COMPOSITIO MATHEMATICA

JOSEPH H. SILVERMAN

The field of definition for dynamical systems on $\mathbb{P}^1$

Compositio Mathematica, tome 98, nº 3 (1995), p. 269-304
<http://www.numdam.org/item?id=CM_1995__98_3_269_0>

Compositio Mathematica **98:** 269–304, 1995.

The field of definition for dynamical systems on $\mathbb{P}^1$

For Wolfgang Schmidt, on the occasion of his 60th birthday

JOSEPH H. SILVERMAN*
Department of Mathematics, Brown University, Providence, Rhode Island, U.S.A.
e-mail: jhs@gauss.math.brown.edu

Received 15 February 1994; accepted in final form: 12 July 1994

Abstract. Let Rat_d denote the set of rational maps $\mathbb{P}^1 \to \mathbb{P}^1$ of degree d, let PGL_2 act on Rat_d by conjugation, $\phi^f = f^{-1} \circ \phi \circ f$, and let M_d be the quotient of Rat_d by this action. A *field of definition* for a $\xi \in \mathrm{M}_d$ is a field over which at least one rational map in ξ is defined. The *field of moduli* of ξ is the fixed field of $\{\sigma \in G_K : \xi^\sigma = \xi\}$. Every field of definition contains the field of moduli. This paper treats the converse problem. We prove that if d is even, or if ξ contains a polynomial map, then the field of moduli of ξ is a field of definition. However, if d is odd, we show that there are numerous ξ's whose field of moduli is not a field of definition.

Introduction

Let $\phi(z) \in K(z)$ be a rational function with coefficients in a field K, or equivalently a rational map ϕ: $\mathbb{P}^1 \to \mathbb{P}^1$ defined over K. Recently there has been a spurt of interest in the number theoretic properties of the iterates of ϕ when K is taken to be an arithmetic field, such as a p-adic field or a number field. See for example [3, 6, 10–12, 14–17, 25–28]. Most of these cited papers deal with the dynamics of ϕ, by which we mean the behavior of points in $\mathbb{P}^1$ under the iterates of ϕ. In particular, the points in $\mathbb{P}^1$ are classified according to various properties they have. Some of these properties, such as periodicity, are purely algebraic, while others such as attracting/repelling depend on the field K having an absolute value, which may be either archimedean or non-archimedean.

The dynamics of a rational map $\phi(z)$ are unchanged if it is conjugated by an automorphism of $\mathbb{P}^1$. In other words, if $f(z) = (az + b)/(cz + d) \in \mathrm{PGL}_2$ is a non-trivial linear fractional transformation, then the rational maps $\phi(z)$ and $\phi^f = f^{-1} \circ \phi \circ f$ have equivalent dynamics. This is clear, since if a point P has some property for ϕ, then $f^{-1}P$ will have the same property for ϕ^f. Thus it

* Research partially supported by NSF DMS-9121727.

makes sense to consider the set of rational maps modulo conjugation by linear fractional transformations. We will call a conjugacy class of rational maps a *dynamical system*, and for a given rational map ϕ, we will denote the associated dynamical system by $[\phi]$.

In order to study arithmetic properties of a rational map ϕ, one needs to start with a field which contains the coefficients of ϕ. For example, the rational map

$$\phi(z) = z^2 + 2\sqrt{2}\,z - \sqrt{2}$$

is certainly defined over the field $\mathbb{Q}(\sqrt{2})$. However, if we conjugate this ϕ by the linear map $f(z) = z - \sqrt{2}$, then we obtain the rational function $\phi^f(z) = z^2 - 2$, which is defined over $\mathbb{Q}$. So the dynamical system $[\phi]$ is defined over $\mathbb{Q}$, since it contains a map with coefficients in $\mathbb{Q}$. We say that a field K is a *field of definition* for a dynamical system ξ if ξ contains a rational map ϕ which is defined over K. Clearly, for a given dynamical system ξ, we would like to find the smallest field of definition, if such a smallest field exists.

On the other hand, we can attach to any dynamical system ξ a unique field which is minimal in a moduli-theoretic sense. Briefly, choose any rational map $\phi \in \xi$ with coefficients in the algebraic closure $\overline{K}$ of K. Then the *field of moduli* of ξ is the fixed field in $\overline{K}$ of

$$\{\sigma \in \mathrm{Gal}(\overline{K}/K) \colon \ \phi^\sigma \in \xi\}.$$

In other words, the field of moduli of $[\phi]$ is the smallest field L with the property that for every $\sigma \in \mathrm{Gal}(\overline{K}/L)$ there is an automorphism $f \in \mathrm{PGL}_2$ such that $\phi^\sigma = \phi^f$.

It is not hard to see that the field of moduli of ξ must be contained in any field of definition for ξ. So our main question becomes:

$$\boxed{\text{Is the field of moduli of } \xi \text{ also a field of definition for } \xi?}$$

In many important situations we will show that this question has an affirmative answer.

THEOREM A. *Let K be a field of characteristic* 0, *and let $\xi = [\phi]$ be a dynamical system whose field of moduli is contained in K. Then K is a field of definition for ξ in either of the following situations:*

(a) *The degree* $\deg(\phi)$ *is even.*

(b) *The map ϕ is a polynomial map (i.e., $\phi(z) \in \overline{K}[z]$).*

In contrast to this positive result, we will show that our question has a negative answer for dynamical systems of odd degree.

THEOREM B. *Let K be a field of characteristic* 0. *Then for every odd integer $d \geqslant 3$ there exist (many) rational maps ϕ of degree d such that K is the field of moduli for $[\phi]$, but K is not a field of definition for $[\phi]$.*

An important ingredient in the proofs of Theorems A and B is an analysis of the stabilizer $\mathcal{A}_\phi$ of a rational map ϕ, where the stabilizer is defined to be

$$\mathcal{A}_\phi = \{f \in \mathrm{PGL}_2\colon\ \phi^f = \phi\}.$$

Not surprisingly, it turns out to be much easier to analyze $[\phi]$ if its stabilizer is trivial. Thus we will actually prove Theorem B by giving an explicit description of all maps ϕ with $\mathcal{A}_\phi = 1$ whose field of moduli is not a field of definition. As an example we cite the rational map

$$\phi(z) = i\left(\frac{z-1}{z+1}\right)^3. \tag{1}$$

Letting τ denote complex conjugation and $f(z) = -1/z$, it is easy to check that $\phi^\tau = \phi^f$, which proves that $\mathbb{Q}$ is the field of moduli of $[\phi]$. On the other hand, we will see in Section 6 that K is a field of definition for this $[\phi]$ if and only if -1 is a sum of two squares in K. In particular, there are no fields of definition for $[\phi]$ contained in $\mathbb{R}$.

In general, if ϕ has trivial stabilizer, we will construct a cohomology class $c_\phi \in H^1(G_K, \mathrm{PGL}_2)$ with the property that $c_\phi = 1$ if and only if K is a field of definition for $[\phi]$. Associated to such a cohomology class is a Brauer–Severi curve $i\colon\ \mathbb{P}^1 \to X_\phi$, where X_ϕ is defined over K and i is an isomorphism defined over $\overline{K}$. We will show that there is a morphism $\psi\colon\ X_\phi \to X_\phi$ defined over K so that the following diagram commutes:

$$\begin{tikzcd} \mathbb{P}^1 \arrow[r, "\phi"] \arrow[d, "i"'] & \mathbb{P}^1 \arrow[d, "i"'] \\ X_\phi \arrow[r, "\psi"] & X_\phi \end{tikzcd} \quad . \tag{2}$$

This cohomological/geometric construction quickly leads to a proof of Theorem A in the case that $\mathcal{A}_\phi = 1$.

If the stabilizer $\mathcal{A}_\phi$ is not trivial, then the situation becomes much more complicated. In Sections 3 and 4 we will analyze the finite subgroups of PGL_2 and prove a cohomology lifting theorem which will allow us to construct X_ϕ and the diagram (2) in certain situations. We will show in Section 5 that the lifting theorem applies to maps of even degree and to polynomial maps, which will complete the proof of Theorem A in all cases.

Couveignes [5] has recently studied the field of moduli for maps $\mathbb{P}^1 \to \mathbb{P}^1$ subject to the equivalence relation $\phi = \phi \circ f$. This is similar in many ways to the subject of this paper, but the different equivalence relation leads to some strikingly different results. For example, Couveignes gives an example in [5] of a polynomial whose field of moduli is not a field of definition, a possibility that is ruled out in our situation by Theorem A. We note that the work of Couveignes has interesting applications to Belyi functions and Grothendieck's "dessins", while the results in this paper are intended for the study of the arithmetic theory of dynamical systems. We also want to mention that there is a corresponding theory of fields of definition and moduli for abelian varieties and the maps connecting them. See for example [20], [21, § 5.5C], [22], and [23].

Although we have restricted our discussion in this introduction to fields of characteristic 0, most of our results are also valid for fields of characteristic $p > 0$. More precisely, we will prove our main results for general fields subject to the condition that the stabilizer group $\mathcal{A}_\phi$ have order prime to p. We also observe that the question of field of definition versus field of moduli can be formulated more generally for rational maps on $\mathbb{P}^n$ or on other varieties. Much of the basic set-up in Sections 1 and 2 carries over to this more general setting. But the proofs of our deeper results, such as Theorems A and B, do not seem to directly carry over, so we have been content in this paper to concentrate on the one-dimensional situation.

We conclude this introduction with a brief organizational survey of the paper. In Section 1 we give basic definitions, set notation, and prove a general cohomological sort of criterion describing fields of definition. We also discuss Brauer–Severi curves. In Section 2 we prove Theorem A (Corollary 2.2) for rational maps with trivial stabilizer. Section 3 contains a description of the finite subgroups of PGL_2, their normalizers, and a lifting theorem for their cohomology. In Section 4 we give a number of preliminary results concerning dynamical systems whose stabilizer group is non-trivial, and in Section 5 we use these results to complete the proof of Theorem A (Theorem 5.1). In section 6 we take up the question of dynamical systems whose field of moduli is not a field of definition, and by an explicit construction we prove a strengthened version of Theorem B (Theorem 6.1). Finally, in Section 7 we consider the $\overline{K}/K$-twists of a rational map $\phi \in K(z)$. We give the usual cohomological description of the set of twists and present some examples, including one which involves twisting by a non-abelian extension of K.

1. Field of definition and field of moduli

We begin by setting the following notation which will be used for the remainder of this paper:

d	an integer $d \geqslant 2$.
K	a field. Later we may make the assumption that K is a local field (a finite extension of $\mathbb{R}$, $\mathbb{Q}_p$ or $\mathbb{F}_p((T))$) or global field (a finite extension of $\mathbb{Q}$ or $\mathbb{F}_p(T)$).
G_K	the Galois group of a separable closure $\overline{K}$ of K.
Rat_d	the set of rational maps $\mathbb{P}^1 \to \mathbb{P}^1$ of degree d. We will often identify Rat_d with a subset of $\overline{K}(z)$. Notice that Rat_d has a natural structure as an affine subvariety of $\mathbb{P}^{2d+1}$.

$\mathrm{Rat}_d(K)$ the set of rational maps $\mathbb{P}^1 \to \mathbb{P}^1$ of degree d defined over K. We identify $\mathrm{Rat}_d(K)$ with a subset of $K(z)$.

PGL_2 the projective linear group. We will often use the natural identifications

$$\mathrm{PGL}_2 = \mathrm{Aut}(\mathbb{P}^1) = \mathrm{Rat}_1 = \left\{ \frac{az+b}{cz+d} \colon ad - bc \neq 0 \right\}.$$

We will say that two rational maps $\phi, \psi \in \mathrm{Rat}_d$ are (*linearly*) *conjugate* if they differ by an automorphism of $\mathbb{P}^1$,

$$\phi \circ f = f \circ \psi \quad \text{for some } f \in \mathrm{PGL}_2.$$

We define an action of $f \in \mathrm{PGL}_2$ on $\phi \in \mathrm{Rat}_d$ by

$$\phi^f \stackrel{\mathrm{def}}{=} f^{-1} \circ \phi \circ f,$$

and then the linear conjugacy class of ϕ is the set of all ϕ^f as f ranges over PGL_2. Notice this is a right action,

$$(\phi^f)^g = \phi^{fg}.$$

Linearly conjugate maps have equivalent dynamics, so we define the *dynamical system of* ϕ, denoted $[\phi]$, to be the image of ϕ in the quotient space

$$\mathrm{M}_d \stackrel{\mathrm{def}}{=} \mathrm{Rat}_d/\mathrm{PGL}_2.$$

Thus M_d is the moduli space of (algebraic) dynamical systems of degree d on $\mathbb{P}^1$, and $[\cdot]\colon \mathrm{Rat}_d \to \mathrm{M}_d$ is the natural map.

Remark. We will treat M_d as an abstract quotient space with no additional structure. Ultimately, of course, one would like to give M_d the structure of an algebraic variety and to find a "good" completion. For example, it seems to be well known among dynamicists that $\mathrm{M}_2 \cong \mathbb{A}^2$, at least as analytic spaces over $\mathbb{C}$. There is a general method for constructing moduli spaces described in [13] which will be used in a subsequent paper to construct M_d as a moduli space over $\mathbb{Z}$ and to show that $\mathrm{M}_2 \cong \mathbb{A}^2$ over $\mathbb{Z}$. However, we will not concern ourselves with such matters in this paper.

For any rational map $\phi \in \mathrm{Rat}_d$, we define the following two important sets:

$\mathrm{Fix}(\phi)$ the fixed set of ϕ, that is, $\{P \in \mathbb{P}^1\colon \phi(P) = P\}$.

$\mathcal{A}_\phi$ the stabilizer of ϕ, that is, $\{f \in \mathrm{PGL}_2\colon \phi^f = \phi\}$.

For future reference we note the easy equalities

$$\mathrm{Fix}(\phi^f) = f^{-1}(\mathrm{Fix}(\phi)) \quad \text{and} \quad \mathcal{A}_{\phi^f} = \mathcal{A}_\phi^f = f^{-1} \circ \mathcal{A}_\phi \circ f. \tag{3}$$

In particular, we define the *stabilizer* or (*automorphism group*) $\mathcal{A}_\xi$ of a dynamical system $\xi \in \mathrm{M}_d$ to be $\mathcal{A}_\phi$ for any map $\phi \in \xi$. Then $\mathcal{A}_\xi$ is well-defined as an abstract group, although as a subgroup of PGL_2 it is only determined up to conjugation.

We now turn to the question of fields of definition. An element $\sigma \in G_K$ acts on a rational map $\phi \in \mathrm{Rat}_d = \mathrm{Rat}_d(\overline{K})$ by acting on its coefficients. We denote this action by ϕ^σ. Note, however, that in spite of our notation, this is actually a left action, $\phi^{\sigma\tau} = (\phi^\tau)^\sigma$, because $\phi^\sigma(P) = \sigma \circ \phi \circ \sigma^{-1}(P)$. It is not hard to show, using Hilbert's theorem 90, that ϕ is defined over K if and only if $\phi^\sigma = \phi$ for all $\sigma \in G_K$, see for example [24, Exercise 1.12].

The matter is much less clear when we consider the dynamical system $[\phi]$ associated to ϕ. Notice that if $\psi = \phi^f$, then $\psi^\sigma = (\phi^\sigma)^{f^\sigma}$. This shows that the action of G_K on Rat_d descends to an action on $\mathrm{M}_d = \mathrm{M}_d(\overline{K})$, so we might say that a dynamical system $\xi \in \mathrm{M}_d$ is "defined" over K if $\xi^\sigma = \xi$ for all $\sigma \in G_K$. Another possible definition would be to require that the equivalence class ξ contain a rational map ϕ which is defined over K. This leads to the following two fundamental concepts.

DEFINITION. Let $\xi \in \mathrm{M}_d(\overline{K})$ be a dynamical system. The *field of moduli of* ξ is the fixed field of the group

$$\{\sigma \in G_K \colon \xi^\sigma = \xi\}.$$

We denote by $\mathrm{M}_d(K)$ the set of dynamical systems whose field of moduli is contained in K. A *field of definition for* ξ is any field L such that ξ contains a map $\phi \in \mathrm{Rat}_d$ defined over L. Equivalently, L is a field of definition for ξ if ξ is in the image of the natural map $\mathrm{Rat}_d(L) \to \mathrm{M}_d(L)$.

It is clear that the field of moduli of ξ is contained in any field of definition. The question of whether the field of moduli is itself a field of definition is far more subtle, and it is this question that we will be trying to answer in the rest of this paper.

We now describe a construction which will be essential for all of our future analysis. For dynamical systems ξ whose stabilizer $\mathcal{A}_\xi$ is trivial, this construction immediately gives a cohomology class whose triviality is equivalent to the field of moduli of ξ being a field of definition. However, if $\mathcal{A}_\xi$ is not trivial, then we only get a "cocycle modulo $\mathcal{A}_\xi$", which unfortunately doesn't even make sense since $\mathcal{A}_\xi$ will not generally be a normal subgroup of PGL_2.

PROPOSITION 1.1. *Let $\xi \in \mathrm{M}_d(K)$ be a dynamical system whose field of moduli is contained in K, and let $\phi \in \xi$ be any rational map in the system ξ.*

(a) *For every $\sigma \in G_K$ there exists an $f_\sigma \in \mathrm{PGL}_2$ such that*

$$\phi^\sigma = \phi^{f_\sigma}. \tag{4}$$

The map f_σ is determined by ϕ and σ up to (left) multiplication by an element of $\mathcal{A}_\phi$.

(b) *Having chosen f_σ's as in* (a), *the resulting map $f\colon G_K \to \mathrm{PGL}_2$ satisfies*

$$f_\sigma f_\tau^\sigma f_{\sigma\tau}^{-1} \in \mathcal{A}_\phi \quad \textit{for all } \sigma,\tau \in G_K. \tag{5}$$

We will say that f is a G_K-to-PGL_2 cocycle relative to $\mathcal{A}_\phi$.

(c) *Let $\Phi \in \xi$ be any other rational map in the system ξ, and for each $\sigma \in G_K$ choose an automorphism $F_\sigma \in \mathrm{PGL}_2$ as in* (a) *so that $\Phi^\sigma = \Phi^{F_\sigma}$. Then there exists a $g \in \mathrm{PGL}_2$ such that*

$$g^{-1}F_\sigma g^\sigma f_\sigma^{-1} \in \mathcal{A}_\phi \quad \textit{for all } \sigma \in G_K. \tag{6}$$

We will say that f and F are G_K-to-PGL_2 cohomologous relative to $\mathcal{A}_\phi$.

(d) *The field K is a field of definition for ξ if and only if there exists a $g \in \mathrm{PGL}_2$ such that*

$$g^{-1}g^\sigma f_\sigma^{-1} \in \mathcal{A}_\phi \quad \textit{for all } \sigma \in G_K. \tag{7}$$

Remark. If a dynamical system ξ has trivial stabilizer $\mathcal{A}_\xi = 1$, then Proposition 1.1 says that the map $f\colon G_K \to \mathrm{PGL}_2$ is a one-cocycle whose cohomology class in the cohomology set $H^1(G_K,\mathrm{PGL}_2)$ depends only on ξ. On the other hand, if $\mathcal{A}_\xi \neq 1$, then the criterion described in (6) is not an equivalence relation, so one cannot even define a "cohomology set relative to $\mathcal{A}_\phi$". If $\mathcal{A}_\phi$ is abelian, one can try to use the fact that the map $(\sigma,\tau) \to f_\sigma f_\tau^\sigma f_{\sigma\tau}^{-1}$ is a G_K-to-$\mathcal{A}_\phi$ two-cocycle to modify f into a true G_K-to-PGL_2 cocycle. But if $\mathcal{A}_\phi$ is not abelian, then $H^2(G_K,\mathcal{A}_\phi)$ does not exist and this approach will not work.

Proof. (a) We are given that $\xi \in \mathrm{M}_d(K)$, so for any $\sigma \in G_K$,

$$[\phi^\sigma] = [\phi]^\sigma = \xi^\sigma = \xi = [\phi].$$

This says precisely that there is an automorphism $f_\sigma \in \mathrm{PGL}_2$ such that $\phi^\sigma = \phi^{f_\sigma}$. Suppose that $f'_\sigma \in \mathrm{PGL}_2$ has the same property. Then

$$\phi^{f'_\sigma} = \phi^\sigma = \phi^{f_\sigma},$$

which proves that $f'_\sigma f_\sigma^{-1} \in \mathcal{A}_\phi$.

(b) Let $\sigma,\tau \in G_K$. We compute

$$\phi^{f_{\sigma\tau}} = \phi^{\sigma\tau} = (\phi^\tau)^\sigma = (\phi^{f_\tau})^\sigma = (\phi^\sigma)^{f_\tau^\sigma} = (\phi^{f_\sigma})^{f_\tau^\sigma} = \phi^{f_\sigma f_\tau^\sigma}.$$

Hence $f_\sigma f_\tau^\sigma f_{\sigma\tau}^{-1} \in \mathcal{A}_\phi$.

(c) Since $[\phi] = \xi = [\Phi]$, we can find some $g \in \mathrm{PGL}_2$ so that $\phi = \Phi^g$. Then for any $\sigma \in G_K$ we compute

$$\phi^{f_\sigma} = \phi^\sigma = (\Phi^g)^\sigma = (\Phi^\sigma)^{g^\sigma} = (\Phi^{F_\sigma})^{g^\sigma} = \phi^{g^{-1}F_\sigma g^\sigma}.$$

Hence $g^{-1}F_\sigma g^\sigma f_\sigma^{-1} \in \mathcal{A}_\phi$.

(d) Suppose first that K is a field of definition for ξ, so there is a map $\Phi \in \xi$ which is defined over K. Then $\Phi^\sigma = \Phi$ for all $\sigma \in G_K$, so in (c) we can take $F_\sigma = 1$, which gives the desired result.

Next suppose that there is a $g \in \mathrm{PGL}_2$ such that (7) holds. We write $h_\sigma = g^{-1}g^\sigma f_\sigma^{-1} \in \mathcal{A}_\phi$ and let $\Phi = \phi^{g^{-1}} \in \xi$. Then

$$\Phi^\sigma = \left(\phi^{g^{-1}}\right)^\sigma = (\phi^\sigma)^{(g^{-1})^\sigma} = \phi^{f_\sigma (g^{-1})^\sigma} = \phi^{h_\sigma^{-1} g^{-1} g^\sigma (g^{-1})^\sigma} = \phi^{g^{-1}} = \Phi.$$

Hence Φ is defined over K, so K is a field of definition for ξ.

One of the main results of this paper says that for polynomial maps, the field of moduli is always a field of definition. However, since we do not have a preferred "point at infinity", we will use the following characterization.

DEFINITION. Let $\phi \in \mathrm{Rat}_d$ be a rational map of degree $d \geqslant 2$. A point $P \in \mathbb{P}^1$ is called an *exceptional point* for ϕ if $\phi^{-1}(P) = \{P\}$. A rational map ϕ is said to be a *polynomial map* if it has an exceptional point. A dynamical system $\xi \in M_d$ of degree $d \geqslant 2$ is said to be *polynomial* if it contains a polynomial map.

Notice that if ξ is a polynomial dynamical system, then every $\phi \in \xi$ will be polynomial. This is clear, since if P is an exceptional point for ϕ and if $f \in \mathrm{PGL}_2$, then $f^{-1}(P)$ is an exceptional point for ϕ^f. We also observe that if we choose a coordinate function z on $\mathbb{P}^1$ so that the exceptional point P of ϕ is at infinity (i.e., $z(P) = \infty$), then ϕ is a polynomial in z in the usual sense, $\phi \in \overline{K}[z]$. Further, if $\phi\colon \mathbb{P}^1 \to \mathbb{P}^1$ is separable (e.g., if $\mathrm{char}(K) = 0$), then an exceptional point is a totally ramified fixed point.

We conclude this section with a brief discussion of $H^1(G_K, \mathrm{PGL}_2)$ and the associated twists of $\mathbb{P}^1$.

DEFINITION. A curve X/K is called a *Brauer–Severi curve* if there is an isomorphism $j\colon \mathbb{P}^1 \to X$ defined over $\overline{K}$. Two Brauer–Severi curves are considered *equivalent* if they are isomorphic over K.

PROPOSITION 1.2. (a) *There is a one-to-one correspondence between the set of Brauer–Severi curves up to equivalence and the cohomology set* $H^1(G_K, \mathrm{PGL}_2)$. *This correspondence is defined as follows. Let* X/K *be a Brauer–Severi curve, and choose a* $\overline{K}$*-isomorphism* $j\colon \mathbb{P}^1 \to X$. *Then the associated cohomology class* $c_X \in H^1(G_K, \mathrm{PGL}_2)$ *is given by the cocycle*

$$G_K \longrightarrow \mathrm{PGL}_2, \qquad \sigma \longmapsto j^{-1} \circ j^\sigma.$$

(b) *The following three conditions are equivalent*:

(i) X *is* K*-isomorphic to* $\mathbb{P}^1$.

(ii) $X(K) \neq \emptyset$.

(iii) $c_X = 1$.

Proof. Brauer–Severi varieties for $\mathbb{P}^n$ are discussed in [18, X §6], and twisting of curves is discussed in [24, X §2]. In particular, Proposition 1.2(a) is a special case of [24, X.2.2]. The equivalence of (i) and (iii) in (b) then follows from (a), while the equivalence of (i) and (ii) is an immediate consequence of the Riemann–Roch theorem.

The following elementary result, valid for arbitrary fields, gives a useful criterion for a Brauer–Severi curve to split. We note that if K is a local or global field, then a much stronger result is available, see Theorem 1.4 below.

PROPOSITION 1.3. *Let X/K be a Brauer–Severi curve. If there is a divisor $D \in \operatorname{Div}(X)$ such that D is defined over K and $\deg(D)$ is odd, then $X(K) \neq \emptyset$.*

Proof. We begin by taking cohomology of the exact sequences

$$1 \to \mu_2 \to \mathrm{SL}_2(\overline{K}) \to \mathrm{PGL}_2(\overline{K}) \to 1$$

and

$$1 \to \mu_2 \to \overline{K}^* \xrightarrow{z \to z^2} \overline{K}^* \to 1 \tag{8}$$

to obtain maps

$$H^1(G_K, \mathrm{PGL}_2) \hookrightarrow H^2(G_K, \mu_2) \xrightarrow{\sim} \mathrm{Br}(K)[2] \subset \mathrm{Br}(K).$$

Note that $H^1(G_K, \mathrm{SL}_2) = 0$ from [18, Chapter X, corollary to Proposition 3].

Let $c_X \in H^1(G_K, \mathrm{PGL}_2)$ be the cohomology class associated to X, and choose a Galois extension M/K such that $X(M) \neq \emptyset$. Proposition 1.2(b) tells us that the restriction of c_X to $H^1(G_M, \mathrm{PGL}_2)$ is trivial, so c_X comes from an element in $H^1(G_{M/K}, \mathrm{PGL}_2(M))$, which by abuse of notation we will again denote by c_X.

For any odd prime p, let G_p be the p-Sylow subgroup of $G_{M/K}$, and let $M_p = M^{G_p}$ be the fixed field of G_p. Taking various inflation and restriction maps, we obtain the following commutative diagram:

$$\begin{tikzcd}
H^1(G_K, \mathrm{PGL}_2) \arrow[r, hook, "1-1"] & H^2(G_K, \mu_2) \arrow[r, "\sim"] & \mathrm{Br}(K)[2] \subset \mathrm{Br}(K) \arrow[d, "\mathrm{Res}"] \\
H^1(G_{M/K}, \mathrm{PGL}(M)) \arrow[u, "\mathrm{Inf}"] \arrow[d, "\mathrm{Res}"] & & \mathrm{Br}(M_p) \\
H^1(G_p, \mathrm{PGL}_2(M)) \arrow[rr, hook, "1-1"] & & H^2(G_p, M^*) \arrow[u, "\mathrm{Inf}", "1-1"']
\end{tikzcd}$$

Here the bottom row comes from taking $G_p = G_{M/M_p}$ cohomology of the exact sequence

$$1 \to M^* \to \mathrm{GL}_2(M) \to \mathrm{PGL}_2(M) \to 1.$$

If we start with $c_X \in H^1(G_{M/K}, \mathrm{PGL}_2(M))$ and trace it around the diagram to $\mathrm{Br}(M_p)$, we find that it has order dividing 2 since it maps through $\mathrm{Br}(K)[2]$, and it has order a power of p since it maps through $H^1(G_p, M^*)$. Hence the image of c_X in $\mathrm{Br}(M_p)$ is zero. Now the injectivity of the maps along the bottom and up the right-hand side shows that $\mathrm{Res}(c_X) = 0$ in $H^1(G_p, \mathrm{PGL}_2(M))$. It follows from Proposition 1.2(b) that $X(M_p) \neq \emptyset$, so there is a divisor $D_p \in \mathrm{Div}(X)$ defined over K whose degree is prime to p. (To see this, take any $P \in X(M_p)$ and let $P_1, \ldots, P_n$ be the complete set of M_p/K conjugates of P. Then n is prime to p, since it divides $[M_p : K]$, and the divisor $(P_1) + \cdots + (P_n)$ is defined over K.)

We have proven that the greatest common divisor of the set

$$\{\deg(D_p)\colon\ p \text{ an odd prime}\}$$

is a power of 2, and $\deg(D)$ is odd by assumption, so we can find a (finite) linear combination

$$E = nD + \sum_{p \text{ odd}} n_p D_p \quad \text{with } \deg(E) = 1.$$

Notice that E is defined over K. The Riemann–Roch theorem tells us that the linear system $|E|$ is isomorphic to $\mathbb{P}^1_K$ and that we have a K-isomorphism

$$X \longrightarrow |E|, \qquad P \longmapsto (P).$$

Therefore X is K-isomorphic to $\mathbb{P}^1$, so $X(K) = \mathbb{P}^1(K)$ is not empty.

When K is a local or global field, the following result greatly strengthens Proposition 1.3. In particular, it says that a Brauer–Severi curve X/K always has points defined over some quadratic extension of K.

THEOREM 1.4. *Let K be a local or global field. For each $b \in K^*$ and each quadratic extension L/K, define a map*

$$[b, L/K]\colon\ G_K \to \mathrm{PGL}_2, \qquad [b, L/K]_\sigma = \begin{cases} z & \text{if } \sigma|_L = \mathrm{id}|_L, \\ b/z & \text{if } \sigma|_L \neq \mathrm{id}|_L. \end{cases}$$

(a) *Every element of $H^1(G_K, \mathrm{PGL}_2)$ is represented by a cocycle $[b, L/K]$.*

(b) *The cocycle $[b, L/K]$ is cohomologous to 1 if and only if $b \in \mathrm{N}_{L/K}(L^*)$.*

(c) *Let* $\mathrm{Br}(K)[2]$ *denote the* 2*-torsion in the Brauer group of* K*, and let* Inf *denote the inflation map on cohomology from* K *to* L*. Then there is a commutative diagram*

$$\begin{array}{ccccc} & & \mathrm{Br}(K)[2] & \xleftarrow{\text{onto}} & H^1(G_K,\mathrm{PGL}_2) \\ & & \uparrow{\scriptstyle\mathrm{Inf}} & & \uparrow{\scriptstyle\mathrm{Inf}} \\ K^*/\mathrm{N}_{L/K}(L^*) & \xrightarrow{\sim} & H^2(G_{L/K},L^*) & \xleftarrow{\text{onto}} & H^1(G_{L/K},\mathrm{PGL}_2(L)) \\ & & & & \\ b & & \longrightarrow & & [b,L/K] \end{array}$$

Proof. The exact sequences (8) already used above give

$$H^1(G_K,\mathrm{PGL}_2) \hookrightarrow H^2(G_K,\mu_2) \xrightarrow{\sim} \mathrm{Br}(K)[2].$$

(Note that the left-hand map is only injective as a map of pointed sets.) For local and global fields, every element of $\mathrm{Br}(K)$ of order 2 splits over a quadratic extension of K. This is a special case of the more general result that an element of $\mathrm{Br}(K)$ of order n splits over a cyclic extension of K of degree dividing n. For local fields this is immediate from [18, Chapter XIII, Proposition 7], which says that any extension of degree n will work. For global fields the desired result is [1, Chapter 10, corollary to Theorem 5].

Hence every element of $H^1(G_K,\mathrm{PGL}_2)$ is represented by a cocycle ω: $G_{L/K} \to \mathrm{PGL}_2(L)$ for some quadratic extension L/K. If we write $G_{L/K} = \{1,\tau\}$, then ω is determined by its value at τ, say $\omega_\tau = (Az+B)/(Cz+D)$. The condition that ω be a cocycle is the single relation $\omega_\tau\omega_\tau^\tau = z$ It is now an exercise to determine the exact form of ω_τ, but lacking a suitable reference, we give the details.

First, if $c \neq 0$, then we let $f = z + d/c$ and replace ω by the cohomologous cocycle $f^\tau\omega_\tau f^{-1} = (az+b)/cz$. Then the condition $\omega_\tau\omega_\tau^\tau = z$ forces $a = 0$ and $(b/c)^\tau = (b/c)$. Hence $\omega = [b/c, L/K]$ with $b/c \in K^*$.

Second, suppose that $c = 0$. Then ω_τ has the form $az+b$, so ω is a 1-cocycle with values in the affine linear group

$$\mathrm{AGL}_2(L) = \{az+b\colon\ a \in L^*,\ b \in L\}.$$

Taking cohomology of the exact sequence

$$\begin{array}{ccccccc} 1 \to & L^+ & \to & \mathrm{AGL}_2(L) & \to & L^* & \to 1 \\ & b & \mapsto & z+b, \quad az+b & \mapsto & a & \end{array}$$

and using [18, Chapter X, Propositions 1, 2] gives

$$0 = H^1(G_{L/K},L^+) \to H^1(G_{L/K},\mathrm{AGL}_2(L)) \to H^1(G_{L/K},L^*) = 0.$$

Hence in this case ω is cohomologous to 1, so it equals $[1, L/K]$. This completes the proof of (a). We will use the following lemma to verify (b).

LEMMA 1.5. *Let L/K be a Galois extension, let ω: $G_{L/K} \to \mathrm{PGL}_m(L)$ be a cocycle. Then ω is cohomologous to 1 if and only if it lifts to a cocycle $\overline{\omega}$: $G_{L/K} \to \mathrm{GL}_m(L)$.*

Proof. We take cohomology of the exact sequence

$$1 \to L^* \to \mathrm{GL}_m(L) \to \mathrm{PGL}_m(L) \to 1$$

and use the fact that $H^1(G_{L/K}, \mathrm{GL}_m(L)) = 0$ [18, Chapter X, Proposition 3]. This gives a map

$$\delta\colon\ H^1(G_{L/K}, \mathrm{PGL}_m(L)) \longrightarrow H^2(G_{L/K}, L^*)$$

with the property that $\delta(c) = 0$ if and only if $c = 0$. Letting $\overline{\omega}$: $G_{L/K} \to \mathrm{GL}_m(L)$ be any lifting of ω, the cohomology class $\delta(\omega)$ is represented by the cocycle

$$\delta(\omega)_{\sigma,\tau} = \overline{\omega}_\sigma \overline{\omega}_\tau{}^\sigma \overline{\omega}_{\sigma\tau}{}^{-1} \quad \text{(mod coboundaries)}.$$

If $\overline{\omega}$ is a cocycle, then $\delta(\omega) = 1$, so ω is cohomologous to 1. Conversely, if $\delta(\omega) = 1$, then there is a map a: $G_{L/K} \to L^*$ such that

$$\delta(\omega)_{\sigma,\tau} = \overline{\omega}_\sigma \overline{\omega}_\tau{}^\sigma \overline{\omega}_{\sigma\tau}^{-1} = a_\sigma a_\tau^\sigma a_{\sigma\tau}^{-1} \quad \text{for all } \sigma, \tau \in G_{L/K}.$$

(Elements of L^* are identified with scalar matrices.) It follows that the map $a^{-1}\overline{\omega}$ is a cocycle $G_{L/K} \to \mathrm{GL}_m(L)$ which is a lifting of ω. This completes the proof of Lemma 1.5.

We now resume the proof of Theorem 1.4. According to Lemma 1.5, the cocycle $[b, L/K]$: $G_{L/K} \to \mathrm{PGL}_2(L)$ is cohomologous to 1 if and only if it can be lifted to a cocycle with values in $\mathrm{GL}_2(L)$. Since $G_{L/K} = \{1, \tau\}$, this is equivalent to the existence of an element $u \in L^*$ such that

$$\begin{pmatrix} 0 & u^{-1}b \\ u^{-1} & 0 \end{pmatrix} \begin{pmatrix} 0 & u^{-1}b \\ u^{-1} & 0 \end{pmatrix}^\tau = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This equality holds exactly when $uu^\tau = b$, which proves that $[b, L/K]$ is cohomologous to 1 if and only if $b \in \mathrm{N}_{L/K}(L^*)$. This completes the proof of (b).

It remains to check the commutative diagram in (c). The isomorphism of $K^*/N_{L/K}(L^*)$ and $H^2(G_{L/K}, L^*)$ is the usual isomorphism of $\widehat{H}^0$ and H^2 for cyclic groups. The surjectivity of the two connecting maps labeled "onto" follows from [18, Chapter X, Propositions 8, 9 and Lemma 1]. Finally, an easy calculation which we leave for the reader shows that the map along the bottom row is given by $b \to [b, L/K]$.

2. Rational maps with trivial stabilizer

In this section we will use the material developed in section 1 to analyze dynamical systems with trivial stabilizer. We refer the reader to [18, appendix to Chapter VII] for a general discussion of non-abelian group cohomology.

THEOREM 2.1. *Let $\xi \in \mathrm{M}_d(K)$ be a dynamical system with trivial stabilizer $\mathcal{A}_\xi = 1$.*

(a) *There is a cohomology class $c_\xi \in H^1(G_K, \mathrm{PGL}_2)$ with the following property: For any rational map $\phi \in \xi$ there is a one-cocycle $f\colon G_K \to \mathrm{PGL}_2$ in the class of c_ξ so that*

$$\phi^\sigma = \phi^{f_\sigma} \quad \text{for all } \sigma \in G_K. \tag{9}$$

(b) *Let X_ξ/K be the Brauer–Severi curve associated to the cohomology class c_ξ. (See Proposition 1.2.) Then for any rational map $\phi \in \xi$ there exists an isomorphism $i\colon \mathbb{P}^1 \to X_\xi$ defined over $\overline{K}$ and a rational map $\Phi\colon X_\xi \to X_\xi$ defined over K so that the following diagram commutes:*

$$\begin{tikzcd} \mathbb{P}^1 \arrow[r, "\phi_{/\overline{K}}"] \arrow[d, "\wr" left, "i_{/\overline{K}}"] & \mathbb{P}^1 \arrow[d, "\wr" left, "i_{/\overline{K}}"] \\ X_\xi \arrow[r, "\Phi_{/K}"] & X_\xi \end{tikzcd} . \tag{10}$$

(c) *The following are equivalent:*

(i) *K is a field of definition for ξ.*

(ii) *$X_\xi(K) \neq \emptyset$.*

(iii) *$c_\xi = 1$.*

Proof. (a) This is immediate from Proposition 1.1 and our assumption that $\mathcal{A}_\xi = 1$. Thus Proposition 1.1(a) says that $f\colon G_K \to \mathrm{PGL}_2$ is determined by ϕ, Proposition 1.1(b) says that f is a one-cocycle, and Proposition 1.1(c) says that any other choice of $\phi \in \xi$ leads to a cohomologous cocycle, so the associated cohomology class depends only on ξ.

(b) Let $j\colon \mathbb{P}^1 \to X_\xi$ be a $\overline{K}$-isomorphism, so c_ξ is the cohomology class associated to the cocycle $\sigma \mapsto j^{-1}j^\sigma$. On the other hand, we know from (a) that c_ξ is associated to the cocycle $\sigma \mapsto f_\sigma$. Hence these two cocycles are cohomologous, so there is an element $g \in \mathrm{PGL}_2$ so that

$$f_\sigma = g^{-1}(j^{-1}j^\sigma)g^\sigma \quad \text{for all } \sigma \in G_K.$$

We let $i = jg$ and define $\Phi = i\phi i^{-1}$. Then the diagram (10) clearly commutes, and it only remains to verify that Φ is defined over K. For any $\sigma \in G_K$ we compute

$$\begin{aligned} \Phi^\sigma &= i^\sigma \phi^\sigma (i^{-1})^\sigma = (j^\sigma g^\sigma)(f_\sigma^{-1}\phi f_\sigma)(j^\sigma g^\sigma)^{-1} \\ &= (j^\sigma g^\sigma)(g^{-1}j^{-1}j^\sigma g^\sigma)^{-1}\phi(g^{-1}j^{-1}j^\sigma g^\sigma)(j^\sigma g^\sigma)^{-1} \\ &= jg\phi g^{-1}j^{-1} = \Phi. \end{aligned}$$

(c) The equivalence of (ii) and (iii) is immediate from Proposition 1.2(b), and the equivalence of (i) and (iii) follows from Proposition 1.1(d) and our assumption that $\mathcal{A}_\xi = 1$.

The following corollary will serve to illustrate the strength of Theorem 2.1. We will later prove that these results hold more generally without the assumption that the stabilizer be trivial.

COROLLARY 2.2. *Let $\xi \in \mathrm{M}_d(K)$ be a dynamical system with $\mathcal{A}_\xi = 1$.*

(a) *If $d \equiv 0 \pmod 2$, then K is a field of definition for ξ.*

(b) *If the dynamical system ξ is polynomial (i.e., ξ contains a polynomial map), then K is a field of definition for ξ.*

Proof. Take any rational map $\phi \in \xi$, and choose i: $\mathbb{P}^1 \to X_\xi$ and Φ: $X_\xi \to X_\xi$ as in Theorem 2.1(b) so that the diagram (10) commutes.

(a) Let $\mathrm{Fix}(\Phi)$ be the set of fixed points of Φ taken with multiplicity. We will treat $\mathrm{Fix}(\Phi)$ as a divisor on $\mathbb{P}^1$. More formally, if we let Γ_Φ be the graph of Φ and Δ: $X_\xi \to X_\xi \times X_\xi$ the diagonal map, then $\mathrm{Fix}(\Phi) \in \mathrm{Div}(X_\xi)$ is the pull-back divisor $\mathrm{Fix}(\Phi) = \Delta^*(\Gamma_\Phi)$. Note that the divisor $\mathrm{Fix}(\Phi)$ is defined over K.

We further observe that the divisor $\mathrm{Fix}(\Phi)$ has degree $d+1$. This follows from the fact that Γ_Φ is a divisor of type $(1, d)$ and the diagonal $\Delta(X_\xi)$ is a divisor of type $(1,1)$ in $\mathrm{Num}(X \times X) = \mathbb{Z} \times \mathbb{Z}$. Equivalently, if we write $\Phi = [\Phi_1, \Phi_2]$, where Φ_1, Φ_2 are homogeneous forms of degree d, then $\mathrm{Fix}(\Phi)$ is the divisor of zeros for the $d+1$ form $y\Phi_1(x,y) - x\Phi_2(x,y)$, so $\deg(\mathrm{Fix}(\Phi)) = d+1$.

Recalling that d is even by assumption, this proves that X_ξ has a divisor of odd degree defined over K, namely $\mathrm{Fix}(\Phi)$. It follows from Proposition 1.2 that $X_\xi(K) \neq \emptyset$, and then Theorem 2.1(c) tells us that K is a field of definition for ξ.

(b) Let $\phi \in \xi$, so ϕ is a polynomial map. By definition, this means that ϕ has an exceptional point $P \in \mathbb{P}^1$. Let $Q = i(P) \in X_\xi$. Then Q is an exceptional point of Φ. This is clear from (10), since i: $\mathbb{P}^1 \to X_\xi$ is an isomorphism. But for any $\sigma \in G_K$ we have

$$\Phi^{-1}(Q^\sigma) = (\Phi^{-1}(Q))^\sigma = \{Q\}^\sigma = \{Q^\sigma\},$$

since Φ is defined over K. Thus Q^σ is also an exceptional point of Φ. We consider two cases.

First, suppose that P is the only exceptional point of ϕ. Then Q is the unique exceptional point of Φ, so from above we have $Q^\sigma = Q$ for all $\sigma \in G_K$. Hence $Q \in X_\xi(K)$, and then Theorem 2.1(c) says that K is a field of definition for ξ.

Next, suppose that ϕ has a second exceptional point P'. Let $g \in \mathrm{PGL}_2$ be a transformation with $g(0) = P$ and $g(\infty) = P'$. Then 0 and ∞ are exceptional points of ϕ^g, so ϕ^g must have the form $\phi = az^d$ for some $a \in \overline{K}^*$. Letting $h(z) = a^{-1/(d-1)}z$, we find that $\phi^{gh} = z^d \in \xi$, which shows directly that K is a field of definition for ξ.

3. Cohomology of finite subgroups of PGL_2

In order to analyze rational maps with non-trivial stabilizers, it is necessary to describe the finite subgroups of PGL_2 and their normalizers. The classification of finite subgroups of PGL_2 is, of course, quite classical, and the subsequent description of their normalizers is a simple exercise.

THEOREM 3.1. *Let A be a finite subgroup of $\mathrm{PGL}_2(\overline{K})$, and suppose either that $\mathrm{char}(K) = 0$ or that the order of A is prime to $\mathrm{char}(K)$.*

(a) *The group A is isomorphic to one of the following groups:*

$A \cong \mathfrak{C}_n =$ *cyclic group of order n, $n \geqslant 1$.*
$A \cong \mathfrak{D}_{2n} =$ *dihedral group of order $2n$, $n \geqslant 2$.*
$A \cong \mathfrak{A}_4 =$ *tetrahedral group $=$ alternating group of order* 12.
$A \cong \mathfrak{S}_4 =$ *octohedral group $=$ symmetric group of order* 24.
$A \cong \mathfrak{A}_5 =$ *icosohedral group $=$ alternating group of order* 60.

(b) *More precisely, if we let ζ_n denote a primitive nth root of unity, then A is linearly conjugate to one of the following subgroups of* PGL_2, *where we identify* PGL_2 *with* Rat_1:

$$\mathfrak{C}_n = \langle \zeta_n z\rangle, \qquad \mathfrak{D}_{2n} = \left\langle \zeta_n z, \frac{1}{z}\right\rangle, \qquad \mathfrak{A}_4 = \left\langle -z, \frac{1}{z}, i\frac{z+1}{z-1}\right\rangle,$$
$$\mathfrak{S}_4 = \left\langle iz, \frac{1}{z}, i\frac{z+1}{z-1}\right\rangle, \qquad \mathfrak{A}_5 = \left\langle \zeta_5 z, -\frac{1}{z}, \frac{(\zeta_5+\zeta_5^{-1})z+1}{1-(\zeta_5+\zeta_5^{-1})z}\right\rangle.$$

(Here $\langle f_1, \dots, f_r\rangle$ denotes the group generated by $f_1, \dots, f_r$.) In particular, A is linearly conjugate to a subgroup of PGL_2 *which is defined over K.*

(c) *Let $\mathfrak{D}_\infty$ denote the infinite dihedral group $\mathbb{G}_m \rtimes \mu_2$, which we think of as embedded in* PGL_2 *via*

$$\mathfrak{D}_\infty = \{az\colon\ a \in \overline{K}^*\} \cup \{b/z\colon\ b \in \overline{K}^*\}.$$

For each of the finite groups A listed in (b), *the normalizer $N(A)$ of A in* PGL_2 *is as follows:*

$$\begin{array}{lll} N(\mathfrak{C}_1) = \mathrm{PGL}_2, & N(\mathfrak{C}_n) = \mathfrak{D}_\infty & (n \geqslant 2), \\ N(\mathfrak{D}_4) = \mathfrak{S}_4, & N(\mathfrak{D}_{2n}) = \mathfrak{D}_{4n} & (n \geqslant 3), \\ N(\mathfrak{A}_4) = \mathfrak{S}_4, & N(\mathfrak{S}_4) = \mathfrak{S}_4, & N(\mathfrak{A}_5) = \mathfrak{A}_5. \end{array}$$

Proof. (a) For $K = \mathbb{C}$, this is a classical result which may be found, for example, in [29, Chapter 9 §68]. The proof for $K = \mathbb{C}$ uses the fact that $\mathrm{SO}_3(\mathbb{R})$ is the maximal compact subgroup of $\mathrm{PGL}_2(\mathbb{C})$, which explains why the symmetry groups of the regular solids make their appearance. As explained in [19, Proposition 16], one can prove the more general result by reworking the classical proof, or, in the case that $\mathrm{char}(K) = 0$, one can appeal to the result over $\mathbb{C}$ and use the Lefschetz principle.

(b) One finds in [29, 9 §§71–78] the explicit representations listed in (b). Again one can either rework the derivation in [29] in the general case, or if working in characteristic 0, reduce directly to $K = \mathbb{C}$. There remains the assertion that the given groups are defined over K. This is clear for $\mathfrak{C}_n$ and $\mathfrak{D}_{2n}$, and for $\mathfrak{A}_4$, $\mathfrak{S}_4$, and $\mathfrak{A}_5$ it is a simple matter using the given generators to write out all of the elements and check that they are G_K invariant.

(c) Let A be one of the groups listed in (b), and let $f = (az+b)/(cz+d)$ be an element of $N(A)$. Further, let $\phi_n(z) = \zeta_n z$ and $\psi(z) = 1/z$.

We begin with the cyclic group $\mathfrak{C}_n$, which is generated by the map ϕ_n. It is clear that $N(\mathfrak{C}_1) = \mathrm{PGL}_2$, so we will assume that $n \geqslant 2$. We are given that $\phi_n^f \in \mathfrak{C}_n$, which means that $\phi_n^f = \phi_n^k$ for some integer k. Written out explicitly, this says that

$$\phi_n^f = \frac{(ad\zeta_n - bc)z + bd(\zeta_n - 1)}{ac(1-\zeta_n)z + (ad - bc\zeta_n)} = \zeta_n^k z = \phi_n^k. \tag{11}$$

It follows that $ac = bd = 0$, since $\zeta_n \neq 1$. On the other hand, we know that $ad - bc \neq 0$, since otherwise f is constant, so we are left with two possibilities, namely $a = d = 0$ or $b = c = 0$. If $a = d = 0$, then (11) reduces to $\phi_n^f = \zeta_n^{-1} z$, and if $b = c = 0$, then (11) becomes $\phi_n^f = \zeta_n z$, so both are possible. This proves that

$$N(\mathfrak{C}_n) = \left\{az\colon\ a \in \overline{K}^*\right\} \cup \left\{b/z\colon\ b \in \overline{K}^*\right\} = \mathfrak{D}_\infty.$$

Next we consider the dihedral group $\mathfrak{D}_{2n}$, which is generated by ϕ_n and ψ. We are given that $\phi_n^f \in \mathfrak{D}_{2n}$, so ϕ_n^f is equal to either some ϕ_n^k or some $\phi_n^k\psi$. Suppose first that $\phi_n^f = \phi_n^k$. Then (11) says that f has the form $f = az$ or $f = b/z$. If $f = az$, then $\psi^f = 1/a^2 z$ will be in $\mathfrak{D}_{2n}$ if and only if $a^{2n} = 1$; and similarly if $f = b/z$, then $\psi^f = b^2/z$ will be in $\mathfrak{D}_{2n}$ if and only if $b^{2n} = 1$.

Next suppose that $\phi_n^f = \phi_n^k\psi$. Writing this out gives the equality

$$\phi_n^f = \frac{(ad\zeta_n - bc)z + bd(\zeta_n - 1)}{ac(1-\zeta_n)z + (ad - bc\zeta_n)} = \frac{\zeta_n^k}{z} = \phi_n^k\psi. \tag{12}$$

Hence $ad\zeta_n - bc = ad - bc\zeta_n = 0$, which implies that

$$ad(\zeta_n - \zeta_n^{-1}) = bc(\zeta_n - \zeta_n^{-1}) = 0. \tag{13}$$

If $n \geqslant 3$ (i.e., $\zeta_n \neq -1$), then (13) implies that $ad = bc = 0$, contradicting the assumption that f has degree 1. Hence if $n \geqslant 3$, then we cannot have $\phi_n^f = \phi_n^k\psi$, and so

$$N(\mathfrak{D}_{2n}) = \left\{az\colon\ a^{2n} = 1\right\} \cup \left\{b/z\colon\ b^{2n} = 1\right\} = \mathfrak{D}_{4n}.$$

Similarly, if $n = 2$, then (12) tells us that $ad + bc = 0$ and that $ac = \pm bd$. Further, we know that $\psi^f \in \mathfrak{D}_4$, say $\psi^f = \phi_n^\ell$. Writing this out yields

$$\psi^f = \frac{(-ab+cd)z + (d^2 - b^2)}{(a^2 - c^2)z + (ab - cd)} = \zeta_n^\ell z = \phi_n^\ell.$$

Thus f must also satisfy $a^2 = c^2$ and $b^2 = d^2$. Taking the various sign choices leads to $N(\mathfrak{D}_4) = \mathfrak{S}_4$. We leave the algebra for the reader. Alternatively, the given restrictions on f show that $N(\mathfrak{D}_4)$ is a finite group, it is well known that $\mathfrak{S}_4$ contains $\mathfrak{D}_4$ as a normal subgroup, and $\mathfrak{A}_5$ is simple, so the equality $N(\mathfrak{D}_4) = \mathfrak{S}_4$ follows from the list in (b).

A similar analysis shows that the normalizers of $\mathfrak{A}_4$, $\mathfrak{S}_4$, and $\mathfrak{A}_5$ are finite. Then using the fact that $\mathfrak{A}_4 \lhd \mathfrak{S}_4$, that $\mathfrak{A}_5$ is simple, and that none of $\mathfrak{A}_4$, $\mathfrak{S}_4$, or $\mathfrak{A}_5$ is contained in a dihedral group, it is clear from the list in (b) that $N(\mathfrak{A}_4) = \mathfrak{S}_4$, $N(\mathfrak{S}_4) = \mathfrak{S}_4$, and $N(\mathfrak{A}_5) = \mathfrak{A}_5$.

The following lifting theorem will be crucial when we attempt to extend Theorem 2.1 to dynamical systems with non-trivial stabilizer groups. We remark that in general, neither part of Theorem 3.2 is true for even values of n.

THEOREM 3.2. *Let A be one of the finite subgroups of* $\mathrm{PGL}_2(\overline{K})$ *listed in Theorem* 3.1(b), *and let N be the normalizer of A in* $\mathrm{PGL}_2(\overline{K})$. *Then the natural map*

$$H^1(G_K, N) \longrightarrow H^1(G_K, N/A) \tag{14}$$

is surjective in the following two cases:
(i) $A = \mathfrak{C}_n$ *with* $n \equiv 1 \pmod 2$.
(ii) $A = \mathfrak{D}_{2n}$ *with* $n \equiv 1 \pmod 2$.

Remark. The group N in Theorem 3.2 is not abelian, so $H^1(G_K, N)$ is only a cohomology set, not a group. Further, even in the case that A is abelian, it will not be in the center of N, so there is no connecting map from $H^1(G_K, N/A)$ to $H^2(G_K, A)$. Thus in order to prove Theorem 3.2, we will have to explicitly lift a cocycle from N/A to N.

Remark. Amplifying on the proceeding remark, we observe that the twisted product $\mathfrak{D}_\infty = \mathbb{G}_m \rtimes \mu_2$ sits in the exact sequence

$$1 \longrightarrow \mathbb{G}_m \longrightarrow \mathfrak{D}_\infty \longrightarrow \mu_2 \longrightarrow 1.$$

Taking cohomology and using Hilbert's theorem 90 gives an exact sequence

$$0 \longrightarrow H^1(G_K, \mathfrak{D}_\infty) \longrightarrow H^1(G_K, \mu_2). \tag{15}$$

However, (15) is an exact sequence of pointed sets, not of groups. In particular, suppose that c_1: $\sigma \mapsto (a_\sigma, t_\sigma)$ is a G_K-to-$\mathfrak{D}_\infty$ cocycle. Then c_2: $\sigma \mapsto (1, t_\sigma)$ is also a cocycle, the cocycles c_1 and c_2 clearly have the same image in $H^1(G_K, \mu_2)$, yet in general c_1 and c_2 will not be cohomologous in $H^1(G_K, \mathfrak{D}_\infty)$. This shows that one needs to be careful when dealing with exact sequences in non-abelian cohomology.

Proof. We start with the cyclic group $\mathfrak{C}_n$. If $n = 1$, then $N(\mathfrak{C}_1) = \mathrm{PGL}_2$ and (14) is the identity map, so we may assume that $n \geqslant 3$. Theorem 3.1(c) tells us that $N(\mathfrak{C}_n) = \mathfrak{D}_\infty = \mathbb{G}_m \rtimes \mu_2$. Note that the group law on $\mathfrak{D}_\infty$, which we will denote by $*$, is given by the twisted product

$$(a, s) * (b, t) = (ab^s, st).$$

The image of $\mathfrak{C}_n$ in $\mathfrak{D}_\infty$ is $\mu_n \times 1$, so there is a natural isomorphism

$$\begin{array}{ccc} (\mathbb{G}_m \rtimes \mu_2)/(\mu_n \times 1) = \mathfrak{D}_\infty/\mathfrak{C}_n & \longrightarrow & \mathfrak{D}_\infty = \mathbb{G}_m \rtimes \mu_2 \\ (a, t) & \longmapsto & (a^n, t). \end{array}$$

With this identification, (14) becomes the map

$$F_n\colon\ H^1(G_K, \mathfrak{D}_\infty) \longrightarrow H^1(G_K, \mathfrak{D}_\infty) \quad \text{induced by} \quad \begin{array}{c} \mathfrak{D}_\infty \longrightarrow \mathfrak{D}_\infty. \\ (a, t) \longmapsto (a^n, t) \end{array} \tag{16}$$

We need to prove that F_n is surjective when n is odd.

Let $C \in H^1(G_K, \mathfrak{D}_\infty)$ be a cohomology class, say represented by the cocycle

$$G_K \longrightarrow \mathfrak{D}_\infty, \qquad \sigma \longmapsto (A_\sigma, T_\sigma).$$

The cocycle condition says that

$$\begin{aligned} (A_{\sigma\tau}, T_{\sigma\tau}) &= (A_\sigma, T_\sigma) * (A_\tau, T_\tau)^\sigma = (A_\sigma, T_\sigma) * (A_\tau^\sigma, T_\tau) \\ &= (A_\sigma (A_\tau^\sigma)^{T_\sigma}, T_\sigma T_\tau), \end{aligned}$$

so we find that

$$T_{\sigma\tau} = T_\sigma T_\tau \quad \text{and} \quad A_{\sigma\tau} = A_\sigma (A_\tau^\sigma)^{T_\sigma} \quad \text{for all } \sigma, \tau \in G_K.$$

Notice that A is almost, but not quite, a G_K-to-$\mathbb{G}_m$ cocycle.

On the other hand, T: $G_K \to \mu_2$ is a homomorphism. We consider two cases. First, if $T_\sigma = 1$ for all $\sigma \in G_K$, then A: $G_K \to \mathbb{G}_m$ is an honest cocycle. Hilbert's theorem 90 then tells us that A is a coboundary, say $A = B^\sigma/B$ for some $B \in \overline{K}^*$. Hence C is represented by the cocycle

$$(A_\sigma, T_\sigma) = (B^\sigma/B, 1) = (B, 1)^\sigma * (B, 1)^{-1}.$$

Thus C is the trivial class in $H^1(G_K, \mathfrak{D}_\infty)$, so it can certainly be lifted in (16).

Second, suppose that T: $G_K \to \mu_2$ is surjective, and let L be the fixed field of the kernel of T. Writing

$$\mathfrak{D}_\infty(L) = \mathfrak{D}_\infty^{G_{L/K}} = L^* \rtimes \mu_2,$$

we consider the inflation–restriction sequence

$$0 \longrightarrow H^1(G_{L/K}, \mathfrak{D}_\infty(L)) \xrightarrow{\text{Inf}} H^1(G_K, \mathfrak{D}_\infty) \xrightarrow{\text{Res}} H^1(G_L, \mathfrak{D}_\infty).$$

(N.B. This is an exact sequence of pointed sets, not of groups.) The class $\text{Res}(C)$ is represented by the cocycle $\sigma \mapsto (A_\sigma, 1)$, so using the above argument with L in place of K, we see that $\text{Res}(C) = 0$. This means that we can write $C = \text{Inf}(c)$, where $c \in H^1(G_{L/K}, \mathfrak{D}_\infty(L))$ is represented by some cocycle

$$G_{L/K} \longrightarrow \mathfrak{D}_\infty(L), \qquad \sigma \longmapsto (a_\sigma, t_\sigma).$$

It thus suffices to show the surjectivity of the map

$$F_{n,L}\colon\ H^1(G_{L/K}, \mathfrak{D}_\infty(L)) \longrightarrow H^1(G_{L/K}, \mathfrak{D}_\infty(L)) \tag{17}$$

induced by the homomorphism

$$\mathfrak{D}_\infty(L) \longrightarrow \mathfrak{D}_\infty(L), \qquad (a, t) \longmapsto (a^n, t).$$

Let $G_{L/K} = \{1, \nu\}$. Then a $G_{L/K}$-to-$\mathfrak{D}_\infty(L)$ cocycle is uniquely determined by the image (x, u) of ν. There is only one cocycle condition, namely

$$(1, 1) = (x, u) * (x, u)^\nu = (x, u) * (x^\nu, u) = (x(x^u)^\nu, 1).$$

In other words, (x, u) defines a cocycle if and only if either

$$u = 1 \text{ and } \mathrm{N}_{L/K}(x) = 1 \quad \text{ or } \quad u = -1 \text{ and } x \in K^*.$$

But if $u = 1$ and $\mathrm{N}_{L/K}(x) = 1$, then Hilbert's theorem 90 tells us that $x = y^\nu/y$ for some $y \in L^*$, and so

$$(x, u) = (y^\nu/y, 1) = (y, 1)^\nu * (y, 1)^{-1}$$

is the trivial class. Thus the cocycles $(x, 1)$ with $\mathrm{N}_{L/K}(x) = 1$ all represent the trivial cohomology class in $H^1(G_{L/K}, \mathfrak{D}_\infty(L))$.

On the other hand, two cocycles $(x, -1)$ and $(x', -1)$ are cohomologous if and only if there is a (y, w) such that

$$\begin{aligned}(x', -1) &= (y, w)^\nu * (x, -1) * (y, w)^{-1} \\ &= (y^\nu x^w, -w) * (y^{-w}, w) = (y^\nu x^w y, -1).\end{aligned}$$

Thus $(x,-1)$ and $(x',-1)$ are cohomologous if and only if there is a $y \in L^*$ such that $x' = x^{\pm 1}\mathrm{N}_{L/K}(y)$. Summarizing our discussion, we have shown that there is a bijection

$$\frac{K^*/\mathrm{N}_{L/K}(L^*)}{(x=x^{-1})} \longrightarrow H^1(G_{L/K}, \mathfrak{D}_\infty(L)).$$
$$x \longmapsto \begin{pmatrix} 1 \mapsto (1,1) \\ \nu \mapsto (x,-1) \end{pmatrix}$$

With this identification, the map $F_{n,L}$ in (17) becomes

$$\frac{K^*/\mathrm{N}_{L/K}(L^*)}{(x=x^{-1})} \longrightarrow \frac{K^*/\mathrm{N}_{L/K}(L^*)}{(x=x^{-1})}, \quad x \longmapsto x^n.$$

The group $K^*/\mathrm{N}_{L/K}(L^*)$ is a group of exponent 2 and n is odd by assumption, so this last map is clearly surjective. This completes the proof of Theorem 3.2 in the case (i) that $A = \mathfrak{C}_n$ with n odd.

Next we consider the case (ii) that $A = \mathfrak{D}_{2n} = \mu_n \rtimes \mu_2$. Theorem 3.1(c) says that $N = \mathfrak{D}_{4n} = \mu_{2n} \rtimes \mu_2$ with the natural inclusion $\mathfrak{D}_{2n} \lhd \mathfrak{D}_{4n}$, and thus we have an isomorphism

$$\mathfrak{D}_{4n}/\mathfrak{D}_{2n} \xrightarrow{\sim} \mu_2, \qquad (\zeta,t) \longmapsto \zeta^n.$$

We thus need to show the surjectivity of the map

$$H^1(G_K, \mathfrak{D}_{4n}) \longrightarrow H^1(G_K, \mu_2) \quad \text{induced by} \quad \begin{array}{c} \mathfrak{D}_{4n} \longrightarrow \mu_2. \\ (\zeta,t) \longmapsto \zeta^n \end{array} \tag{18}$$

Hilbert's theorem 90 implies that every cocycle in $H^1(G_K,\mu_2)$ has the form $\sigma \mapsto \alpha^\sigma/\alpha$ for some $\alpha \in \overline{K}^*$ such that $a = \alpha^2 \in K$. Then the map

$$G_K \longrightarrow \mathfrak{D}_{4n}, \qquad \sigma \longmapsto (\alpha^\sigma/\alpha, 1)$$

is clearly a cocycle, so it represents an element of $H^1(G_K, \mathfrak{D}_{4n})$. Its image under the map (18) is represented by the cocycle

$$\sigma \longmapsto (\alpha^\sigma/\alpha)^n = (a^\sigma/a)^{(n-1)/2}(\alpha^\sigma/\alpha) = \alpha^\sigma/\alpha,$$

since n is odd and $a = \alpha^2 \in K$. Hence (18) is surjective, which completes the proof of Theorem 3.2 in the case (ii) that $A = \mathfrak{D}_n$ with n odd.

4. Rational maps with non-trivial stabilizers

In this section we will prove a number of preliminary results concerning dynamical systems with non-trivial stabilizers. These will be used in the next section to generalize Corollary 2.2 to arbitrary dynamical systems.

PROPOSITION 4.1. *Let $\xi \in \mathrm{M}_d$. Then the stabilizer $\mathcal{A}_\xi$ is a finite group.*

Proof. This result is well known, at least when $K \subset \mathbb{C}$. It appears, for example, as exercise 6.2.5 in [2]. We briefly sketch the proof. Let

$$\mathrm{Per}_n^*(\phi) = \{P \in \mathbb{P}^1(K^a)\colon\ \phi^n(P) = P \text{ and } \phi^i(P) \neq P \text{ for } 0 < i < n\}$$

be the primitive n-periodic points of ϕ. (Note we are taking all points defined over an algebraic closure K^a of K.) For any $g \in \mathrm{PGL}_2$ we have

$$\mathrm{Per}_n^*(\phi^g) = g^{-1}(\mathrm{Per}_n^*(\phi)),$$

so in particular, if $g \in \mathcal{A}_\phi$, then g permutes the points in $\mathrm{Per}_n^*(\phi)$.

It is not hard to prove that $\mathrm{Per}_n^*(\phi)$ is non-empty for infinitely many values of n. There is an elementary proof in [2, §6.1] in the case that $K \subset \mathbb{C}$, and the exact same proof works in general if one considers only points whose period is a prime q with $q \neq \mathrm{char}(K)$. (See also [11, Lemma 3.4].) We choose three values n_1, n_2, n_3 of n for which $\mathrm{Per}_n^*(\phi)$ is non-empty, and consider the set

$$W = \mathrm{Per}_{n_1}^*(\phi) \cup \mathrm{Per}_{n_2}^*(\phi) \cup \mathrm{Per}_{n_3}^*(\phi) = \{P_1, \ldots, P_r\}.$$

As explained above, each $g \in \mathcal{A}_\phi$ will permute the points in W, so g determines a permutation $\pi_g \in \mathfrak{S}_r$ according to the rule $f(P_i) = P_{\pi_g(i)}$. In this way we get a homomorphism $\pi\colon\ \mathcal{A}_\phi \to \mathfrak{S}_r$. Further, the fact that $r \geqslant 3$ implies that π is injective, since an element of PGL_2 is uniquely determined by its value at three distinct points. Hence $\mathcal{A}_\phi$ sits as a subgroup of $\mathfrak{S}_r$, so it is finite.

Next we show that the f_σ's attached to a given rational map ϕ lie in the normalizer of its stabilizer.

LEMMA 4.2. *Let $\xi \in \mathrm{M}_d(K)$ and choose a $\phi \in \xi$ whose stabilizer $\mathcal{A}_\phi$ is defined over K. For each $\sigma \in G_K$, write $\phi^\sigma = \phi^{f_\sigma}$ as usual.*

(a) $f_\sigma \in N(\mathcal{A}_\phi)$.

(b) *The map*

$$G_K \longrightarrow N(\mathcal{A}_\phi)/\mathcal{A}_\phi, \qquad \sigma \longmapsto f_\sigma \bmod \mathcal{A}_\phi,$$

is a well-defined 1-cocycle.

Proof. (a) For any $\sigma \in G_K$ we use (3) and the fact that $\mathcal{A}_\phi$ is defined over K to compute

$$\mathcal{A}_\phi = \mathcal{A}_\phi^\sigma = \mathcal{A}_{\phi^\sigma} = \mathcal{A}_{\phi^{f_\sigma}} = f_\sigma^{-1} \circ \mathcal{A}_\phi \circ f_\sigma.$$

Therefore $f_\sigma \in N(\mathcal{A}_\phi)$.

(b) Proposition 1.1 says that $f_\sigma f_\tau^\sigma f_{\sigma\tau}^{-1} \in \mathcal{A}_\phi$, and (a) says that $f : G_K \to N(\mathcal{A}_\phi)$, so f defines a 1-cocycle with values in the quotient group $N(\mathcal{A}_\phi)/\mathcal{A}_\phi$.

We next prove the following somewhat strange looking result which has a very useful corollary. The notation is taken from Theorem 3.1(b).

PROPOSITION 4.3. *Let $\xi \in \mathrm{M}_d$, and suppose that there is a rational map $\phi \in \xi$ with the following two properties:*

(i) $\mathfrak{C}_n = \langle \zeta_n z \rangle \subset \mathcal{A}_\phi$.

(ii) *There is a $\sigma \in G_K$ and an $f = b/z \in \mathrm{PGL}_2$ such that $\phi^\sigma = \phi^f$.*

Then

$$d \equiv \pm 1 \pmod{n}. \tag{19}$$

COROLLARY 4.4. *Let $\xi \in \mathrm{M}_d$ by a dynamical system, and if* $\mathrm{char}(K) = p > 0$, *assume that $\#\mathcal{A}_\xi$ is prime to p.*

(a) *If $d \equiv 0 \pmod{2}$, then the stabilizer of ξ is either*

$$\mathcal{A}_\xi = \mathfrak{C}_n \quad \text{or} \quad \mathcal{A}_\xi = \mathfrak{D}_{4n+2}.$$

(b) *If the dynamical system ξ is polynomial (i.e., ξ contains a polynomial map), then the stabilizer of ξ is either*

$$\mathcal{A}_\xi = \mathfrak{C}_n \quad \text{or} \quad \mathcal{A}_\xi = \mathfrak{D}_{2d-2}.$$

Further, the following three conditions are equivalent:

(i) $\mathcal{A}_\xi = \mathfrak{D}_{2d-2}$.

(ii) $z^d \in \xi$.

(iii) *Some (every) $\phi \in \xi$ has more than one exceptional point.*

Proof of Proposition 4.3. If $n = 1$ then (19) is trivial, so we assume that $n \geqslant 2$. The fact that $\zeta_n z \in \mathcal{A}_\phi$ means that $\zeta_n^{-1}\phi(\zeta_n z) = \phi(z)$, so the rational function $z^{-1}\phi(z)$ is invariant under the substitution $z \mapsto \zeta_n z$. Hence $z^{-1}\phi(z)$ is a function of z^n, say

$$\phi(z) = z\Phi(z^n) \quad \text{for some } \Phi(w) \in \overline{K}(w). \tag{20}$$

Note that (20) does not itself imply that $d \equiv 1 \pmod{n}$. For example, the rational function $z/(z^n + 1)$ has degree n.

However, (20) does give some information about the order of ϕ at $z = 0$ and at $z = \infty$. Thus

$$\begin{aligned} \mathrm{ord}_0(\phi) &= 1 + n\,\mathrm{ord}_0(\Phi) \equiv 1 \pmod{n}, & (21)\\ \mathrm{ord}_\infty(\phi) &= -1 + n\,\mathrm{ord}_\infty(\Phi) \equiv -1 \pmod{n}. & (22) \end{aligned}$$

The fact that $n \geqslant 2$ then implies that

$$\phi(0) = 0 \text{ or } \infty \quad \text{and} \quad \phi(\infty) = 0 \text{ or } \infty.$$

In other words, ϕ maps the set $\{0, \infty\}$ to itself.

Next we write out the given property $\phi^\sigma = \phi^f$ to obtain

$$\phi^\sigma(z)\phi(b/z) = b.$$

Putting $z = 0$ and using the fact that σ fixes 0 and ∞, we find that $\phi(0)\phi(\infty) = b$. This means that $\phi(0)$ and $\phi(\infty)$ cannot both be 0 and cannot both be ∞, so ϕ permutes the two elements in the set $\{0, \infty\}$. This leads to two cases, depending on whether ϕ fixes 0 and ∞ or switches them.

Suppose first that $\phi(0) = 0$ and $\phi(\infty) = \infty$. Then (21) and (22) tell us that $\mathrm{ord}_0(\Phi) \geqslant 0$ and $\mathrm{ord}_\infty(\Phi) \leqslant 0$, so Φ must have the form

$$\Phi(w) = \frac{aw^r + \cdots}{cw^s + \cdots + d} \quad \text{with } acd \neq 0 \text{ and } r \geqslant s.$$

Hence

$$d = \deg(\phi) = \deg(z\Phi(z^n)) = rn + 1 \equiv 1 \pmod{n}.$$

Similarly, suppose that $\phi(0) = \infty$ and $\phi(\infty) = 0$. Then (21) and (22) give $\mathrm{ord}_0(\Phi) < 0$ and $\mathrm{ord}_\infty(\Phi) > 0$, so Φ must have the form

$$\Phi(w) = \frac{aw^r + \cdots + b}{cw^s + \cdots + dw} \quad \text{with } abc \neq 0 \text{ and } s > r.$$

Then ϕ looks like

$$\phi(z) = z\Phi(z^n) = \frac{az^{nr} + \cdots + b}{cz^{ns-1} + \cdots + dz^{n-1}},$$

and now the fact that $ns - 1 \geqslant n(r+1) - 1 > nr$ implies that

$$d = \deg(\phi) = ns - 1 \equiv -1 \pmod{n}.$$

Proof of Corollary 4.4. (a) It is easy to see that each of the groups $\mathfrak{D}_{4n}$, $\mathfrak{A}_4$, $\mathfrak{S}_4$, and $\mathfrak{A}_5$ contains a copy of the four group $\mathfrak{D}_4$. Hence it suffices to show that if the stabilizer of $\xi \in \mathrm{M}_d$ contains $\mathfrak{D}_4$, then d must be odd.

So we make the assumption that $\mathfrak{D}_4 \subset \mathcal{A}_\xi$. Then Theorem 3.1 says that we can find a rational map $\phi \in \xi$ so that

$$\{\pm z, \pm 1/z\} \subset \mathcal{A}_\phi.$$

In particular, $\mathfrak{C}_2 = \{\pm z\} \subset \mathcal{A}_\phi$, and if we let $f(z) = 1/z$, then $\phi = \phi^f$. Thus we can apply Proposition 4.3 with $n = 2$ and $\sigma = 1$ to conclude that $d \equiv \pm 1 \pmod{2}$, which is the desired result.

(b) Take any $\phi \in \xi$, and let P be an exceptional point for ϕ. Then for any $f \in \mathrm{PGL}_2$, the point $f^{-1}(P)$ is an exceptional point for ϕ^f. In particular, if $f \in \mathcal{A}_\phi$, then $f^{-1}(P)$ is an exceptional point for ϕ. We consider two cases.

First, suppose that ϕ has only one exceptional point. Then $f(P) = P$ for all $f \in \mathcal{A}_\phi$. In other words, the maps in $\mathcal{A}_\phi$ have a common fixed point. Proposition 4.1 says that $\mathcal{A}_\phi$ is a finite group, and looking at the list of possibilities described in Theorem 3.1(b), we see that $\mathcal{A}_\phi$ must be a cyclic group $\mathfrak{C}_n$.

Next, suppose that ϕ has a second exceptional point P'. Let $g \in \mathrm{PGL}_2$ be a transformation with $g(0) = P$ and $g(\infty) = P'$. Then 0 and ∞ are exceptional points of ϕ^g, so ϕ^g must have the form $\phi = az^d$ for some $a \in \overline{K}^*$. Letting $h(z) = a^{-1/(d-1)}z$, we find that $\phi^{gh} = z^d \in \xi$, which proves that (iii) implies (ii). Next we note that any element of $\mathcal{A}_{z^d}$ must either fix or permute 0 and ∞, from which it is easy to see that

$$\mathcal{A}_{z^d} = \{\zeta z \,:\, \zeta \in \mu_{d-1}\} \cup \{\zeta/z \,:\, \zeta \in \mu_{d-1}\} = \mathfrak{D}_{2d-2}.$$

This shows that (ii) implies (i).

Finally, suppose that $\mathcal{A}_\xi = \mathfrak{D}_{2d-2}$. Theorem 3.1(b) says that we can find a $\phi \in \xi$ whose stabilizer $\mathcal{A}_\phi$ contains the maps $f(z) = \zeta z$ and $g(z) = 1/z$, where ζ is a primitive n^{th} root of unity. Then P, $f(P)$, and $g(P)$ are all exceptional points of ϕ. They cannot all be equal, since f and g have no common fixed points, so ϕ has at least two exceptional points. This proves that (i) implies (iii), which completes the proof of Corollary 4.4

In the case that a dynamical system $\xi \in \mathrm{M}_d(K)$ has trivial stabilizer, Theorem 2.1 and Corollary 2.2 gave powerful tools for proving that K is a field of definition for ξ. The following two results give similar, but weaker, tools in the case that $\mathcal{A}_\xi$ is non-trivial. Essentially, they say that Theorem 2.1 and Corollary 2.2 are still true provided that the f_σ's can be chosen to give a true cocycle, instead of a cocycle relative to $\mathcal{A}_\xi$. This will explain why our lifting result (Theorem 3.2) will be so useful.

PROPOSITION 4.5. *Let $\xi \in \mathrm{M}_d(K)$, let $\phi \in \xi$, and suppose that there is a map $f\colon G_K \to \mathrm{PGL}_2$ with the following two properties:*

$$\phi^\sigma = \phi^{f_\sigma} \quad \textit{and} \quad f_{\sigma\tau} = f_\sigma f_\tau^\sigma \ \textit{for all}\ \sigma,\tau \in G_K. \tag{23}$$

(N.B. f is required to be a true cocycle, not merely a cocycle modulo $\mathcal{A}_\phi$.) Let $c \in H^1(G_K, \mathrm{PGL}_2)$ be the associated cohomology class, and let X/K be the associated Brauer–Severi curve (Proposition 1.2).

(a) *There exists an isomorphism i: $\mathbb{P}^1 \to X_\xi$ defined over $\overline{K}$ and a rational map Φ: $X_\xi \to X_\xi$ defined over K so that the following diagram commutes:*

$$\begin{tikzcd} \mathbb{P}^1 \arrow[r, "\phi_{/\overline{K}}"] \arrow[d, "\wr"', "i_{/\overline{K}}"] & \mathbb{P}^1 \arrow[d, "\wr"', "i_{/\overline{K}}"] \\ X_\xi \arrow[r, "\Phi_{/K}"] & X_\xi \end{tikzcd} .$$

(b) *The following are equivalent:*
(i) *K is a field of definition for ξ.*
(ii) *$X(K) \neq \emptyset$.*
(iii) *$c = 1$.*

COROLLARY 4.6. *Let $\xi \in \mathrm{M}_d(K)$, and suppose that there is a $\phi \in \xi$, and a map $f\colon G_K \to \mathrm{PGL}_2$ satisfying the two conditions in* (23).

(a) *If $d \equiv 0 \pmod 2$, then K is a field of definition for ξ.*

(b) *If the dynamical system ξ is polynomial (i.e., ξ contains a polynomial map), then K is a field of definition for ξ.*

Proof. The proof of Proposition 4.5 follows, word-for-word, the proof of Theorem 2.1(b,c). Similarly, the proof of Corollary 4.6 is identical to the proof of Corollary 2.2

5. Field of moduli equals field of definition

In this section we will prove Corollary 2.2 without the assumption that the stabilizer be trivial. The proof will use all of the tools we have developed in the previous four sections.

THEOREM 5.1. *Let $\xi \in \mathrm{M}_d(K)$ be a dynamical system, and if* $\mathrm{char}(K) = p > 0$, *assume that $\#\mathcal{A}_\xi$ is prime to p.*

(a) *If $d \equiv 0 \pmod 2$, then K is a field of definition for ξ.*

(b) *If the dynamical system ξ is polynomial (i.e., ξ contains a polynomial map), then K is a field of definition for ξ.*

Proof. (a) Corollary 4.4(a) says that $\mathcal{A}_\xi$ is either cyclic or dihedral. Suppose first that $\mathcal{A}_\xi = \mathfrak{C}_n$. The case $n = 1$ is already covered by Corollary 2.2, so we may assume that $n \geqslant 2$. Then Theorem 3.1(b) tells us that we can find a map $\phi \in \xi$ with

$$\mathfrak{C}_n = \langle \zeta_n z \rangle = \mathcal{A}_\phi.$$

Further, Theorem 3.1(c) says that

$$N(\mathcal{A}_\phi) = \mathfrak{D}_\infty = \{az\colon\ a \in \overline{K}^*\} \cup \{b/z\colon\ b \in \overline{K}^*\}.$$

Writing $\phi^\sigma = \phi^{f_\sigma}$ as usual, Lemma 4.2 says that $f_\sigma \in N(\mathcal{A}_\phi)$ and that f induces a 1-cocycle with values in $N(\mathcal{A}_\phi)/\mathcal{A}_\phi$. We consider two subcases. First, suppose that every f_σ has the form $f_\sigma = a_\sigma z$. The a_σ's are well-defined modulo μ_n, so we get a well-defined 1-cocycle

$$G_K \longrightarrow \overline{K}^*/\mu_n, \qquad \sigma \longmapsto a_\sigma \pmod{\mu_n}.$$

But there is an isomorphism of Galois modules

$$\overline{K}^*/\mu_n \xrightarrow{\sim} \overline{K}^*, \qquad a \pmod{\mu_n} \longmapsto a^n,$$

and Hilbert's theorem 90 tells us that $H^1(G_K, \overline{K}^*/\mu_n) \cong H^1(G_K, \overline{K}^*) = 0$. Thus there is an $\alpha \in \overline{K}^*$ satisfying

$$a_\sigma \equiv \alpha^{-1}\alpha^\sigma \pmod{\mu_n} \quad \text{for all } \sigma \in G_K.$$

Setting $g = \alpha z$, we find that $g^{-1}g^{\sigma}f_{\sigma}^{-1} = (\alpha^{-1}\alpha^{\sigma}a_{\sigma}^{-1})z \in \mathcal{A}_{\phi}$. Now Proposition 1.1(d) tells us that K is a field of definition for ξ.

Second, suppose that there is some $\tau \in G_K$ such that $f_{\tau} = b_{\tau}/z$. We now have the situation that $\langle \zeta_n z\rangle = \mathcal{A}_{\phi}$ and $\phi^{\tau} = \phi^{f_{\tau}}$ with $f_{\tau} = b_{\tau}/z$. This is exactly the situation in which we can apply Proposition 4.3 to deduce that $d \equiv \pm 1 \pmod{n}$. Since we have assumed that the degree d of ξ is even, it follows that n is odd. This means we can use case (i) of our lifting result Theorem 3.2 to deduce that the map

$$H^1(G_K, N(\mathcal{A}_{\phi})) \longrightarrow H^1(G_K, N(\mathcal{A}_{\phi})/\mathcal{A}_{\phi}) \tag{24}$$

is surjective. Thus the map $f\colon G_K \to N(\mathcal{A}_{\phi})$, which a priori is only a "cocycle modulo $\mathcal{A}_{\phi}$," can be modified to yield a true cocycle. In other words, although the condition $\phi^{\sigma} = \phi^{f_{\sigma}}$ only determines the f_{σ}'s up to left multiplication by an element of $\mathcal{A}_{\phi}$, it is possible to choose the f_{σ}'s in such a way that they satisfy $f_{\sigma}f_{\tau}^{\sigma} = f_{\sigma\tau}$. Having successfully lifted f, it only remains to apply Corollary 4.6(a) to conclude that K is a field of definition for ξ. This completes the proof in the case that $\mathcal{A}_{\xi}$ is cyclic.

Next suppose that $\mathcal{A}_{\xi} = \mathfrak{D}_{2n}$. Corollary 4.4(a) and our assumption that d is even implies that n is odd, and then Theorem 3.2 tells us that the map (24) is surjective. So again we can lift f to be a true cocycle, and then another application of Corollary 4.6(a) tells us that K is a field of definition for ξ.

(b) Corollary 4.4(b) says that $\mathcal{A}_{\xi}$ is either $\mathfrak{C}_n$ or $\mathfrak{D}_n$. Further, if $\mathcal{A}_{\xi} = \mathfrak{D}_n$, then $z^d \in \xi$, so any field K will be a field of definition for ξ. It thus suffices to consider the case that $\mathcal{A}_{\xi} = \mathfrak{C}_n$. Further, we already dealt with the case $n = 1$ in Corollary 2.2(b), so we may assume that $n \geqslant 2$. Then Theorem 3.1 allows us to choose a $\phi \in \xi$ such that

$$\mathcal{A}_{\phi} = \langle \zeta_n z\rangle = \mathfrak{C}_n \quad \text{and} \quad N(\mathcal{A}_{\phi}) = \{az\} \cup \{b/z\} = \mathfrak{D}_{\infty}.$$

Corollary 4.4(b) also tells us that ϕ has a unique exceptional point, and since $\mathcal{A}_{\phi}$ sends exceptional points to exceptional points, that unique exceptional point must be $z = \infty$.

For any $\sigma \in G_K$ we have

$$\begin{aligned}\{\infty\} &= \{\infty\}^{\sigma} = (\phi^{-1}(\infty))^{\sigma} = (\phi^{\sigma})^{-1}(\infty) = (\phi^{f_{\sigma}})^{-1}(\infty)\\ &= f_{\sigma} \circ \phi^{-1} \circ f_{\sigma}^{-1}(\infty).\end{aligned}$$

Thus $f_{\sigma}^{-1}(\infty)$ is an exceptional point of ϕ, which means we must have $f_{\sigma}^{-1}(\infty) = \infty$. In other words, every f_{σ} must have the form $f_{\sigma} = a_{\sigma}z$; none of the f_{σ}'s can have the form b/z. Now just as in the proof of (a), the a_{σ}'s give a cocycle $G_K \to \overline{K}^*/\mu_n$ which is a coboundary by Hilbert's theorem 90, say $\alpha^{-1}\alpha^{\sigma}a_{\sigma}^{-1} \in \mu_n$. Then $g = \alpha z$ gives $g^{-1}g^{\sigma}f_{\sigma}^{-1} \in \mathcal{A}_{\phi}$, and we use Proposition 1.1(d) to conclude that K is a field of definition for ξ.

6. Field of moduli not equal to field of definition

In the last section we showed that the field of moduli of a dynamical system of even degree is always a field of definition. We are now going to construct a large class of examples of odd degree whose field of moduli is not a field of definition. Recall from Theorem 2.1 that for each dynamical system $\xi \in \mathrm{M}_d(K)$ with trivial stabilizer, we constructed a cohomology class $c_\xi \in H^1(G_K, \mathrm{PGL}_2)$ whose triviality is equivalent to the assertion that K is a field of definition for ξ. In other words, if we let

$$\mathrm{Rat}_d(K,1) = \{\phi \in \mathrm{Rat}_d(K)\colon\ \mathcal{A}_\phi = 1\}$$

and

$$\mathrm{M}_d(K,1) = \{\xi \in \mathrm{M}_d(K)\colon\ \mathcal{A}_\xi = 1\},$$

then we have an exact sequence of sets

$$\begin{array}{ccccc} \mathrm{Rat}_d(K,1) & \longrightarrow & \mathrm{M}_d(K,1) & \longrightarrow & H^1(G_K,\mathrm{PGL}_2). \\ & & \xi & \longmapsto & c_\xi \end{array}$$

Thus the image of $\mathrm{M}_d(K,1)$ in $H^1(G_K,\mathrm{PGL}_2)$ measures the extent to which there exist dynamical systems whose field of moduli is not a field of definition.

THEOREM 6.1. *Let $d \equiv 1 \pmod 2$, and let K be a local or a global field. Then the map*

$$\mathrm{M}_d(K,1) \longrightarrow H^1(G_K,\mathrm{PGL}_2), \qquad \xi \longmapsto c_\xi, \tag{25}$$

is surjective. In particular, there exist dynamical systems $\xi \in \mathrm{M}_d(K)$ with trivial stabilizer such that the field of moduli of ξ is not a field of definition.

Proof. The second statement follows from the surjectivity of (25), the surjectivity of the connecting map from $H^1(G_K,\mathrm{PGL}_2)$ to $\mathrm{Br}(K)[2]$ (Theorem 1.4(c)), and the fact that $\mathrm{Br}(K)[2] \neq 0$ for local and global fields. More precisely, for a local field $\mathrm{Br}(K)[2] = \mathbb{Z}/2\mathbb{Z}$, see [18, Chapter XIII, Proposition 6]; and for a global field $\mathrm{Br}(K)[2]$ is a countable direct sum of copies of $\mathbb{Z}/2\mathbb{Z}$, see [1, Chapter VII].

We will prove the surjectivity of (25) by explicitly constructing, for each element of $H^1(G_K,\mathrm{PGL}_2)$, a family of rational maps of degree d whose corresponding cocycle is the given cohomology class. All of this, and considerably more, is contained in the following proposition and corollary.

PROPOSITION 6.2. *Let $d \equiv 1 \pmod 2$, and let K be a local or a global field.*

(a) *Let L/K be a quadratic extension, say with $G_{L/K} = \{1,\tau\}$, let $b \in K^*$, let $\gamma_0,\dots,\gamma_d \in L$, and let ξ be the dynamical system containing the map*

$$\phi(z) = b^{(d+1)/2} \sum_{j=0}^{d} \gamma_{d-j}^{\tau}(z/b)^j \Big/ \sum_{j=0}^{d} \gamma_j z^j. \tag{26}$$

Suppose further that $\mathcal{A}_\xi = 1$. *Then*

$$c_\xi = [b, L/K] \quad \text{in } H^1(G_K, \mathrm{PGL}_2),$$

where c_ξ *is the cohomology class associated to* ξ *in Theorem* 2.1 *and* $[b, L/K]$ *is the cocycle described in Theorem* 1.4.

(b) *Conversely, let* $\xi \in \mathrm{M}_d(K, 1)$ *be a dynamical system whose associated cohomology class* c_ξ *is non-trivial. Then there exists an* L/K, *a* $b \in K^*$, *and elements* $\gamma_0, \ldots, \gamma_d \in L$ *as in* (a) *so that the map* $\phi(z)$ *defined by* (26) *is in* ξ.

In order to apply Proposition 6.2(a), we need to find maps (26) which have trivial stabilizer. It's not hard to produce many examples of such maps, as in the following result.

COROLLARY 6.3. *Let* $d \equiv 1 \pmod 2$, *let* K *be a local or a global field, let* L/K *be a quadratic extension, say with* $G_{L/K} = \{1, \tau\}$, *let* $b \in K^*$, *and let* $\gamma \in L^*$. *Suppose that these quantities satisfy the following three conditions:*

$$b \notin \mathrm{N}_{L/K}(L^*), \qquad \mathrm{N}_{L/K}(\gamma) \neq b^d, \quad \text{and} \quad (\gamma/\gamma^\tau)^{d-1} \neq 1. \tag{27}$$

Then the dynamical system ξ_γ *containing the rational map*

$$\phi_\gamma(z) = b^{(d+1)/2}\left(\frac{z^d + \gamma^\tau}{\gamma z^d + b^d}\right)$$

satisfies

$$\mathcal{A}_{\xi_\gamma} = 1 \quad \text{and} \quad c_{\xi_\gamma} = [b, L/K]. \tag{28}$$

In particular, for any quadratic extension L/K *and any element* $b \in K^*$ *with* $b \notin \mathrm{N}_{L/K}(L^*)$, *there are infinitely many* $\gamma \in L^*$ *such that the field of moduli of* ξ_γ *is contained in* K, *but* K *is not a field of definition for* ξ_γ.

EXAMPLE. We can use Proposition 6.2 to construct many examples of dynamical systems whose field of moduli is not a field of definition, in addition to the examples given in Corollary 6.3. An interesting example arises by taking $b = -1$ and $\gamma_j = (1+i)^{d+1}\binom{d}{j}$ in (26). Then $(1+i)^\tau = -i(1+i)$, so after a little algebra the rational map (26) becomes

$$\phi(z) = i\left(\frac{z-1}{z+1}\right)^d.$$

We will leave it to the reader to prove that if d is odd, then $\mathcal{A}_\phi = 1$. (The proof is very similar to the proof of Corollary 6.3.) So for odd values of d, the map $\phi(z)$ has field of moduli $\mathbb{Q}$, but every field of definition has degree at least 2.

More precisely, Proposition 6.2, Theorem 1.4, and Theorem 2.1, imply that a quadratic extension $K/\mathbb{Q}$ is a field of definition for this ϕ if and only if

$-1 \in \mathrm{N}_{K(i)/K}(K(i)^*)$. For example, the field $K = \mathbb{Q}(\sqrt{-2})$ is a field of definition for ϕ, since

$$b = -1 = \mathrm{N}_{K(i)/K}(\sqrt{-2} + i).$$

We can also see this directly by conjugating ϕ by the map

$$f = \frac{z + \left(\sqrt{-2} + i\right)}{-\left(\sqrt{-2} + i\right) z + 1}.$$

A rather messy computation then shows that $\phi^f \in \mathbb{Q}(\sqrt{-2})(z)$. It is possible to give an explicit (but complicated) formula for ϕ^f which displays it as a rational map with coefficients in $\mathbb{Q}(\sqrt{-2})$. We will be content to give the result for $d = 3$, in which case one can check that

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

Proof of Proposition 6.2. (a) Let $\phi(z)$ be defined by (26) and let $f(z) = b/z$. Then $\phi^\tau = \phi^f$ by a trivial computation, so the cohomology class c_ξ obtained from ϕ is precisely $[b, L/K]$.

(b) Theorem 1.4 says that the non-trivial cohomology class c_ξ is represented by a cocycle $[b, L/K]$ for some quadratic extension L/K and some element $b \in K^*$ with $b \notin N_{L/K}(L^*)$. Then the restriction $\mathrm{Res}_{L/K}(c_\xi) \in H^1(G_L, \mathrm{PGL}_2)$ is clearly trivial, so Theorem 2.1(c) tells us that L is a field of definition for ξ. More precisely, we can find a rational map $\phi \in \xi \cap \mathrm{Rat}_d(L)$ whose associated cocycle is $[b, L/K]$. In other words, if we let $f(z) = b/z$ as before, then $\phi^\tau = \phi^f$.

We write $\phi = \sum \alpha_j z^j / \sum \beta_j z^j$ as a rational function with coefficients in L. The condition $\phi^\tau = \phi^f$ becomes

$$\sum \alpha_j^\tau z^j \Big/ \sum \beta_j^\tau z^j = \sum \beta_{d-j} b^{d-j+1} z^j \Big/ \sum \alpha_{d-j} b^{d-j} z^j,$$

so we find that there exists a $\lambda \in L^*$ such that

$$\alpha_j^\tau = \lambda \beta_{d-j} b^{d-j+1} \quad \text{and} \quad \beta_j^\tau = \lambda \alpha_{d-j} b^{d-j} \quad \text{for all } 0 \leqslant j \leqslant d.$$

Applying τ to the first formula and then using the second yields

$$\alpha_j = \lambda^\tau \beta_{d-j}^\tau b^{d-j+1} = \lambda^\tau (\lambda \alpha_j b^j) b^{d-j+1} = \lambda\lambda^\tau b^{d+1} \alpha_j. \tag{29}$$

Certainly the α_j's cannot all equal zero, so we conclude that $\lambda\lambda^\tau b^{d+1} = 1$.

The fact that d is odd means we can write this last equality as

$$N_{L/K}(\lambda b^{(d+1)/2}) = (\lambda b^{(d+1)/2})(\lambda b^{(d+1)/2})^\tau = \lambda\lambda^\tau b^{d+1} = 1.$$

Now Hilbert's theorem 90 tells us that there is a $\nu \in L^*$ such that $\lambda b^{(d+1)/2} = \nu/\nu^\tau$. Substituting this into the left-hand equality of (29) gives

$$\alpha_j = \frac{\nu^\tau}{\nu} b^{-(d+1)/2} \beta_{d-j}^\tau b^{d-j+1} = \frac{\nu^\tau}{\nu} b^{(d+1)/2-j} \beta_{d-j}^\tau.$$

So if we set $\gamma_j = \nu\beta_j$, then we have

$$\alpha_j = \nu^{-1} b^{(d+1)/2-j} \gamma_{d-j}^\tau \quad \text{and} \quad \beta_j = \nu^{-1}\gamma_j.$$

Substituting this into the formula for ϕ, canceling ν^{-1} from numerator and denominator, and doing a little algebra, we find that ϕ has the desired form (26).

Proof of Corollary 6.3. The map ϕ_γ is a particular case of the map (26), so once we prove that ϕ_γ has degree d and trivial stabilizer, the second statement in (28) will follow from Proposition 6.2. Further, the fact that K is not a field of definition for ξ_γ will then follow from Theorem 1.4(b), Theorem 2.1(c), and our assumption (27) that $b \notin \mathrm{N}_{L/K}(L^*)$.

The assumption $\mathrm{N}_{L/K}(\gamma) = \gamma\gamma^\tau \neq b^d$ from (27) implies that the polynomials $z^d + \gamma^\tau$ and $\gamma z^d + b^d$ do not have a common root, which shows that ϕ_γ has degree d. Next we observe that 0 and ∞ satisfy

$$\phi^{-1}(\phi(\infty)) = \{\infty\} \quad \text{and} \quad \phi^{-1}(\phi(0)) = \{0\},$$

and that these are the only two points in $\mathbb{P}^1$ with this property. It follows that any $g \in \mathcal{A}_{\phi_\gamma}$ must either fix or permute 0 and ∞, which leads to the usual two cases.

First, if g fixes 0 and ∞, then $g(z) = az$. Evaluating the identity

$$\phi(z) = \phi^g(z) = a^{-1}\phi(az)$$

at $z = \infty$ gives $\phi(\infty) = a^{-1}\phi(\infty)$. This implies that $a = 1$, since $\phi(\infty) = b^{(d+1)/2}/\gamma \neq 0$.

Next, if g switches 0 and ∞, then $g(z) = a/z$. This gives the identity $\phi(z) = \phi^g(z) = a/\phi(a/z)$, so $\phi(z)\phi(a/z) = a$. Multiplying this out, we find that

$$(\gamma^\tau b - a\gamma)b^d z^{2d} + \left((\gamma^\tau)^2 b^{d+1} + a^d b^{d+1} - a^{d+1}\gamma^2 - ab^{2d}\right)z^d$$
$$+(\gamma^\tau b - a\gamma)a^d b^d = 0.$$

This identity holds for all z, so all three coefficients must vanish. The first and third coefficients tell us that $a = (\gamma^\tau/\gamma)b$, and if we substitute this into the second coefficient, we find after some algebra that

$$\begin{aligned} 0 &= \gamma^{\tau 2} b^{d+1} + (\gamma^\tau/\gamma)^d b^{2d+1} - \gamma^{\tau d+1}\gamma^{-d+1} b^{d+1} - (\gamma^\tau/\gamma) b^{2d+1} \\ &= b^{d+1}\gamma^{-d}\gamma^\tau (b^d - \gamma\gamma^\tau)\left((\gamma^\tau)^{d-1} - \gamma^{d-1}\right). \end{aligned}$$

This contradicts the last two assumptions in (27). Therefore ϕ_γ cannot be stabilized by a map of the form a/z, which concludes the proof that $\mathcal{A}_{\phi_\gamma} = 1$.

Next we observe that since K is a local or global field, the norm map $\mathrm{N}_{L/K}\colon L^* \to K^*$ is not surjective, so there are lots of choices for b. It remains to show that there are infinitely many $\gamma \in L^*$ satisfying the three conditions in (27). Write $L = K(\sqrt{D})$ with $D \in K$, and set $\gamma = x + \sqrt{D}$ for some $x \in K$. We want to choose x so that $N_{L/K}(\gamma) \neq b^d$ and $(\gamma/\gamma^\sigma)^{d-1} \neq 1$. In order to satisfy these two conditions, we merely need to choose x so that

$$x^2 - D \neq b^d \quad \text{and} \quad (x + \sqrt{D})^{d-1} \neq (x - \sqrt{D})^{d-1}.$$

As long as $d \geqslant 2$, these are non-trivial polynomial inequalities, so the fact that K has infinitely many elements allows us to find infinitely many x's.

7. Non-trivial stabilizers and twists

Let $\xi \in \mathrm{M}_d$ be a dynamical system, and suppose that $\phi, \phi' \in \xi$ are rational maps defined over K. Then ϕ and ϕ' are linearly conjugate, which means that $\phi' = \phi^f$ for some $f \in \mathrm{PGL}_2(\overline{K})$. However, the arithmetic properties of ϕ and ϕ' as applied to $\mathbb{P}^n(K)$ will not be equivalent unless the automorphism f is defined over K. To see that this is not a moot question, consider the maps

$$\phi_a(z) = \frac{z}{1 + az^2} \in \mathrm{Rat}_2(K) \quad \text{for } a \in K^*.$$

All of the ϕ_a's are $\mathrm{PGL}_2(\overline{K})$-conjugate, since if we let $f(z) = \sqrt{a}\,z$, then $\phi_a = \phi_1^f$. But ϕ_a is $\mathrm{PGL}_2(K)$-conjugate to ϕ_1 if and only if a is a square in K. This prompts the following definition.

DEFINITION 7.1. Let $\phi \in \mathrm{Rat}_d(K)$ be a rational map defined over K. The set of *K-twists of ϕ* is the set

$$\mathrm{Twist}(\phi/K) = \frac{\{\psi \in [\phi] \colon \psi \text{ is defined over } K\}}{\mathrm{PGL}_2(K)\text{-conjugacy}}.$$

The next result gives the usual sort of cohomological description of such twists. Notice in particular that if $\mathcal{A}_\phi = 1$, then ϕ has no non-trivial twists.

PROPOSITION 7.2. *Let $\phi \in \mathrm{Rat}_d(K)$ be a rational map defined over K. Then there is a natural inclusion*

$$\mathrm{Twist}(\phi/K) \hookrightarrow H^1(G_K, \mathcal{A}_\phi) \tag{30}$$

defined as follows: Let $\psi \in [\phi]$ be defined over K, and write $\phi = \psi^f$ for some $f \in \mathrm{PGL}_2(\overline{K})$. Then ψ is sent to the cohomology class associated to the cocycle $\sigma \mapsto f^{-1}f^\sigma$.

The image of (30) *is precisely the kernel of the map*

$H^1(G_K, \mathcal{A}_\phi) \to H^1(G_K, \mathrm{PGL}_2)$ *induced by the inclusion* $\mathcal{A}_\phi \hookrightarrow \mathrm{PGL}_2$.

Proof. Since ψ and ϕ are defined over K, we have

$$\phi = \phi^\sigma = (\psi^f)^\sigma = (\psi^\sigma)^{f^\sigma} = \psi^{f^\sigma} = \phi^{f^{-1}f^\sigma},$$

so $f^{-1}f^\sigma \in \mathcal{A}_\phi$. One easily checks that the map $\sigma \mapsto f^{-1}f^\sigma$ is a cocycle, so we get a well-defined cohomology class in $H^1(G_K, \mathcal{A}_\phi)$.

Next suppose that ψ_1 and ψ_2 give the same cohomology class. Writing $\phi = \psi_i^{f_i}$, this means that there is a $g \in \mathcal{A}_\phi$ such that

$$f_1^{-1}f_1^\sigma = g^{-1}f_2^{-1}f_2^\sigma g^\sigma \quad \text{for all } \sigma \in G_K.$$

Thus $f_2gf_1^{-1} = (f_2gf_1^{-1})^\sigma$, so $f_2gf_1^{-1} \in \mathrm{PGL}_2(K)$. Further,

$$\psi_1 = \phi^{f_1^{-1}} = \phi^{gf_1^{-1}} = (\phi^{f_2^{-1}})^{f_2gf_1^{-1}} = \psi_2^{f_2gf_1^{-1}},$$

which shows that ψ_1 and ψ_2 are $\mathrm{PGL}_2(K)$-conjugate. This proves that the map (30) is injective. Further, its image is clearly contained in the kernel of the map $H^1(G_K, \mathcal{A}_\phi) \to H^1(G_K, \mathrm{PGL}_2)$, since $\sigma \mapsto f^{-1}f^\sigma$ is a coboundary for PGL_2.

Finally, let c: $G_K \to \mathcal{A}_\phi$ be a cocycle representing a cohomology class in $H^1(G_K, \mathcal{A}_\phi)$ whose image in $H^1(G_K, \mathrm{PGL}_2)$ is trivial. This means that we can find an $f \in \mathrm{PGL}_2(\overline{K})$ such that $c_\sigma = f^{-1}f^\sigma$. We define $\psi \in [\phi]$ by $\psi = \phi^{f^{-1}}$. Using the fact that ϕ is defined over K and that c_σ fixes ϕ, we compute

$$\psi^\sigma = \left(\phi^{f^{-1}}\right)^\sigma = \phi^{(f^{-1})^\sigma} = \phi^{c_\sigma^{-1}f^{-1}} = \phi^{f^{-1}} = \psi,$$

so ψ is defined over K. And it is clear from the definitions that (30) sends ψ to the cohomology class of the cocycle $\sigma \mapsto f^{-1}f^\sigma = c_\sigma$, so we have proven that the image of (30) equals the kernel of $H^1(G_K, \mathcal{A}_\phi) \to H^1(G_K, \mathrm{PGL}_2)$. This completes the proof of Proposition 7.1.

In order to give some examples of interesting twists, we need to find rational maps with non-trivial stabilizer groups.

PROPOSITION 7.3. *Let* $\xi \in \mathrm{M}_d$ *be a dynamical system.*

(a) $\mathfrak{C}_n \subset \mathcal{A}_\xi$ *for some* $n \geqslant 2$ *if and only if there is a rational map* $\psi \in \overline{K}(z)$ *such that* $z\psi(z^n) \in \xi$.

(b) $\mathfrak{D}_{2n} \subset \mathcal{A}_\xi$ *for some* $n \geqslant 2$ *if and only if there is a rational map* $\lambda \in \overline{K}(z)$ *such that*

$$z\frac{(z^n+1)\lambda(z^n+z^{-n}) - (z^n-1)}{(z^n+1)\lambda(z^n+z^{-n}) + (z^n-1)} \in \xi.$$

Proof. (a) Let ζ be a primitive nth root of unity. Theorem 3.1 tells us that there is a rational map $\phi(z) \in \xi$ whose stabilizer contains the map ζz. In other words, $\phi(z) = \zeta^{-1}\phi(\zeta z)$. This means that the function $z^{-1}\phi(z)$ is invariant under the substitution $z \to \zeta z$, so this function is in $\overline{K}(z^n)$, say $z^{-1}\phi(z) = \psi(z^n)$. Hence $z\psi(z^n) = \phi(z) \in \xi$.

(b) In this case Theorem 3.1 tells us that there is a rational map $\phi(z) \in \xi$ whose stabilizer contains ζz and z^{-1}. The argument in (a) shows that ϕ must have the form $\phi(z) = z\psi(z^n)$ for some $\psi(w) \in \overline{K}(w)$. Then the fact that $z^{-1} \in \mathcal{A}_\phi$ implies that $\psi(w)\psi(w^{-1}) = 1$. Consider the function

$$\frac{w-1}{w+1} \cdot \frac{\psi(w)+1}{\psi(w)-1}.$$

It is invariant under the substitution $w \to w^{-1}$, so it must be a polynomial in $w + w^{-1}$, say equal to $\lambda(w + w^{-1})$. Solving for ψ gives

$$\psi(w) = \frac{(w+1)\lambda(w+w^{-1}) - (w-1)}{(w+1)\lambda(w+w^{-1}) + (w-1)},$$

and then using $\phi(z) = z\psi(z^n)$ gives the desired result.

EXAMPLE. Let $\phi(z) = z\psi(z^n) \in K(z)$ be a rational map whose stabilizer contains the cyclic group $\mathfrak{C}_n = \langle \zeta z \rangle$ as described in Proposition 7.2. Then

$$H^1(G_K, \mathcal{A}_\phi) = H^1(G_K, \mathfrak{C}_n) \cong H^1(G_K, \mu_n) \cong K^*/K^{*n}.$$

For any element $a \in K^*$, we can produce a twist of ϕ by setting $\alpha = a^{1/n}$ and conjugating ϕ by the map $f(z) = \alpha z$. This is the right map to use because if $\sigma \in G_K$ satisfies $\alpha^\sigma = \zeta\alpha$, then $f^{-1}f^\sigma(z) = \zeta z$. The corresponding twist is

$$\phi^f(z) = \alpha^{-1}\phi(\alpha z) = \alpha^{-1}(\alpha z\psi(\alpha^n z^n)) = z\psi(az^n).$$

In this way we get a map

$$K^*/K^{*n} \hookrightarrow \text{Twist}(z\psi(z^n)/K), \qquad a \longmapsto z\psi(az^n).$$

EXAMPLE. In a similar way one can write down twists for rational maps with other stabilizer groups. In general, this will get quite complicated, so we will be content to analyze the map $\phi(z) = z^{-2}$ obtained by setting $n = 3$ and $\lambda(z) = 1$ in Proposition 7.2(b). Then $\mathcal{A}_\phi = \langle \zeta z, z^{-1} \rangle$, where ζ is a primitive cube root of unity. Notice that the stabilizer $\mathcal{A}_\phi = \mathfrak{D}_6$ is the symmetry group of a triangle, which is isomorphic to the symmetric group $\mathfrak{S}_3$ on three letters.

It turns out to be easier to describe the twists of ϕ if we move its fixed points from $1, \zeta, \zeta^2$ to $0, 1, \infty$. So we conjugate ϕ by the map $(\zeta z + 1)/(z + \zeta)$, which after some calculation gives a new ϕ, namely

$$\phi(z) = \frac{z^2 - 2z}{-2z + 1} \quad \text{with} \quad \mathcal{A}_\phi = \left\{ z, \frac{1}{z}, \frac{z-1}{z}, \frac{1}{1-z}, \frac{z}{z-1}, 1 - z \right\}.$$

Notice that each map in $\mathcal{A}_\phi$ is now defined over K, so

$$H^1(G_K, \mathcal{A}_\phi) = H^1(G_K, \mathfrak{S}_3) = \operatorname{Hom}(G_K, \mathfrak{S}_3).$$

Proposition 7.1 says that the twists of ϕ are classified by the kernel of the map $H^1(G_K, \mathcal{A}_\phi) \to H^1(G_K, \mathrm{PGL}_2)$. Let c: $G_K \longrightarrow \mathfrak{S}_3$ be a homomorphism whose image has order 3 or 6. We are going to construct the twist of ϕ corresponding to c.

Let L be the fixed field of the kernel of c, and let

$$F(X) = X^3 - pX - q = (X - \alpha_0)(X - \alpha_1)(X - \alpha_\infty)$$

be an irreducible polynomial in $K[X]$ whose splitting field is L. We have used the set $\operatorname{Fix}(\phi) = \{0, 1, \infty\}$ to label the roots of ϕ so that

$$\alpha_t^\sigma = \alpha_{c_\sigma(t)} \qquad \text{for all } \sigma \in G_K \text{ and } t \in \{0, 1, \infty\}.$$

Define a linear fractional transformation $f \in \mathrm{PGL}_2$ by

$$f(z) = \frac{\alpha_\infty(\alpha_1 - \alpha_0)z - \alpha_0(\alpha_1 - \alpha_\infty)}{(\alpha_1 - \alpha_0)z - (\alpha_1 - \alpha_\infty)},$$

so

$$f^{-1}(z) = \frac{(\alpha_1 - \alpha_\infty)(z - \alpha_0)}{(\alpha_1 - \alpha_0)(z - \alpha_\infty)}.$$

This map f satisfies

$$f(0) = \alpha_0, \quad f(1) = \alpha_1, \quad f(\infty) = \alpha_\infty.$$

We claim that

$$f^{-1} \circ f^\sigma(z) = c_\sigma(z) \quad \text{for all } \sigma \in G_K.$$

To verify this, we let $t \in \{0, 1, \infty\}$ and compute

$$\begin{aligned}
f^{-1} \circ f^\sigma(t) &= f^{-1}(f(t)^\sigma) && \text{since } t^\sigma = t, \\
&= f^{-1}(\alpha_t^\sigma) && \text{since } f(t) = \alpha_t, \\
&= f^{-1}(\alpha_{c_\sigma(t)}) && \text{from the labeling of the } \alpha\text{'s}, \\
&= c_\sigma(t) && \text{by definition of } f.
\end{aligned}$$

This proves that $f^{-1} \circ f^\sigma$ and c_σ agree on the set $\{0, 1, \infty\}$. But an element of PGL_2 is determined by its values at three points, which completes the verification that $f^{-1} \circ f^\sigma = c_\sigma$.

It is now a simple (but tedious) matter to compute the twist

$$\begin{aligned}
\phi_c &= \phi^{f^{-1}} = f \circ \phi \circ f^{-1} \\
&= \frac{(\alpha_0 + \alpha_1 + \alpha_\infty)z^2 - 2(\alpha_0\alpha_1 + \alpha_0\alpha_\infty + \alpha_1\alpha_\infty)z + 3\alpha_0\alpha_1\alpha_\infty}{3z^2 - 2(\alpha_0 + \alpha_1 + \alpha_\infty)z + (\alpha_0\alpha_1 + \alpha_0\alpha_\infty + \alpha_1\alpha_\infty)} \\
&= \frac{2pz - 3q}{3z^2 - p}.
\end{aligned}$$

This is the twist of $\phi(z) = (z^2 - 2z)/(-2z + 1)$ by the splitting field L of the irreducible polynomial $X^3 - pX - q \in K[X]$. Proposition 7.1 tells us that two twists will be $\mathrm{PGL}_2(K)$-equivalent if and only if their cocycles are cohomologous. In our case, the cocycles are homomorphisms, so ϕ_c and $\phi_{c'}$ will be equivalent if and only if their associated fields L and L' are the same.

Remark. The twists of the map $\phi(z) = (z^2 - 2z)/(-2z + 1)$ considered in the last example have an interesting property. Continuing with the notation of that example, let

$$\begin{aligned} \phi(z) &= \frac{z^2 - 2z}{-2z + 1}, \qquad f^{-1}(z) = \frac{(\alpha_1 - \alpha_\infty)(z - \alpha_0)}{(\alpha_1 - \alpha_0)(z - \alpha_\infty)}, \\ \phi_c(z) &= \phi^{f^{-1}} = \frac{2pz + q}{3z^2 - p}, \\ F(X) &= X^3 - pX - q = (X - \alpha_0)(X - \alpha_1)(X - \alpha_\infty). \end{aligned}$$

Then

$$\phi_c(z) - z = \frac{-3F(z)}{3z^2 - p},$$

which shows that $\mathrm{Fix}(\phi_c) = \{\alpha_0, \alpha_1, \alpha_\infty\}$. Further,

$$\mathcal{A}_{\phi_c} = f \circ \mathcal{A}_\phi \circ f^{-1}$$

consists of the six elements of PGL_2 which permute the set $\{\alpha_0, \alpha_1, \alpha_\infty\}$. Thus the map ϕ_c is defined over K, but the non-trivial elements in its stabilizer group are only defined over $K(\alpha_0, \alpha_1, \alpha_\infty) = L$. This is similar to the situation that arises for elliptic curves, where an elliptic curve may be defined over K but have endomorphisms which are only defined over a quadratic extension of K.

Acknowledgements

I would like to thank Dick Gross, Paul Lockhart, Barry Mazur, Mike Rosen and the referee for numerous helpful suggestions which greatly improved the scope of this paper. I would also like to thank IHES, Université Paris 7, Boston University, and Harvard University for their hospitality during the period when some of this research was completed.

References

1. Artin, E. and Tate, J.: *Class Field Theory*, Benjamin New York, 1967.
2. Beardon, A.: *Iteration of Rational Functions*, Graduate Texts in Math. 132, Springer-Verlag, New York, 1991.
3. Ben-Menahem, S.: *p-adic iterations*, TAUP-1627-88 preprint, March 1, 1988.

4. Call, G. and Silverman, J. H.: Canonical heights on varieties with morphisms, *Compositio Math.* **89** (1993), 163–205.
5. Couveignes, J.-M.: Calcul et rationalité de fonctions de Belyi en genre 0, *Fourier Annales* (to appear).
6. Denis, L.: Arithmétique et automorphismes affine, preprint, November 1993.
7. Devaney, R.: *An Introduction to Chaotic Dynamical Systems*, 2nd ed., Addison-Wesley, Redwood City, CA, 1989.
8. Hartshorne, R.: *Algebraic Geometry*, Graduate Texts in Math. 52, Springer-Verlag, New York, 1978.
9. Lang, S.: *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.
10. Morton, P.: Arithmetic properties of periodic points of quadratic maps, *Acat Arith.* **LXII** (1992), 343–372.
11. Morton, P. and Silverman, J. H.: Periodic points, multiplicities, and dynamical units, *J. Reine ang. Math.* (to appear).
12. Morton, P. and Silverman, J. H.: Rational periodic points of rational functions, *Inter. Math. Research Notices* **2** (1994), 97–109.
13. Mumford, D. and Fogarty, J.: *Geometric Invariant Theory* 2nd ed., Springer-Verlag, Berlin, 1982.
14. Narkiewicz, W.: Polynomial cycles in algebraic number fields, *Colloquium Math.* **58** (1989), 151–155.
15. Pezda, T.: Polynomial cycles in certain local domains, *Acta Arith.* **LXVI** (1994), 11–22.
16. Pezda, T.: Cycles of polynomial mappings in several variables, preprint, 1993.
17. Russo, P. and Walde, R.: Rational periodic points of the quadratic function $Q_c(x) = x^2 + c$, *Am. Math. Monthly* (1994) (to appear).
18. Serre, J.-P.: *Local Fields*, Springer-Verlag, New York, 1979.
19. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
20. Shimura, G.: On the field of definition for a field of automorphic functions. I, *Annals of Math.* **80** (1964), 160–189; II, **81** (1965), 124–165; III, **83** (1965), 377–385.
21. Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Forms*, Iwanami Shoten and Princeton University Press, Princeton, NJ, 1971.
22. Silverberg, A.: Fields of definition for homomorphisms of abelian varieties, *J. Pure Appl. Algebra* **77** (1992), 253–262.
23. Silverberg, A. and Zarhin, Yu.: Isogenies of abelian varieties, *J. Pure Appl. Algebra* **90** (1993), 23–37.
24. Silverman, J. H.: *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. 106, Springer-Verlag, Berlin, New York, 1986.
25. Silverman, J. H.: Integer points, Diophantine approximation, and iteration of rational maps, *Duke Math. J.* **71** (1993), 793–829.
26. Silverman, J. H.: Geometric and arithmetic properties of the Hénon map, *Math. Zeit.* **215** (1994), 237–250.
27. Thiran, E., Verstegen, D. and Weyers, J.: p-adic dynamics, *J. Statistical Physics* **54** (1989), 893–913.
28. Verstegen, D.: p-adic dynamical systems, in J.-M. Luck, P. Moussa, M. Waldschmidt (eds), *Number Theory and Physics*, Springer-Verlag, Berlin, 1990, pp. 235–242.
29. Weber, H.: *Lehrbuch der Algebra*, vol. II, Braunschweig, 1899.