism must permute the fixed points of a map and can only permute fixed points with the same multipliers because multipliers are invariant under conjugation. Utilizing this fact, in characteristic 0 the locus $\mathcal{A}_2\subset\mathcal{M}_2(\mathbb{C})$ is worked out in detail in [9] but is also discussed in [13]. The starting point is the discriminant of the multiplier polynomial:

$$x^3-\sigma_1x^2+\sigma_2x-(\sigma_1-2),\tag{4.1}$$

where σ_1, σ_2, and σ_3 are the elementary symmetric polynomials evaluated at the multipliers of the three fixed points. Note that we used the standard relation

$$\sigma_3=\sigma_1-2$$

to write (4.1) using only σ_1 and σ_2, see Milnor [13, Lemma 3.1]. For there to be a nontrivial automorphism, there must be two distinct fixed points with the same multiplier, so the discriminant of the multiplier polynomial vanishes if there is a nontrivial automorphism. The two components of the curve defined by the vanishing of (4.1) are then analyzed, only one of which corresponds to the existence of a nontrivial automorphism. This provides a description of $\mathcal{A}_2\subset\mathcal{M}_2(\mathbb{C})$ as a cuspidal cubic where every map has automorphism group C_2, except at the cusp, where it is S_3. In particular, in characteristic 0, the locus $\mathcal{A}_2$ is Zariski-closed and irreducible. We proceed similarly in characteristic $p>0$ to arrive at Theorem 1.8, which shows starkly different geometry in the $p=2$ case.

As an element of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$, an automorphism is completely determined by specifying the images of three points. It follows that if a map has three distinct fixed point multipliers, the three fixed points are fixed by any automorphism, and the map has no nontrivial automorphisms. We first show that every map with two distinct fixed points with the same multiplier has a nontrivial automorphism. We use several times the basic fact that a fixed point has multiplicity 1 if and only if its multiplier is not 1. Since the fixed points are the zeros of

$$f(x)-x,$$

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

they are simple roots (multiplicity one) if and only if the derivative

$$f'(x) - 1$$

does not also vanish.

Lemma 4.1. *Let $f \in \mathrm{Rat}_2(\bar{\mathbb{F}}_p)$. If f has two distinct fixed points with the same multiplier, then there exists an automorphism which maps the two fixed points to each other and fixes the third.*

Proof. Let $f \in \mathrm{Rat}_2(\bar{\mathbb{F}}_p)$ be a rational map which has two fixed points with the same multiplier λ. Note that $\lambda \neq 1$, since otherwise each fixed point has multiplicity at least 2, and there can only be three fixed points for a degree 2 map when counted with multiplicity. Label the multipliers of the three (with multiplicity) fixed points as λ_1, λ_2, and λ_3. Recall $\lambda_1\lambda_2 = 1 \iff \lambda_1 = \lambda_2 = 1$ even in positive characteristic since the relation $\sigma_1 = \sigma_3 + 2$ implies the (formal) identities:

$$(\lambda_1 - 1)^2 = (\lambda_1\lambda_2 - 1)(\lambda_1\lambda_3 - 1) \quad \text{and} \quad (\lambda_2 - 1)^2 = (\lambda_2\lambda_1 - 1)(\lambda_2\lambda_3 - 1).$$

So we are in the case that $\lambda_1\lambda_2 \neq 1$ and, by the Normal Forms Lemma [15, Lemma 5.3], the map f must be conjugate to a map of the form:

$$\phi(z) = \frac{z^2 + \lambda z}{\lambda z + 1}.$$

Then, conjugation by $z \mapsto \frac{1}{z}$ is an automorphism that permutes the fixed points 0 and ∞. □

4.1. Automorphism locus over $\mathbb{F}_p$, for $p \neq 2, 3$

In this case, we can follow Fujimura and Nishizawa [9, Proposition 1], since no coefficients that arise have prime divisors other than 2 and 3. For a map corresponding to the point (σ_1, σ_2) to have a nontrivial automorphism, at least two multipliers must be equal. The multipliers are the roots of the polynomial:

$$x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_1 + 2, \tag{4.2}$$

which has multiple roots if and only if its discriminant is 0. Therefore, there are at least two equal multipliers exactly at the vanishing of its discriminant, which is

$$(\sigma_2 - 2\sigma_1 + 3)(2\sigma_1^3 + \sigma_1^2\sigma_2 - \sigma_1^2 - 4\sigma_2^2 - 8\sigma_1\sigma_2 + 12\sigma_1 + 12\sigma_2 - 36). \tag{4.3}$$

Note that this equivalence holds over any field. The polynomial (4.3) is presented with two factors. The zero locus of the first, $\sigma_2 - 2\sigma_1 + 3$, is exactly the set of points corresponding to maps with a fixed point of multiplier 1. This is because a fixed point multiplier λ is a root of (4.2); substituting 1 for x yields $\sigma_2 - 2\sigma_1 + 3$. Following Milnor [13], we call the vanishing locus of this polynomial $\mathrm{Per}_1(1)$, since the locus is the set of all conjugacy classes that have a fixed point with multiplier of 1.

We claim that the second curve, a cuspidal cubic denoted S, is the automorphism locus of quadratic rational maps over $\mathbb{F}_p$ for $p > 3$.

We use the fact that a multiplier of a fixed point is equal to 1 if and only if its fixed point occurs with multiplicity greater than 1. The two curves have a unique point of intersection at $(\sigma_1, \sigma_2) = (3, 3)$, which corresponds to a triple fixed point where $\lambda_1 = \lambda_2 = \lambda_3 = 1$. All other points on $\mathrm{Per}_1(1)$ correspond to maps with a double fixed point and a single fixed point. Again by the Normal Forms Lemma [15, Lemma 5.3], maps with $\lambda_1 = \lambda_2 = 1$ are conjugate to a map of the form:

$$f(z) = z + \frac{1}{z} + \sqrt{1 - \lambda_3},$$

which has a double fixed point at infinity and a single fixed point at $\frac{-1}{\sqrt{1-\lambda_3}}$. Infinity has preimages 0 and itself; we know that automorphisms permute the set of fixed points and permute their preimages. The

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

only possible element of PGL_2 which could be an automorphism, then, is the map $z \mapsto \frac{1}{z}$, which is not an automorphism of f.

It follows that any map with a nontrivial automorphism must lie on S. Points with exactly two equal multipliers have C_2 as their automorphism group by Lemma 4.1. Points with all three multipliers equal must have $\sigma_1 = 3\lambda$ and $\sigma_3 = \lambda^3$, so the multiplier must be a root of the polynomial:

$$x^3 - 3x + 2. \tag{4.4}$$

This factors as $(x+2)(x-1)^2$, so there are only two points on S with triple multipliers: $(\sigma_1, \sigma_2) \in \{(-6, 12), (3, 3)\}$. The point $(\sigma_1, \sigma_2) = (-6, 12)$ has all three multipliers equal to -2, so by Lemma 4.1 applied to each pair of fixed points, its automorphism group is S_3. The point $(\sigma_1, \sigma_2) = (3, 3)$ corresponds to the map $f(z) = z + \frac{1}{z}$ [15, Lemma 5.3], which has $z \mapsto -z$ as its only nontrivial automorphism.

This completes the proof of Theorem 1.8 part (3), except for the verification that the cubic is cuspidal. We defer this to Section 4.3.

4.2. Automorphism locus over $\bar{\mathbb{F}}_2$

In $\bar{\mathbb{F}}_2$, we still have the automorphism locus contained in $S \cup \mathrm{Per}_1(1)$, but equation (4.3) reduces and we have the components:

$$\begin{aligned} S &= V(\sigma_1^2\sigma_2 - \sigma_1^2) = V(\sigma_1) \cup V(\sigma_2 - 1) \\ \mathrm{Per}_1(1) &= V(\sigma_2 - 1). \end{aligned}$$

As before, the only point on $\mathrm{Per}_1(1) \setminus \{(0, 1)\}$ that might have a nontrivial automorphism is the map with $\lambda_1 = \lambda_2 = \lambda_3 = 1$, which is $(\sigma_1, \sigma_2) = (1, 1)$, or by the second part of the Normal Forms Lemma, $f(z) = z + \frac{1}{z}$. This has no nontrivial automorphisms over $\bar{\mathbb{F}}_2$. Its unique fixed point is ∞, the other preimage of ∞ is 0, and the unique preimage of 0 in $\bar{\mathbb{F}}_2$ is 1. We would have expected $z \mapsto -z$ to be an automorphism, but it collapses to the identity map in characteristic 2.

Now we consider the intersection of the two components given by $\{(\sigma_1, \sigma_2) = (0, 1)\}$. This map is conjugate to $f(z) = z^2 + z$. Any possible automorphism of f must fix the point at infinity, so must be of the form $\phi(z) = az + b$, where $a, b \in \bar{\mathbb{F}}_2$ and $a \neq 0$. The equation

$$f \circ \phi = \phi \circ f$$

expands to

$$z^2a^2 + (2b + 1)za + (b^2 + b) = (z^2 + z)a + b. \tag{4.5}$$

Thus, we have the following relations on a and b:

$$a^2 = a, \quad \text{and} \quad 2ab + a = a, \quad \text{and} \quad b^2 + b = b. \tag{4.6}$$

Since a cannot be zero, we have $a = 1$ and $b = 0$, so the only automorphism is the identity.

Remark 4.2. *To recover a Zariski-closed automorphism locus, one can work instead with the automorphism group scheme [8]. By definition, the automorphism group scheme of a rational map f over $\bar{\mathbb{F}}_2$ is a closed subgroup scheme of*

$$\mathrm{PGL}_2 = \mathrm{Proj}\ \bar{\mathbb{F}}_2[a, b, c, d, (ad - bc)^{-1}]$$

determined by the ideal generated by the equation $f \circ \phi = \phi \circ f$, where $\phi \in \mathrm{PGL}_2$ is given by coordinates a, b, c, d. In the case of the map $f(z) = z^2 + z$, we can set $a = c = d = 1$ by the above reasoning about the fixed points, so the automorphism group scheme of f is isomorphic to a closed subgroup scheme of $\bar{\mathbb{F}}_2[b]$. With this identification, the group scheme structure on $\bar{\mathbb{F}}_2[b]$ is just that of the additive group scheme $\mathbb{G}_a$, reflecting the fact that these elements of PGL_2 are translations. By (4.6), the relation determining the automorphism group scheme of f is $b^2 = 0$; hence, we obtain the automorphism group scheme:

$$\alpha_2 := \mathrm{Spec}\ \bar{\mathbb{F}}_2[b]/(b^2).$$

This is a nontrivial closed subgroup scheme of $\mathbb{G}_a$, which is only possible in positive characteristic. The group scheme α_2 has just one closed point, reflecting the fact that f has only the identity automorphism, but the group scheme structure is nevertheless nontrivial. It is clear that there will be other instances in positive characteristic where the more general formulation of the automorphism group as a group scheme is needed in order to recover a Zariski-closed automorphism locus.

It remains to investigate $S \setminus \mathrm{Per}_1(1) = V(\sigma_1) \setminus \{(0, 1)\}$. Since this component is disjoint from $\mathrm{Per}_1(1)$, none of the multipliers are 1, and so corresponding maps have three distinct fixed points, but they still have at least two equal multipliers. There is only a single point with a triple multiplier, since (4.4) reduces to $x(x-1)^2$ and $\lambda = 1$ is on $\mathrm{Per}_1(1)$. The point given by $\lambda = 0$ again has S_3 as its automorphism group by Lemma 4.1, and every other point on $V(\sigma_1) \setminus \{(0, 1)\}$ has C_2 as its automorphism group.

This completes the proof of Theorem 1.8 part (1).

4.2.1. Normal form for $\mathcal{A}_2$

The symmetry locus in Rat_2 traced out via the Normal Forms Lemma is also parameterized by the family $f_c(z) = z^2 + cz$ defined in the discussion after Theorem 1.8. The Normal Forms Lemma sheds some light on what is happening in the family f_c. There are two finite fixed points with multiplier c, and ∞ is a fixed point of multiplier 0. From this, we can compute $\sigma_1 = 0$ and $\sigma_2 = c^2$. These maps always have the order 2 automorphism $z \mapsto z + c - 1$, which collapses to the identity when $c = 1$ (giving α_2). For a more geometric picture, the two finite fixed points are distinct, but they collapse onto each other when $c = 1$.

4.3. Automorphism locus over $\bar{\mathbb{F}}_3$

In $\bar{\mathbb{F}}_3$, equation (4.3) again reduces and we have

$$S = V(2\sigma_1^3 + \sigma_1^2\sigma_2 - \sigma_1^2 - \sigma_2^2 - 2\sigma_1\sigma_2) \tag{4.7}$$

$$\mathrm{Per}_1(1) = V(\sigma_2 - 2\sigma_1).$$

Over $\bar{\mathbb{F}}_3$, both $(\sigma_1, \sigma_2) = (3, 3)$ and $(\sigma_1, \sigma_2) = (-6, 12)$ (the triple-repeated multiplier maps) reduce to $(\sigma_1, \sigma_2) = (0, 0)$, the unique intersection of the two curves. This is the only possibility for a map with all three multipliers equal, since equation (4.4) reduces to $x^3 - 1$, which factors as $(x-1)^3$. Thus, there is no map with all three fixed points distinct and all three multipliers equal, so, by the same arguments as before, there is no map with automorphism group S_3.

On the remainder of $S \setminus \mathrm{Per}_1(1)$, it is still true that all three fixed points are distinct and two multipliers are equal, so corresponding maps have automorphism group C_2. Thus, the automorphism locus over $\bar{\mathbb{F}}_3$ is a cuspidal cubic S on which all maps have automorphism group C_2.

This completes the proof of Theorem 1.8 part (2), except for the verification that the cubic is cuspidal. We do this next.

4.4. Geometry of the automorphism locus

For every prime $p \neq 2$, we have shown that the automorphism locus is given by a cubic. It is natural to ask if this cubic is cuspidal, as is the case in characteristic 0, or if reduction modulo p changes the geometry. We now prove the curve remains cuspidal.

Proposition 4.3. *Let $p > 2$. Then the automorphism locus $\mathcal{A}_2 \subset \mathcal{M}_2(\bar{\mathbb{F}}_p)$ is a cuspidal cubic. In particular, it is irreducible. Furthermore, if $p > 3$, then the cusp is the unique point with automorphism group S_3 and all other points have automorphism group C_2.*

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

Proof. We first show that the automorphism locus has a unique singularity. If the locus were reducible, it would be the union of three lines or the union of a line and a degree 2 curve. In either case, one of the tangent lines would divide the defining polynomial. So it suffices to show that the tangent lines do not divide the defining polynomial. If there is a single tangent line with multiplicity 2, then the curve is cuspidal by definition.

In the case where $p = 3$, the automorphism locus is given by equation (4.7). The singularities are given by the common vanishing of the partial derivatives:

$$f_{\sigma_1} = 2\sigma_1\sigma_2 - 2\sigma_1 - 2\sigma_2$$
$$f_{\sigma_2} = \sigma_1^2 - 2\sigma_1 - 2\sigma_2,$$

which is the single point $(\sigma_1, \sigma_2) = (0, 0)$. The tangent lines at this singularity are given by the lowest degree homogeneous component of equation (4.7), which is $-\sigma_1^2 - \sigma_2^2 - 2\sigma_1\sigma_2 = -(\sigma_1 + \sigma_2)^2$. This is a double tangent line, and since $\sigma_1 + \sigma_2$ does not divide (4.7), we are done.

In the case where $p > 3$, the automorphism locus is given by:

$$S = V(2\sigma_1^3 + \sigma_1^2\sigma_2 - \sigma_1^2 - 4\sigma_2^2 - 8\sigma_1\sigma_2 + 12\sigma_1 + 12\sigma_2 - 36).$$

The partial derivatives are

$$S_{\sigma_1} = 6\sigma_1^2 + 2\sigma_1\sigma_2 - 2\sigma_1 - 8\sigma_2 + 12,$$
$$S_{\sigma_2} = \sigma_1^2 - 8\sigma_2 - 8\sigma_1 + 12\sigma_2,$$

and the only singularity is $(\sigma_1, \sigma_2) = (- 6, 12)$, which was shown above to have S_3 as its automorphism group. To compute the tangent lines, we need to first move the singularity to the origin with the translation $\sigma_1' = \sigma_1 + 6$ and $\sigma_2' = \sigma_2 - 12$, so then

$$S' = V(2\sigma_1'^3 + \sigma_1'^2\sigma_2' - 25\sigma_1'^2 - 20\sigma_1'\sigma_2' - 4\sigma_2'^2).$$

From this form, we can see that the tangent lines are given by:

$$-25\sigma_1'^2 - 20\sigma_1'\sigma_2' - 4\sigma_2'^2 = -(5\sigma_1' + 2\sigma_2')^2.$$

Once again, there is a double tangent line which does not divide the defining polynomial. □

This completes the proof of Theorem 1.8.

Appendix

In this Appendix, we summarize the classification of finite subgroups of $\mathrm{PGL}_2(k)$ up to conjugacy, where k is an algebraically closed field of prime characteristic p. The results are essentially due to Dickson [5] and Beauville [1]; for details and proofs, see Faber [7].

Let $B(k) \subset \mathrm{PGL}_2(k)$ be the *Borel group*, that is, the group of affine transformations $z \mapsto \alpha z + \beta$, where $\alpha \in k^\times$ and $\beta \in k^+$. Each finite subgroup of $B(k)$ may be written as a semi-direct product $\mu \rtimes \Lambda$, where μ is a finite subgroup of $k^\times$ and Λ is a finite subgroup of k^+.

A finite group is called *p-semi-elementary* if it has a unique p-Sylow subgroup of order p. Each subgroup of $B(k)$ is either 1, a p-regular cyclic group of order at least 2, or a p-semi-elementary group.

Table A1 should be read as follows:

- The empty set symbol $\emptyset$ denotes that no finite group isomorphic to Γ exists in $\mathrm{PGL}_2(k)$. For each entry that is not marked $\emptyset$, a finite group isomorphic to Γ exists in $\mathrm{PGL}_2(k)$.
- The entry p-reg in row Γ means that the group Γ exists in $\mathrm{PGL}_2(k)$, is unique up to conjugacy, and Γ is p-regular.
- The entry p-irr means that Γ exists in $\mathrm{PGL}_2(k)$, is unique up to conjugacy, and Γ is p-irregular.
- The entry p-irr* means that Γ exists in $\mathrm{PGL}_2(k)$, possibly with multiple conjugacy classes, and Γ is p-irregular.

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press

Table A1. *Finite subgroups of* $\mathrm{PGL}_2(k)$ *up to conjugacy, where k is an algebraically closed field of prime characteristic p.*

Group	...where...	$p=2$	$p=3$	$p=5$	$p\geq 7$
$\mathrm{PGL}_2(\mathbb{F}_q)$	q is a power of p	p-irr	p-irr	p-irr	p-irr
$\mathrm{PSL}_2(\mathbb{F}_q)$	q is a power of p	(p-irr)	p-irr	p-irr	p-irr
1		p-reg	p-reg	p-reg	p-reg
Cyclic C_n	$n\geq 2$ and $(n,p)=1$	p-reg	p-reg	p-reg	p-reg
p-Semi-elementary $\mu\rtimes\Lambda$	$\mu\subseteq k^\times$ and $\Lambda\subseteq k^+$	p-irr*	p-irr*	p-irr*	p-irr*
Dihedral D_{2n}	$n=2$	$\emptyset$	p-reg	p-reg	p-reg
Dihedral D_{2n}	$n>2$ and $(n,p)=1$	p-irr	p-reg	p-reg	p-reg
Tetrahedral A_4		(p-irr)	(p-irr)	p-reg	p-reg
Icosahedral A_5		(p-irr)	p-irr	(p-irr)	p-reg
Octahedral S_4		$\emptyset$	(p-irr)	p-reg	p-reg

- We mark some entries with parentheses (p-irr) to denote that, while the group Γ exists in $\mathrm{PGL}_2(k)$, it is accounted for elsewhere in Table A1 due to an accidental isomorphism. Thus, given a field k, each subgroup Γ of $\mathrm{PGL}_2(k)$ belongs to exactly one row marked p-reg, p-irr, or p-irr*. For the purposes of the realizability problem, it suffices to study just these cases.

The complete list of accidental isomorphisms for the entries marked (p-irr) is as follows:

- If $p=2$ and q is a power of p, then $\mathrm{PGL}_2(\mathbb{F}_q)\cong\mathrm{PSL}_2(\mathbb{F}_q)$.
- If $p=2$, then $A_4\cong B(\mathbb{F}_4)$ is p-semi-elementary.
- If $p=2$, then $A_5\cong\mathrm{PGL}_2(\mathbb{F}_4)$.
- If $p=3$, then $A_4\cong\mathrm{PSL}_2(\mathbb{F}_3)$.
- If $p=3$, then $S_4\cong\mathrm{PGL}_2(\mathbb{F}_3)$.
- If $p=5$, then $A_5\cong\mathrm{PSL}_2(\mathbb{F}_5)$.

For our applications, it is also useful to understand the possible containments between these subgroups of $\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$. By [7, Remark 2.1], a finite subgroup $\Gamma\subset\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$ is p-semi-elementary if and only if it fixes a unique point in $\mathbb{P}^1(\bar{\mathbb{F}}_p)$. A subgroup is dihedral if and only if it stabilizes, but does not fix, a subset of $\mathbb{P}^1(\bar{\mathbb{F}}_p)$ of cardinality 2. From these facts, and general group theory, we can deduce that for any strict inclusion of subgroups $\Gamma\subsetneq\Gamma'\subset\mathrm{PGL}_2(\bar{\mathbb{F}}_p)$,

(1) If $\Gamma\cong A_4$, then Γ' is isomorphic to S_4, $\mathrm{PGL}_2(\mathbb{F}_q)$, or $\mathrm{PSL}_2(\mathbb{F}_q)$ for some power q of p.
(2) If $\Gamma\cong A_5$ or $\Gamma\cong S_4$, then Γ' is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_q)$ or $\mathrm{PSL}_2(\mathbb{F}_q)$ for some power q of p.
(3) If $\Gamma\cong\mathrm{PSL}_2(\mathbb{F}_q)$ for some power q of p, then Γ' is isomorphic to $\mathrm{PGL}_2(\mathbb{F}'_q)$ or $\mathrm{PSL}_2(\mathbb{F}'_q)$ for some power q' of p.

References

[1] A. Beauville, Finite subgroups of *$PGL_2(K)$*, *Contemp. Math.* **522** (2010), 23–29.

[2] D. J. Benson, *Polynomial invariants of finite groups*, *LMS Lecture Notes*, vol. 190 (Cambridge University Press, New York, 1993).

[3] W. Bosma, J. Cannon and C. Playoust, The magma algebra system. I. The user language, *J. Symb. Comput.* **24**(3–4) (1997), 235–265.

[4] J. de Faria and B. Hutz, Automorphism groups and invariant theory on PN, *J. Algebra Appl.* **17**(9) (2017). https://doi.org/10.1142/S0219498818501621.

[5] L. E. Dickson, *Linear groups: With an exposition of the Galois field theory* (Dover Publication, New York, 1958).

[6] P. Doyle and C. McMullen, Solving the quintic by iteration, *Acta Math.* **163**(3–4) (1989), 151–180.

[7] X. Faber, Finite p-Irregular Subgroups of PGL(2,k), arXiv e-prints, p. arXiv:1112.1999 (2011).

[8] X. Faber, M. Manes and B. Viray, Computing conjugating sets and automorphism groups of rational functions, *J. Algebra* **423** (2015), 1161–1190.

[9] M. Fujimura and K. Nishizawa, Moduli spaces and symmetry loci of polynomial maps, in *Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation*, ISSAC'97 (ACM, New York, NY, USA, 1997), 342–348.

[10] B. Gontmacher, B. Hutz, G. Jorgenson, S. Srimani and S. Xu, Automorphism loci for degree 3 and degree 4 endomorphisms of the projective line, *New York J. Math.* **27** (2021), 1613–1702.

[11] F. Klein, *Vorlesungen Über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade* (Leipzig, Teubner, 1884).

[12] N. Miasnikov, B. Stout and P. Williams, Automorphism loci for the moduli space of rational maps, *Acta Arith.* **180**(3) (2017), 267–296.

[13] J. Milnor Geometry and dynamics of quadratic rational maps, *Exp. Math.* **2**(1) (1993), 37–83.

[14] J. H. Silverman, The field of definition for dynamical systems on $\mathbb{P}^1$, *Compositio Mathematica* **98** (1995), 269–304.

[15] J. H. Silverman, The space of rational maps on $\mathbf{P}^1$, *Duke Math. J.* **94**(1) (1998), 41–77.

[16] J. H. Silverman, *The arithmetic of dynamical systems*, *Graduate Texts in Mathematics*, vol. 241 (Springer-Verlag, New York, 2007).

[17] J. H. Silverman, *Moduli spaces and arithmetic dynamics*, *CRM Monograph Series*, vol. 30 (American Mathematical Society, Providence, RI, 2012).

[18] L. Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics (Taylor & Francis, New York, 1995).

[19] W. Stein and D. Joyner, SAGE: System for algebra and geometry experimentation, *Commun. Comput. Algebra (SIGSAM Bull.)* **39**(4) (2005), 61–64. http://www.sagemath.org.

[20] L. W. West, The moduli space of cubic rational maps, arXiv:1408.3247 (2014).

https://doi.org/10.1017/S0017089522000222 Published online by Cambridge University Press