WDC 2024

Equality of Field of Definition and Field of Moduli

Younghun Jo

January 9, 2024

Contents

In this article, we cover Silverman's result [3] on the problem of characterizing fields of definition for dynamical systems on $\mathbb{P}^1$. Theoretical background is based on [5, Section 4].

Throughout this article, let K be a field of characteristic 0, and $\overline{K}$ be its algebraic closure.

1 Rational Functions and Dynamical Systems

In this section, we review general theory of rational functions.

1.1 The Moduli Spaces of Rational Functions and Dynamical Systems

A *rational function* $\phi(z) \in K(z)$ is a quotient of polynomials

$$\phi(z) = \frac{F(z)}{G(z)} = \frac{a_0 + a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}$$

with no common factors, and let the *degree of* ϕ be

$$\deg \phi = \max\{\deg F, \deg G\}.$$

Or equivalently, we consider a degree d rational function $\phi(z) \in K(z)$ as a rational map

$$\phi = [F : G] : \mathbb{P}^1 \to \mathbb{P}^1$$

defined over K, where $F, G \in K[X, Y]$ are homogeneous polynomials of degree d with no common factors. One of the main concern of arithmetic dynamics is the dynamics of ϕ, namely the behavior of points in $\mathbb{P}^1$ under iterates of ϕ. We will mostly deal with the case when $d \geq 2$.

The dynamics of a rational map ϕ remains unchanged under a change of variables on $\mathbb{P}^1$. For a *linear fractional transformation* (or *Möbius transformation*)

$$f(z) = \frac{az + b}{cz + d} \in \mathrm{Aut}(\mathbb{P}^1) = \mathrm{PGL}_2,$$

the *linear conjugate of* ϕ *by* f is the map

$$\phi^f = f^{-1} \circ \phi \circ f.$$

We call the conjugacy class of ϕ the *dynamical system associated to* ϕ, and denote by $[\phi]$.

When we study the dynamics of rational maps, it is natural to consider the moduli space of all rational functions. The space Rat_d of rational maps $\mathbb{P}^1 \to \mathbb{P}^1$ of degree d is an affine variety defined over $\mathbb{Q}$ with the natural identification

$$\begin{array}{rcl} \{[\mathbf{a} : \mathbf{b}] \in \mathbb{P}^{2d+1} : \mathrm{Res}(F_{\mathbf{a}}, F_{\mathbf{b}}) \neq 0\} & \longrightarrow & \mathrm{Rat}_d \\ [\mathbf{a} : \mathbf{b}] & \longmapsto & \phi = [F_{\mathbf{a}} : F_{\mathbf{b}}] \end{array}$$

where

$$F_{\mathbf{a}}(X, Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d$$

for a $(d+1)$-tuple $\mathbf{a} = (a_0, \ldots, a_d)$.

Note that the ring of regular functions of Rat_d is given by

$$\mathbb{Q}[\mathrm{Rat}_d] = (\mathbb{Q}[\mathbf{a}, \mathbf{b}]_{\mathrm{Res}(F_{\mathbf{a}}, F_{\mathbf{b}})})_0,$$

that is, the set of degree 0 elements in the localization of the graded algebra $\mathbb{Q}[\mathbf{a}, \mathbf{b}]$ at the multiplicative set generated by $\mathrm{Res}(F_{\mathbf{a}}, F_{\mathbf{b}})$. Also note that Rat_d is a *fine moduli space* of rational maps $\mathbb{P}^1 \to \mathbb{P}^1$ of degree d. More precisely, the space Rat_d represents the functor from schemes to sets given by

$$S \longmapsto \left\{ S\text{-morphisms } \phi : \mathbb{P}^1_S \to \mathbb{P}^1_S \text{ with } \phi^* \mathcal{O}_{\mathbb{P}^1_S}(1) \cong \mathcal{O}_{\mathbb{P}^1_S}(d) \right\}.$$

This can be easily proved by an affine-local argument.

The linear conjugation induces an algebraic group action of PGL_2 on Rat_d. The *moduli space $\mathcal{M}_d$ of dynamical systems of degree d on $\mathbb{P}^1$* is defined as the quotient space

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

the abstract quotient space with no additional structure. The canonical map is denoted by $[\,\cdot\,] : \mathrm{Rat}_d \to \mathcal{M}_d$.

Alternatively, with the aid of geometric invariant theory, we may give $\mathcal{M}_d$ the structure of an algebraic variety. Note that PGL_2-action induces the action of PSL_2 on Rat_d. The algebraic variety $\mathcal{M}_d$ is defined as the GIT quotient

$$\mathcal{M}_d = \mathrm{Rat}_d \,/\!/\, \mathrm{PSL}_2 = \mathrm{Spec}\, \mathbb{Q}[\mathrm{Rat}_d]^{\mathrm{PSL}_2}.$$

Adopting this definition, $\mathcal{M}_d$ is a connected integral affine scheme of dimension $2d-2$ defined over $\mathbb{Q}$, and is a *coarse moduli space* of dynamical systems of degree d on $\mathbb{P}^1$. More precisely, there exists a natural transformation from the functor from schemes to sets given by

$$S \longmapsto \left\{ S\text{-morphisms } \phi : \mathbb{P}^1_S \to \mathbb{P}^1_S \text{ with } \phi^* \mathcal{O}_{\mathbb{P}^1_S}(1) \cong \mathcal{O}_{\mathbb{P}^1_S}(d) \right\} \Big/ \sim$$

where the equivalence relation is given by the linear conjugation, to the hom functor into $\mathcal{M}_d$. Moreover, Milnor's multiplier spectrum construction shows that there is an isomorphism

$$(\sigma_1, \sigma_2) : \mathcal{M}_2 \xrightarrow{\sim} \mathbb{A}_2$$

that can be described explicitly. However, this is beyond the aim of this article, so we will not concern ourselves with these matters.

1.2 Fields of Definition and the Field of Moduli

Let ξ be a dynamical system on $\mathbb{P}^1$. We say that a field K is a *field of definition (FOD) of* ξ if ξ contains a rational map ϕ defined over K. One of our main concern is to characterize fields of definition of a dynamical system ξ, and to find the minimal one if it exists.

One natural candidate for the minimal field of definition is the field of moduli, which can be defined using Galois theory. Let $\phi \in \xi$ be a rational map of degree d defined on $\overline{K}$. Then the Galois group $\mathrm{Gal}(\overline{K}/K)$ naturally act on ϕ by

$$\phi^\sigma = \sigma\left(\frac{a_0 + a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}\right) = \frac{\sigma(a_0) + \sigma(a_1) z + \cdots + \sigma(a_d) z^d}{\sigma(b_0) + \sigma(b_1) z + \cdots + \sigma(b_d) z^d}$$

where $\sigma \in \mathrm{Gal}(\overline{K}/K)$. The *field of moduli (FOM) of* ξ is the fixed field in $\overline{K}$ of the group

$$G_\phi = \{\sigma \in \mathrm{Gal}(\overline{K}/K) : \phi^\sigma \in \xi\},$$

that is, the subgroup of $\mathrm{Gal}(\overline{K}/K)$ fixing the dynamical system ξ. If we interpret $\mathcal{M}_d$ as an algebraic variety, then it is equal to the field generated by the coordinates of the point ξ in $\mathcal{M}_d$ by Hilbert's Satz 90.

Suppose that L is a field of definition for ϕ, that is, there is a linear fractional transformation $f \in \mathrm{PGL}_2(\overline{K})$ such that $\phi^f \in L(z)$. Then for $\sigma \in \mathrm{Gal}(\overline{K}/L)$, we have

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

so L contains the field of moduli for ξ. Hence, every field of definition for ϕ contains the field of moduli of ξ.

The problem is that, the field of moduli may *not* be a field of definition.

Example 1.1 (FOD $\neq$ FOM)**.** Let

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

Note that $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) = \{1, \tau\}$ where τ is the complex conjugation. For $g(z) = -1/z$, we have $\phi^\tau = \phi^g$, so $G_\phi = \{1, \tau\}$. Hence, $\mathbb{Q}$ is the field of moduli for ϕ. However, we can easily deduce that $\mathbb{Q}$ is not a field of definition for ϕ.

Nevertheless, the field of moduli is indeed a field of definition for a large class of dynamical systems on $\mathbb{P}^1$. The following theorem is the main goal of this article.

Theorem 1.2 (Silverman [3], FOD = FOM)**.** *Let K be a field of characteristic 0, and let $\xi = [\phi] \in \mathcal{M}_d(\overline{K})$ be a dynamical system of degree d on $\mathbb{P}^1$ with field of moduli K. Then, K is a field of definition for ξ in the following two cases:*

(a) The degree d is even.

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

2 Equality of FOD and FOM

In this section, we look into the proof of Theorem 1.2. Throughout this section, let $\phi \in \overline{K}(z)$ be a rational function of degree $d \geq 2$ with field of moduli K, and denote the associated dynamical system by $\xi = [\phi]$.

2.1 Group Cohomology

Before we begin, let us briefly review some basic notions of group cohomology theory. Throughout this section, let G be a group.

Definition 2.1 (G-module)**.** The *group ring* $\mathbb{Z}[G]$ *over* $\mathbb{Z}$ is a free module over $\mathbb{Z}$ generated by elements of G, that is also a ring under the multiplication linearly extended from the group law of G. A $\mathbb{Z}[G]$-module M is called a *G-module*.

Definition 2.2 (Group cohomology)**.** For a G-module M, let M^G be the submodule of G-invariant elements, that is,

$$M^G = \mathrm{Hom}_G(\mathbb{Z}, M) = \{f \in M : \sigma f = f \ \forall \sigma \in G\}.$$

Then $(-)^G = \mathrm{Hom}_G(\mathbb{Z}, -)$ is a left exact functor from G-modules to abelian groups. The *group cohomology functors $H^\bullet(G, -)$ of G* are given by the right derived functors

$$H^n(G, -) = R^n(-)^G.$$

Alternatively, we can define the cohomology groups of G in a more explicit manner. We will restrict our focus on the 1st cohomology group.

Definition 2.3 (1st cohomology group)**.** Let M be a G-module. The group of 1-*cocycles of G into M* consists of the maps $g = (\sigma \mapsto g_\sigma) : G \to M$ satisfying the cocycle condition

$$g_{\sigma\tau} = g_\sigma \sigma(g_\tau) \qquad \forall \sigma, \tau \in G.$$

The group of 1-*coboundaries of G into M* consists of the maps $g : G \to M$ of the form

$$\sigma \longmapsto g_\sigma = f\sigma(f^{-1})$$

for some $f \in M$. The 1*st cohomology group $H^1(G, M)$ of G with coefficient in M* is defined to be the group of 1-cocycles modulo the group of 1-coboundaries.

The 0th and 1st cohomology can also be recovered in the non-abelian setting.

Definition 2.4 (Non-abelian group cohomology)**.** A *G-group M* is a (not necessarily abelian) group together with an action by G. The 0*th cohomology of G with coefficients in M* is defined to be the subgroup $H^0(G, M) = M^G$ of G-invariant elements in M. The set of 1-*cocycles of G into M* consists of the maps $g = (\sigma \mapsto g_\sigma) : G \to M$ satisfying the cocycle condition

$$g_{\sigma\tau} = g_\sigma \sigma(g_\tau) \qquad \forall \sigma, \tau \in G.$$

Two 1-cycles g, g' are said to be *cohomologous* if there exists $f \in M$ such that

$$fg_\sigma = g'_\sigma \sigma(f) \qquad \forall \sigma \in G.$$

Note that this defines an equivalence relation on the set of 1-cocycles. The 1*th cohomology* $H^1(G, M)$ *of* G *with coefficients in* M is the pointed set given by the set of 1-cocycles modulo this relation, with the identity element as distinguished point.

One can require G and M to be topological groups, and the action of G on M to be continuous. Then we may adjust our definitions to allow only continuous cocycles. For the rest of this article, when G is the Galois group $\mathrm{Gal}(\overline{K}/K)$, we will consider the profinite topology on $\mathrm{Gal}(\overline{K}/K)$ and the discrete topology on M.

2.2 Cohomological Obstruction

Let us consider the automorphism group of rational maps and dynamical systems first.

Definition 2.5 (Automorphism group)**.** For a rational function $\phi \in \overline{K}(z)$, the *automorphism group of* ϕ is the group

$$\mathrm{Aut}(\phi) = \{f \in \mathrm{PGL}_2(\overline{K}) : \phi^f = \phi\} \leq \mathrm{PGL}_2(\overline{K}).$$

For a dynamical system $\xi \in \mathcal{M}_d(\overline{K})$, the *automorphism group of* ξ is $\mathrm{Aut}(\phi)$ for any $\phi \in \xi$ as as an abstract group, that is, $\mathrm{Aut}(\phi)$ up to conjugation by an element of $\mathrm{PGL}_2(\overline{K})$.

One important fact about the automorphism group is that it is always a finite subgroup of the projective linear group $\mathrm{PGL}_2(\overline{K})$.

Proposition 2.6 (Finiteness of automorphism group)**.** *Let* $\phi \in \overline{K}(z)$ *be a rational function of degree* d. *Then, the automorphism group* $\mathrm{Aut}(\phi)$ *is finite, and its order can be effectively bounded by a function of* d.

Proof. Note that for each n, the automorphism group permutes the set $\mathrm{Per}_n^{**}(\phi)$ of periodic points of ϕ with explicit period n, whose order can be effectively bounded by a function of d and n. We may choose distinct n_1, n_2, n_3, bounded effectively in d, so that each $\mathrm{Per}_{n_i}^{**}(\phi)$ is nonempty. (See [5, Corollary 4.7]) Hence, ϕ induces a group homomorphism

$$\psi : \mathrm{Aut}(\phi) \longrightarrow \prod_{i=1}^{3} \mathrm{Sym}(\mathrm{Per}_{n_i}^{**}(\phi))$$

where $\mathrm{Sym}(S)$ is the permutation group on a set S. Since a linear fractional transformation fixing three distinct points is an identity, the map ψ is injective. $\square$

Taking the automorphism group into our account, the notion of Galois cohomology naturally arises when we deal with the problem of fields of definition. Note that the projective linear group $\mathrm{PGL}_2(\overline{K})$ is a $\mathrm{Gal}(\overline{K}/K)$-group in the natural way.

Proposition 2.7. *Let $\phi \in \overline{K}(z)$ be a rational function of degree $d \geq 2$ with field of moduli K.*

(a) For each $\sigma \in \operatorname{Gal}(\overline{K}/K)$, there exists $g_\sigma \in \mathrm{PGL}_2(\overline{K})$ such that $\phi^\sigma = \phi^{g_\sigma}$, which is determined up to left multiplication by an element of $\operatorname{Aut}(\phi)$. Moreover, g_σ is contained in $N(\operatorname{Aut}(\phi))$, the normalizer of $\operatorname{Aut}(\phi)$ in $\mathrm{PGL}_2(\overline{K})$.

(b) Choosing g_σ as in (a), the resulting map

$$g : \operatorname{Gal}(\overline{K}/K) \longrightarrow Q(\operatorname{Aut}(\phi))$$

is a 1-cocycle of $\operatorname{Gal}(\overline{K}/K)$ into $Q(\operatorname{Aut}(\phi))$, where

$$Q(\operatorname{Aut}(\phi)) = N(\operatorname{Aut}(\phi))/\operatorname{Aut}(\phi).$$

Hence, ϕ determines a cohomology class $[g]$ in the 1st cohomology set

$$H^1(\operatorname{Gal}(\overline{K}/K), Q(\operatorname{Aut}(\phi))).$$

In particular, if the automorphism group $\operatorname{Aut}(\phi)$ of ϕ is trivial, then ϕ determines a cohomology class in $H^1(\operatorname{Gal}(\overline{K}/K), \mathrm{PGL}_2(\overline{K}))$.

(c) The quotient and inclusion maps $N(\operatorname{Aut}(\phi)) \twoheadrightarrow Q(\operatorname{Aut}(\phi))$ and $N(\operatorname{Aut}(\phi)) \hookrightarrow \mathrm{PGL}_2(\overline{K})$ induce the following maps p and i between cohomology sets.

$$\begin{tikzcd} H^1(\operatorname{Gal}(\overline{K}/K), N(\operatorname{Aut}(\phi))) \arrow[r, "i"] \arrow[d, "p"'] & H^1(\operatorname{Gal}(\overline{K}/K), \mathrm{PGL}_2(\overline{K})) \\ H^1(\operatorname{Gal}(\overline{K}/K), Q(\operatorname{Aut}(\phi))) & \end{tikzcd}$$

The field K is a field of definition of $[\phi]$ if and only if the (possibly empty) set $I_K(\phi) = i(p^{-1}([g]))$ contains the trivial class. In particular, if the automorphism group $\operatorname{Aut}(\phi)$ is trivial, then K is a field of definition of $[\phi]$ if and only if the class $[g]$ is trivial.

We call the set $I_K(\phi)$ the *cohomological obstruction of ϕ over K*.

Proof. (a) The existence of g_σ is obvious. Also, since $\operatorname{Aut}(\phi)$ is defined over K, we have that

$$\operatorname{Aut}(\phi) = \operatorname{Aut}(\phi)^\sigma = \operatorname{Aut}(\phi^\sigma) = \operatorname{Aut}(\phi^{g_\sigma}) = g_\sigma^{-1} \operatorname{Aut}(\phi) g_\sigma,$$

so g_σ is contained in the normalizer of $\operatorname{Aut}(\phi)$.

(b) For $\sigma, \tau \in \operatorname{Gal}(\overline{K}/K)$, we have that

$$\phi^{g_{\sigma\tau}} = (\phi^\tau)^\sigma = (\phi^{g_\tau})^\sigma = (\phi^\sigma)^{\sigma(g_\tau)} = \phi^{g_\sigma \sigma(g_\tau)},$$

hence $g_{\sigma\tau} = g_\sigma \sigma(g_\tau) \bmod \operatorname{Aut}(\phi)$.

(c) Suppose that K is a field of definition for $[\phi]$, that is, there exists some $f \in \mathrm{PGL}_2(\overline{K})$ so that ϕ^f is defined over K. Then, for $\sigma \in \operatorname{Gal}(\overline{K}/K)$,

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

so $g_\sigma = f\sigma(f^{-1}) \bmod \operatorname{Aut}(\phi)$. Hence, $[g]$ can be represented by the 1-cocycle $f\sigma(f^{-1})$, which clearly lifts to a cocycle in $N(\operatorname{Aut}(\phi))$ and is a 1-coboundary in $\mathrm{PGL}_2(\overline{K})$.

For the opposite direction, we only prove for the case of trivial automorphism group. Suppose that g is a 1-coboundary, that is, $g_\sigma = f\sigma(f^{-1})$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ for some $f \in \mathrm{PGL}_2(\overline{K})$. Then, for $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$(\phi^f)^\sigma = (\phi^\sigma)^{\sigma(f)} = (\phi^{g_\sigma})^{\sigma(f)} = \phi^f,$$

so by Hilbert's Satz 90, ϕ^f is defined over K. The proof for the general case will be given in Section 2.4. □

2.3 Theory of Twists

To deal with the FOD = FOM problem, at least for the trivial automorphism group case, what we have to consider is the 1st cohomology set with coefficient in $\mathrm{Aut}(\mathbb{P}^1/\overline{K}) = \mathrm{PGL}_2(\overline{K})$. The theory on twists of algebraic curves gives an efficient device to handle this.

We begin with a general setting. Throughout this section, let X and Y be objects defined over K, for instance, algebraic varieties, algebraic curves, or rational maps. We write $X \cong_K Y$ if there is a K-isomorphism between X and Y, and denote the K-isomorphism class of X by $[X]_K$. Similarly, write $X \cong Y$ if there is a $\overline{K}$-isomorphism between X and Y, and denote the $\overline{K}$-isomorphism class of X by $[X]$.

Definition 2.8 (Twist)**.** The set of *twists of X over K* is the set of K-isomorphism classes

$$\mathrm{Twist}(X/K) = \{[Y]_K : X \cong Y\}.$$

The notion of twists is also closely related to Galois cohomology.

Proposition 2.9. *Let X be an object defined over K, and Y be a representative for a twist of X over K.*

(a) Pick a $\overline{K}$-isomorphism $i : Y \to X$. Define $g : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(X)$ by

$$\sigma \longmapsto g_\sigma = i\sigma(i^{-1}).$$

Then, g satisfies the cocycle condition.

(b) The cohomology class $[g]$ is determined by the K-isomorphism class $[Y]_K$, and is independent of the choice of i. Hence, we obtain a natural map

$$\mathrm{Twist}(X/K) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{Aut}(X)).$$

(c) The twist $[Y]_K$ is trivial if and only if the class $[g]$ is trivial.

Proof. (a) For $\sigma, \tau \in \mathrm{Gal}(\overline{K}/K)$, we have

$$g_{\sigma\tau} = i\sigma(\tau(i^{-1})) = i\sigma(i^{-1}i\tau(i^{-1})) = g_\sigma\sigma(g_\tau).$$

(b) Let Y' be another K-twist of X that is isomorphic to Y, and $j : Y' \to X$ be a $\overline{K}$-isomorphism. Let g' be the 1-cocycle associated to Y' and j. Consider a K-isomorphism $k : Y' \to Y$. Then for $f = jki^{-1}$, we have

$$fg_\sigma = jk\sigma(i^{-1}) = j\sigma(k)\sigma(i^{-1}) = g'_\sigma\sigma(f),$$

so g and g' are cohomologous.

(c) If Y is K-isomorphic to X, then the 1-cocycle g associated to a K-isomorphism $i : Y \to X$ is a 1-coboundary.

For the opposite direction, suppose that g is a 1-coboundary, that is, $g_\sigma = f\sigma(f^{-1})$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$ for some $f \in \mathrm{Aut}(X)$. Then, for $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$\sigma(f^{-1}i) = f^{-1}g_\sigma\sigma(i) = f^{-1}i,$$

so $f^{-1}i : Y \to X$ is an isomorphism defined over K. □

2.4 Theory of Algebraic Curves

The cohomological obstruction $I_K(\phi)$ for FOD = FOM is a subset of the cohomology set

$$H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{PGL}_2(\overline{K})).$$

Since $\mathrm{PGL}_2(\overline{K})$ coincides with the automorphism group of the projective line $\mathbb{P}^1$, the cohomology classes might be associated to twists of $\mathbb{P}^1$. In the previous section, we have seen that every twist gives rise to a cohomology class, but in general, not every cohomology class comes from a twist. Fortunately, for the case of twists of $\mathbb{P}^1$, we can construct a twist of $\mathbb{P}^1$ from a given cohomology class.

Definition 2.10 (Brauer–Severi curve)**.** A *Brauer–Severi curve X over K* is a curve over K that is $\overline{K}$-isomorphic to $\mathbb{P}^1$, or equivalently, a smooth projective curve over K of genus 0. Two Brauer–Severi curves over K are said to be *equivalent* if they are K-isomorphic.

Proposition 2.11. *The natural map*

$$\mathrm{Twist}(\mathbb{P}^1/K) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), \mathrm{PGL}_2(\overline{K}))$$

is a bijection.

Proof. We proved the injectivity in the previous section, so we only need to prove surjectivity. Let g be a 1-cocycle of $\mathrm{Gal}(\overline{K}/K)$ into $\mathrm{PGL}_2(\overline{K})$. We will construct a Brauer–Severi curve X/K and a $\overline{K}$-isomorphism $i : X \to \mathbb{P}^1$ whose associated 1-cocycle is g.

Note that $\mathrm{Gal}(\overline{K}/K)$ acts naturally on the field $\overline{K}(\mathbb{P}^1) = \overline{K}(z)$. Consider the field $\overline{K}(\mathbb{P}^1)_g = \overline{K}(w)$ with a natural isomorphism $Z : \overline{K}(z) \to \overline{K}(w)$, but with a twisted action, given by

$$Z(\phi)^\sigma = Z((g_\sigma^{-1})^*\phi^\sigma) = Z(\phi^\sigma g_\sigma^{-1})$$

where $(g_\sigma^{-1})^* : \overline{K}(\mathbb{P}^1) \to \overline{K}(\mathbb{P}^1)$ is the map induced by $g_\sigma^{-1} : \mathbb{P}^1 \to \mathbb{P}^1$. Put

$$\mathcal{K} = \overline{K}(\mathbb{P}^1)_g^{\mathrm{Gal}(\overline{K}/K)},$$

the subfield of $\overline{K}(\mathbb{P}^1)_g$ fixed by the twisted action.

The field $\mathcal{K}$ has the following properties:

(i) $\mathcal{K} \cap \overline{K} = K$

(ii) $\overline{K}\mathcal{K} = \overline{K}(\mathbb{P}^1)_g$

(iii) $\mathrm{tr.deg}_K\,\mathcal{K} = 1$

The property (i) is obvious from Galois theory, and the property (ii) follows from Speiser's lemma (See [6, Lemma II.5.8.1]). Also, (ii) implies (iii).

By property (i) and (iii), there exists a smooth curve X/K with $K(X) \cong \mathcal{K}$. By (ii),

$$\overline{K}(X) = \overline{K}\mathcal{K} = \overline{K}(\mathbb{P}^1)_g \cong \overline{K}(\mathbb{P}^1),$$

so X is rational, hence is a twist of $\mathbb{P}^1$. Let $i : X \to \mathbb{P}^1$ be a $\overline{K}$-isomorphism, then the associated map i^* is isomorphism of fields

$$i^* = Z : \overline{K}(\mathbb{P}^1) \longrightarrow \overline{K}(\mathbb{P}^1)_g = \overline{K}(X).$$

Hence, for $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have

$$\phi^\sigma \sigma(i) = Z(\phi)^\sigma = Z(\phi^\sigma g_\sigma^{-1}) = \phi^\sigma g_\sigma^{-1} i$$

for all $\phi \in \overline{K}(\mathbb{P}^1)$, so $g_\sigma = i\sigma(i^{-1})$. □

Now we can prove the general case of Proposition 2.7(c).

Proof of Proposition 2.7(c). Suppose that g is a 1-cocycle of $\mathrm{Gal}(\overline{K}/K)$ into $\mathrm{PGL}_2(\overline{K})$ representing a class in the cohomological obstruction $I_K(\phi)$. Let X/K be the Brauer–Severi curve associated to g with a $\overline{K}$-isomorphism $i : X \to \mathbb{P}^1$. Consider $\Phi = i^{-1}\phi i : X \to X$, then

$$\Phi^\sigma = \sigma(i^{-1})\phi^\sigma \sigma(i) = \sigma(i^{-1})\phi^{g_\sigma}\sigma(i) = i^{-1}\phi i = \Phi,$$

so by Satz 90, Φ is defined over K. In particular, if g is a 1-coboundary, then i is a K-isomorphism, so $\phi = i\Phi i^{-1}$ is also defined over K. □

The problem of determining whether a twist of $\mathbb{P}^1$ is trivial can be addressed through the theory of algebraic curves, with a particular focus on the Riemann–Roch theorem.

Theorem 2.12 (Riemann–Roch theorem)**.** *Let X/K be a smooth projective curve of genus g. Then for $D \in \mathrm{Div}(X)$, we have*

$$\ell(D) - \ell(D_0 - D) = \deg(D) + 1 - g$$

where D_0 is a canonical divisor of X, with $\ell(D) = \dim H^0(X, \mathcal{L}(D))$.

Corollary 2.12.1. *Let X/K be a smooth projective curve of genus g, and $D \in \mathrm{Div}(X)$.*

(a) The canonical divisor D_0 of X is of degree $2g - 2$.
(b) If $\deg(D) \geq 2g + 1$, then D is very ample.

Proposition 2.13. *Let X be a twist of $\mathbb{P}^1$ over K. Then, the following are equivalent.*

(a) X is the trivial twist of $\mathbb{P}^1$ over K.
(b) $X(K)$ is nonempty.
(c) There exists a divisor on X of odd degree defined over K.

Proof. If there is a K-isomorphism $i : X \to \mathbb{P}^1$, then $i : X(K) \to \mathbb{P}^1(K)$ is a bijection, so (a) implies (b).

If $P \in X(K)$, then the divisor $D = (P)$ is of odd degree and defined over K, so (b) implies (c).

Let D be a divisor on X defined over K, and suppose that the degree $n = \deg(D)$ is odd. Consider a canonical divisor $D_0 \in \mathrm{Div}(X)$ having degree -2. Put

$$E = D + \frac{n-1}{2} D_0,$$

then E is a divisor of degree 1 defined over K. Hence, by the previous corollary, E is very ample and defines a closed immersion $X \to \mathbb{P}^1$ over K, which is an isomorphism. Thus, (c) implies (a). □

For later use, we state the Riemann–Hurwitz formula here.

Theorem 2.14 (Riemann–Hurwitz formula)**.** *Let $\Phi : X \to Y$ be a finite separable morphism of smooth projective curves over K. Then,*

$$2g(X) - 2 = (\deg \Phi)(2g(Y) - 2) + \sum_{P \in X} (e_P - 1)$$

where e_P is the ramification index of Φ at P.

2.5 The Case of Trivial Automorphism Group

Our problem becomes simple under the assumption that the automorphism group of the dynamical system is trivial.

Theorem 2.15 (FOD = FOM, $\mathrm{Aut}(\phi) = 1$ case)**.** *Let K be a field of characteristic 0, and let $\xi = [\phi] \in \mathcal{M}_d(\overline{K})$ be a dynamical system of degree d on $\mathbb{P}^1$ with field of moduli K. Suppose that the automorphism group $\mathrm{Aut}(\phi)$ of ϕ is trivial. Then, K is a field of definition for ξ in the following two cases:*

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

Proof. Let $g : \mathrm{Gal}(\overline{K}/K) \to \mathrm{PGL}_2(\overline{K})$ be the 1-cocycle associated to ϕ, and X/K be the corresponding Brauer–Severi curve with a $\overline{K}$ isomorphism $i : X \to \mathbb{P}^1$. It sufficies to show that X is a trivial twist of $\mathbb{P}^1$ over K.

Consier $\Phi = i^{-1}\phi i : X \to X$, then fir $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have

$$\Phi^\sigma = \sigma(i^{-1})\phi^\sigma\sigma(i) = \sigma(i^{-1})\phi^{g_\sigma}\sigma(i) = i^{-1}\phi i = \Phi,$$

so Φ is defined over K. Also note that $\deg \Phi = \deg \phi = d$.

(a) Let $D_\Phi = \mathrm{Div}(X)$ be the divisor of fixed points of Φ, that is, $D_\Phi = \Delta^*(\mathrm{graph}(\Phi))$ where $\Delta : X \to X \times_K X$ is the diagonal morphism. Then the degree $\deg(D_\Phi) = d + 1$ is odd, and D_Φ is defined over K, so X is a trivial twist of $\mathbb{P}^1$ over K.

(b) Since ϕ is a polynomial, there exists a totally ramified fixed point $P \in \mathbb{P}^1(\overline{K})$ of ϕ. Note that by the Riemann–Hurwitz formula, there are at most two totally ramified fixed points of ϕ.

If P is the only totally ramified fixed point of ϕ, then $Q = i^{-1}(P) \in X(\overline{K})$ is the unique totally ramified fixed point of Φ. Hence, for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have $\sigma(Q) = Q$, so Q is a K-point of X.

If ϕ has two distinct totally ramified fixed points, then ϕ is linearly equivalent to $\phi^f(z) = az^d$ for some $a \in \overline{K}^\times$. In this case, for $f'(z) = a^{-1/(d-1)}z$, the conjugate $\phi^{ff'}(z) = z^d$ is defined over K. □

2.6 The General Case

The general case of our problem becomes much harder without the assumption that the automorphism group is trivial. The main difficulty is that the 1-cocycle of $\mathrm{Gal}(\overline{K}/K)$ into $Q(\mathrm{Aut}(\phi))$ associated to ϕ might not lift to a cocycle into $N(\mathrm{Aut}(\phi))$. Nevertheless, we can obtain such lifting theorem for certain cases, and it is sufficient to cover our case.

Recall that $\mathrm{Aut}(\phi)$ is always a finite subgroup of $\mathrm{PGL}_2(\overline{K})$. We begin with a well-known classification of finite subgroup of $\mathrm{PGL}_2(\overline{K})$.

Theorem 2.16. *Let A be a finite subgroup of $\mathrm{PGL}_2(\overline{K})$.*

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

$$\begin{aligned}
C_n &= \textit{cyclic group of order } n, \quad n \geq 1. \\
D_{2n} &= \textit{dihedral group of order } 2n, \quad n \geq 2. \\
A_4 &= \textit{tetrahedral group} = \textit{alternating group of order } 12. \\
S_4 &= \textit{octahedral group} = \textit{symmetric group of order } 24. \\
A_5 &= \textit{icosahedral group} = \textit{alternating group of order } 60.
\end{aligned}$$

(b) More precisely, A is linearly conjugate to one of the following subgroups of $\mathrm{PGL}_2(\overline{K})$:

$$\begin{aligned}
C_n &= \langle \zeta_n z \rangle, \\
D_{2n} &= \left\langle \zeta_n z, \frac{1}{z} \right\rangle, \\
A_4 &= \left\langle -z, \frac{1}{z}, i\frac{z+1}{z-1} \right\rangle, \\
S_4 &= \left\langle iz, \frac{1}{z}, i\frac{z+1}{z-1} \right\rangle, \\
A_5 &= \left\langle \zeta_5 z, -\frac{1}{z}, \frac{(\zeta_5+\zeta_5^{-1})z+1}{1-(\zeta_5+\zeta_5^{-1})z} \right\rangle.
\end{aligned}$$

(c) For each of the groups A listed in (b), the normalizer $N(A)$ of A in $\mathrm{PGL}_2(\overline{K})$ is as follows:

$$\begin{array}{lll}
N(C_1) = \mathrm{PGL}_2(\overline{K}), & N(C_n) = D_\infty & (n \geq 2), \\
N(D_4) = S_4, & N(D_{2n}) = D_{4n} & (n \geq 3), \\
N(A_4) = S_4, & N(S_4) = S_4, & N(A_5) = A_5
\end{array}$$

where $D_\infty \cong \mathbb{G}_m \rtimes \mu_2$ is the infinite dihedral group, which is embedded in $\mathrm{PGL}_2(\overline{K})$ as

$$D_\infty = \{az : a \in \overline{K}^\times\} \cup \{b/z : b \in \overline{K}^\times\}.$$

Proof. By the Lefschetz principle, we may assume that $K = \mathbb{C}$.

Let A be a finite subgroup of $\mathrm{PGL}_2(\mathbb{C})$. Note that $\mathrm{PGL}_2(\mathbb{C})$ is isomorphic to the group $\mathrm{Isom}^+(\mathbb{H}^3)$ of orientation-preserving isometries of the hyperbolic 3-space $\mathbb{H}^3$. Hence, A can be viewed as a finite Kleinian group, which is conjugate to a finite subgroup of $\mathrm{SO}_3(\mathbb{R})$ acting on the Poincaré disc by rigid rotations fixing the origin. Thus, we may regard A as a finite group of rotations of a sphere.

If an orbit of A is planar, then A acts on a circle, so is isomorphic to a cyclic group C_n or a dihedral group D_{2n}. Assume that an orbit of A is not planar. Then A must be a group of rotational symmetries of a regular polyhedron, which is one of A_4, S_4, and A_5. Detailed explanation can be found in various literature.

For (c), see [3, Theorem 3.1]. $\square$

For certain types of finite subgroups of $\mathrm{PGL}_2(\overline{K})$, we establish a cohomology lifting theorem.

Theorem 2.17 (Cohomology lifting theorem)**.** *Let A be a finite subgroup of $\mathrm{PGL}_2(\overline{K})$ listed in Theorem 2.16(b). Then, the map*

$$H^1(\mathrm{Gal}(\overline{K}/K), N(A)) \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K), N(A)/A)$$

induced from the projection $p : N(A) \twoheadrightarrow N(A)/A$ is surjective in the following two cases:

(a) $A = C_n$ with n odd.

(b) $A = D_{2n}$ with n odd.

Proof. We have to manually construct a lifting of a cocycle. See [3, Theorem 3.2]. $\square$

Proposition 2.18. *Let K be a field of characteristic 0, and let $\xi = [\phi] \in \mathcal{M}_d(\overline{K})$ be a dynamical system of degree d on $\mathbb{P}^1$. Suppose that ϕ satisfies the following two properties:*

(i) $C_n = \langle \zeta_n z \rangle \subseteq \mathrm{Aut}(\phi)$.

(ii) There exists $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $f(z) = b/z \in \mathrm{PGL}_2(\overline{K})$ such that $\phi^\sigma = \phi^f$.

Then, $d \equiv \pm 1 \pmod{n}$.

Proof. We may assume that $n \geq 2$. Since ϕ is stable under conjugation by $\zeta_n z$, $z^{-1}\phi(z)$ is a function of z^n, say $\phi(z) = z\Phi(z^n)$ for some $\Phi \in \overline{K}(z)$. Hence,

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

Since $n \geq 2$, $\phi(0) = 0$ or ∞, and $\phi(\infty) = 0$ or ∞. Note that $\phi^\sigma(b/z)\phi(z) = b$. Putting $z = 0$ gives $\phi(0)\phi(\infty) = b$, so $\phi(0)$ and $\phi(\infty)$ cannot be both 0 and cannot be both ∞. Thus, ϕ permutes 0 and ∞.

First, suppose that $\phi(0) = 0$ and $\phi(\infty) = \infty$. Then $\mathrm{ord}_0(\Phi) \geq 0$ and $\mathrm{ord}_\infty(\Phi) \leq 0$, so Φ is of the form

$$\Phi(w) = \frac{a_r w^r + \cdots}{b_s w^s + \cdots + b_0} \qquad \text{with } a_r b_s b_0 \neq 0, r \geq s.$$

Hence,

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

Second, suppose that $\phi(0) = \infty$ and $\phi(\infty) = 0$. Then $\mathrm{ord}_0(\Phi) < 0$ and $\mathrm{ord}_\infty(\Phi) > 0$, so Φ is of the form

$$\Phi(w) = \frac{a_r w^r + \cdots + a_0}{b_s w^s + \cdots + b_1 w} \qquad \text{with } a_r a_0 b_s \neq 0, s > r.$$

Hence,

$$d = \deg(\phi) = \deg(z\Phi(z^n)) = -1 + ns \equiv -1 \pmod{n}. \qquad \square$$

Corollary 2.18.1. *Let K be a field of characteristic 0, and let $\xi = [\phi] \in \mathcal{M}_d(\overline{K})$ be a dynamical system of degree d on $\mathbb{P}^1$.*

(a) If d is odd, then the automorphism group of ξ is either

$$\mathrm{Aut}(\xi) = C_n \qquad \textit{or} \qquad \mathrm{Aut}(\xi) = D_{4n+2}.$$

(b) If ϕ is a polynomial, then the automorphism group of ξ is either

$$\mathrm{Aut}(\xi) = C_n \qquad \textit{or} \qquad \mathrm{Aut}(\xi) = D_{2d-2}.$$

Furthermore, the following are equivalent.

(i) $\mathrm{Aut}(\xi) = D_{2d-2}$.

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

(iii) The map ϕ has more than one exceptional point.

Proof. See [3, Corollary 4.4]. □

Now we prove our main theorem.

Theorem 2.19 (FOD = FOM, general case)**.** *Let K be a field of characteristic 0, and let $\xi = [\phi] \in \mathcal{M}_d(\overline{K})$ be a dynamical system of degree d on $\mathbb{P}^1$ with field of moduli K. Then, K is a field of definition for ξ in the following two cases:*

(a) The degree d is even.

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

Proof. (a) By the previous corollary, $\mathrm{Aut}(\xi)$ is either a cyclic group or a dihedral group. First suppose that $\mathrm{Aut}(\xi) = C_n$, and $n \geq 2$ since we have already proved $\mathrm{Aut}(\xi) = 1$ case. We may assume that $\mathrm{Aut}(\phi) = C_n = \langle \zeta_n z \rangle$. Recall that

$$N(\mathrm{Aut}(\phi)) = D_\infty = \{az : a \in \overline{K}^\times\} \cup \{b/z : b \in \overline{K}^\times\}.$$

Let $g : \mathrm{Gal}(\overline{K}/K) \to N(\mathrm{Aut}(\phi))$ be map associated to ϕ inducing a 1-cocycle into $Q(\mathrm{Aut}(\phi))$.

First, suppose that for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $g_\sigma = a_\sigma z$ for some $a_\sigma \in \overline{K}^\times$. Then a_σ is determined modulo μ_n, we obtain a 1-cocycle a of $\mathrm{Gal}(\overline{K}/K)$ into $\overline{K}^\times/\mu_n$. Since $\overline{K}^\times/\mu_n$ is isomorphic to $\overline{K}^\times$ as a $\mathrm{Gal}(\overline{K}/K)$-module by an isomorphism $a \mapsto a^n$, and the 1st cohomology of $\overline{K}^\times$ is trivial by Satz 90, the cocycle a is trivial in the cohomology group. Hence, there exists $\alpha \in \overline{K}^\times$ such that

$$a_\sigma = \alpha\sigma(\alpha^{-1}) \pmod{\mu_n} \qquad \forall \sigma \in \mathrm{Gal}(\overline{K}/K).$$

Put $f(z) = \alpha z \in N(\mathrm{Aut}(\phi))$, then $g_\sigma = f\sigma(f^{-1})$, so $f\sigma(f^{-1})$ is a lifting of g that is trivial in cohomology. Thus, K is a field of definition of ξ.

Second, suppose that $g_\sigma = b_\sigma/z$ for some $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $b_\sigma \in \overline{K}^\times$. Then by Proposition 2.18, we have $d \equiv \pm 1 \pmod{n}$, so n is odd. By the cohomology lifting theorem, we obtain a 1-cocycle of $\mathrm{Gal}(\overline{K}/K)$ into $\mathrm{PGL}_2(\overline{K})$. Verbatim et literatim, the rest of the proof is identical to that of the trivial automorphism group case.

Now suppose that $\mathrm{Aut}(\phi) = D_{2n}$. By the previous corollary, n is odd, so we can also apply the lifting theorem and mimic the proof for the trivial automorphism case.

(b) By the previous corollary, $\mathrm{Aut}(\xi)$ is either a cyclic group or a dihedral group. If $\mathrm{Aut}(\xi)$ is dihedral, then ξ contains z^d, so we are done. Hence, we may assume that $\mathrm{Aut}(\phi) = C_n = \langle \zeta_n z \rangle$ and $n \geq 2$. Moreover, ϕ has a unique totally ramified fixed point, which is stable under $\mathrm{Aut}(\phi)$, so it must be $z = \infty$.

For each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, we have

$$\{\infty\} = \{\infty\}^\sigma = \phi^{-1}(\infty)^\sigma = (\phi^{g_\sigma})^{-1}(\infty) = g_\sigma \phi^{-1}(g_\sigma^{-1}(\infty)),$$

so $\phi^{-1}(g_\sigma^{-1}(\infty)) = \{g_\sigma^{-1}(\infty)\}$, that is, $g_\sigma^{-1}(\infty)$ is an exceptional point of ϕ. Hence, $g_\sigma^{-1}(\infty) = \infty$, so g_σ is of the form $a_\sigma z$ for some $a_\sigma \in \overline{K}^\times$. The rest of the proof is identical to that of (a). □

References

[1] Hartshorne, R. (1977). Algebraic geometry. Springer.

[2] Lang, S. (1996). Topics in cohomology of groups. Springer.

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

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

[5] Silverman, J. H. (2007). The arithmetic of dynamical systems. Springer.

[6] Silverman, J. H. (2009). The arithmetic of elliptic curves. Springer.

[7] West, L. W. (2015). The moduli space of rational maps. *PhD thesis*. The City University of New York.