BELYI'S THEOREM

ANAND DEOPURKAR

1. Introduction

There are two fundamentally distinct ways of viewing a Riemann surface: the complex analytic point of view, in which it becomes a compact complex manifold, and the algebro-geometric point of view, in which it becomes a smooth projective complex variety. Many questions about Riemann surfaces can be approached from either side, but there are some that seem completely opaque from one side. One such question is the following:

Question 1.1. *Given a Riemann surface X, can it be defined over a number field?*

More precisely, given a (smooth, projective) curve X over $\mathbf{C}$, is there a number field K and a curve $\mathcal{X}$ over K such that $X = \mathcal{X} \times_K \mathbf{C}$? Concretely, can X be realised as the zero locus of a set of polynomials with coefficients in K? This question is natural from the algebro-geometric point of view. But it seems impenetrable from the complex analytic point of view. Belyi's theorem is a remarkable statement that bridges this gap—it gives a topological characterisation of Riemann surfaces that can be defined over a number field.

Theorem 1.2 (Belyi)**.** *Let X be a Riemann surface. The following two are equivalent:*

(1) *X can be defined over a number field.*
(2) *X can be realised as a branched cover of $\mathbf{P}^1_{\mathbf{C}}$ with branch locus contained in $\{0, 1, \infty\}$.*

The second condition means that there exists a finite morphism

$$f\colon X \to \mathbf{P}^1_{\mathbf{C}},$$

which is unramified over $\mathbf{P}^1_{\mathbf{C}} \setminus \{0, 1, \infty\}$. Such a map $f\colon X \to \mathbf{P}^1_{\mathbf{C}}$ is called a *Belyi map*. It is not unique. Belyi's theorem says that X admits a Belyi map if and only if it can be defined over a number field.

The three points $\{0, 1, \infty\}$ are not special. We could have chosen any three points, or just said "three points", without specifying which ones. After all, any set of 3 points on $\mathbf{P}^1$ can be moved to any other set of 3 points by a projective linear transformation, so all of these versions are equivalent.

Saying that X is defined over a number field is equivalent to saying that X is defined over $\overline{\mathbf{Q}}$.

1.1. Belyi's theorem and uniformisation.

Consider a Riemann surface X with a Belyi map $f\colon X \to \mathbf{P}^1_{\mathbf{C}}$. Let $U = \mathbf{P}^1_{\mathbf{C}} \setminus \{0, 1, \infty\}$ and set $X^\circ = f^{-1}(U)$. Then $f\colon X^\circ \to U$ is a covering space. The universal cover of U is the upper half plane $\mathbb{H}$. Let $\Lambda = \Gamma(2) \subset \mathrm{PSL}_2(\mathbf{Z})$ be the kernel of $\mathrm{PSL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/2\mathbf{Z})$. Then Λ is isomorphic to the free group on 2 letters. It is the fundamental group of U is Λ, and it acts on $\mathbb{H}$ by fractional linear transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}.$$

Since $X^\circ \to U$ is a covering space of finite degree, the fundamental group of X° embeds as a finite index subgroup $G \subset \Lambda$ and

$$X^\circ = \mathbb{H}/G.$$

An equivalent form of Belyi's theorem is that X can be defined over a number field if and only if it can be realised as (the compactification of) $\mathbb{H}/G$ for a finite index subgroup $G \subset \Lambda$.

Date: November 11, 2021.

2. Defined over $\overline{\mathbf{Q}}$ implies $\exists$ Belyi map

The goal of this section is to prove that if X is defined over $\overline{\mathbf{Q}}$, then it admits a Belyi map. The proof is elementary but involves some work by hand. This is what Belyi proved in his 1979 paper. (The other direction was already known and follows by "general principles".) I present a proof from Köck [2004].

2.1. **Step 1: Pick $\phi\colon X \to \mathbf{P}^1$ defined over $\overline{\mathbf{Q}}$.** Since X is a smooth projective curve over $\overline{\mathbf{Q}}$, there exists a finite map $\phi\colon X \to \mathbf{P}^1_{\overline{\mathbf{Q}}}$. Pick one. Let $S \subset \mathbf{P}^1(\overline{\mathbf{Q}})$ be the set $\operatorname{Crit}\phi$ of critical values of ϕ. Then, by definition, ϕ is unramified over $\mathbf{P}^1_{\overline{\mathbf{Q}}} \setminus S$.

2.2. **Step 2: Arrange so that $\operatorname{Crit}\phi \subset \mathbf{P}^1(\mathbf{Q})$.** We do this using the following.

Lemma 2.1. *Let $\phi\colon X \to \mathbf{P}^1_{\overline{\mathbf{Q}}}$ be a finite map and $S \subset \mathbf{P}^1(\overline{\mathbf{Q}})$ a finite set containing $\operatorname{Crit}\phi$. Then there exists a finite map $p\colon \mathbf{P}^1_{\mathbf{Q}} \to \mathbf{P}^1_{\mathbf{Q}}$ such that $\operatorname{Crit}(p\circ\phi) \subset \mathbf{P}^1(\mathbf{Q})$.*

Proof. Enlarge S so that it is $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-invariant (add all the Galois conjugates). Let $S^{\mathrm{irr}} \subset S$ be the set of points of S that are not $\mathbf{Q}$-points. We induct on the size n of S^{irr}. If $n = 0$, then we are done. Otherwise, consider $p\colon \mathbf{P}^1_{\mathbf{Q}} \to \mathbf{P}^1_{\mathbf{Q}}$ defined by the polynomial

$$p(x) = \prod_{s\in S^{\mathrm{irr}}} (x - s).$$

Note that p is defined over $\mathbf{Q}$ and sends S^{irr} to 0. Let $R \subset \mathbf{A}^1(\overline{\mathbf{Q}})$ be the set of roots of $p'(x)$. Then the critical points of p consist of R and the point at infinity. The critical values of $p\circ\phi$ are contained in the set $S' = p(S) \cup p(R) \cup \{\infty\}$. Note that S' is $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-invariant. The only possible irrational points in S' are the points of $p(R)$, of which there are at most $(n-1)$. We replace ϕ by $p\circ\phi$ and continue inductively. ☐

2.3. **Step 3: Arrange so that $\operatorname{Crit}\phi \subset \{0, 1, \infty\}$.**

Lemma 2.2. *Let $S \subset \mathbf{P}^1(\mathbf{Q})$ be a finite set. Then there exists a finite map $f\colon \mathbf{P}^1_{\mathbf{Q}} \to \mathbf{P}^1_{\mathbf{Q}}$ such that $f(S) \cup \operatorname{Crit} f \subset \{0, 1, \infty\}$.*

Proof. The magic sauce is the fuction $q\colon \mathbf{P}^1_{\mathbf{Q}} \to \mathbf{P}^1_{\mathbf{Q}}$ defined by the polynomial

$$q(x) = c \cdot x^m (1 - x)^n,$$

where m, n are positive integers and $c \in \mathbf{Q}$ is a constant. The critical points of q are $\{0, 1, \infty, \frac{m}{m+n}\}$. The map q sends $0, 1 \mapsto 0$ and $\infty \mapsto \infty$. By choosing the right c, we can ensure that it sends $\frac{m}{m+n}$ to 1. Then the critical values of q lie in $0, 1, \infty$.

To prove the lemma, we may assume that S contains at least 3 points. After applying a fractional linear transformation, we may assume that S contains $\{0, 1, \infty\}$. Write $S = \{0, 1, \infty\} \cup T$, where T is disjoint from $\{0, 1, \infty\}$. We induct on the size of T. If T is empty, there is nothing to prove. Otherwise, pick a $t \in T$. Using a combination of $z \mapsto 1-z$ and $z \mapsto 1/z$, both of which preserve the triplet $\{0, 1, \infty\}$, we may assume that $t \in \mathbf{Q}$ satisfies $0 < t < 1$. Then $t = \frac{m}{m+n}$ for some positive integers m, n. Let $q\colon \mathbf{P}^1_{\mathbf{Q}} \to \mathbf{P}^1_{\mathbf{Q}}$ be as above. We let $S' = q(T) \cup \{0, 1, \infty\}$. Then $S' = \{0, 1, \infty\} \cup T'$, where $T' \subset q(T - \{t\})$ has fewer elements than T. By the inductive hypothesis, there is a $g\colon \mathbf{P}^1_{\mathbf{Q}} \to \mathbf{P}^1_{\mathbf{Q}}$ such that $g(q(S')) \cup \operatorname{Crit} g \subset \{0, 1, \infty\}$. Then $f = g \circ q$ satisfies $f(S) \cup \operatorname{Crit} f \subset \{0, 1, \infty\}$. ☐

To finish the construction of the Belyi map, let $\phi\colon X \to \mathbf{P}^1$ be as in Step 2, namely, with $\operatorname{Crit}\phi \subset \mathbf{P}^1(\mathbf{Q})$. Apply the last lemma with $S = \operatorname{Crit}\phi$ to get an $f\colon \mathbf{P}^1 \to \mathbf{P}^1$ with $f(S) \cup \operatorname{Crit} f \subset \{0, 1, \infty\}$. Then $f\circ\phi\colon X \to \mathbf{P}^1$ is a Belyi map.

3. $\exists$ Belyi map implies defined over $\overline{\mathbf{Q}}$

The goal of this section is to prove that if X admits a Belyi map $f\colon X \to \mathbf{P}^1_{\mathbf{C}}$, then X can be defined over $\overline{\mathbf{Q}}$. As mentioned before, this follows by quite soft arguments in algebraic geometry.

Let $K \subset \mathbf{C}$ be a field. Given an effective divisor $D \subset \mathbf{P}^1_{\mathbf{C}}$, we say that D is K-rational if it is the divisor of a homogeneous form $F(X, Y)$ whose coefficients are in K. In other words, D is obtained by base-change from an effective divisor on $\mathbf{P}^1_K$. Let X be a smooth projective curve of genus g over K and $\phi\colon X \to \mathbf{P}^1_K$ a finite map of degree d. To ϕ, we can associate an effective divisor $\operatorname{Br}\phi \subset \mathbf{P}^1_K$ of degree $b = 2g + 2d - 2$, called the *branch divisor*. The set of $\mathbf{C}$-points underlying $\operatorname{Br}\phi$ is the set of critical values of ϕ, but the divisor also contains the data of multiplicities for each point that encodes the amount of ramification over each point, and it also turns out to be K-rational. The branch divisor is defined as the divisor associated to a homogeneous form called the *discriminant* of ϕ. The map ϕ is unramified over the complement of $\operatorname{Br}\phi$. (We will not go into the construction of $\operatorname{Br}\phi$.)

Proposition 3.1. *Let X be a smooth projective curve over $\mathbf{C}$ and let $\phi\colon X \to \mathbf{P}^1$ be a finite map. If $\operatorname{Br}\phi$ is K-rational for some subfield $K \subset \mathbf{C}$, then X can be defined over a finite extension of K.*

The "easy" direction of Belyi's theorem follows from this proposition, since any divisor supported on $\{0, 1, \infty\}$ is $\mathbf{Q}$-rational.

3.1. **Sketch of a proof of Proposition 3.1.** Fix a genus g and a degree d. The key point is that there is a *moduli space* that parametrizes degree d and genus g branched covers of $\mathbf{P}^1$. I will first explain a false (but "morally " true) version of what this means and then make corrections.

Consider maps $\phi\colon X \to \mathbf{P}^1$ where X is a smooth projective curve of genus g and ϕ is a finite map of degree d, up to isomorphism, where we treat two maps $\phi_1\colon X_1 \to \mathbf{P}^1$ and $\phi_2\colon X_2 \to \mathbf{P}^1$ as isomorphic if there is an isomorphism $i\colon X_1 \to X_2$ making the following diagram commute:

$$\begin{array}{ccc} X_1 & \xrightarrow{\;i\;} & X_2 \\ \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} \\ \mathbf{P}^1 & = & \mathbf{P}^1. \end{array}$$

Proposition 3.2 (Not literally true)**.** *There is a scheme $\mathcal{H}_{d,g}$ of finite type over $\mathbf{Q}$ with a natural isomorphism*

$$\mathcal{H}_{d,g}(K) \cong \{\phi_K\colon X_K \to \mathbf{P}^1_K\}/iso$$

for every field extension $K/\mathbf{Q}$.

In fact, the natural isomorphism holds for $\mathcal{H}_{d,g}(S)$ for any $\mathbf{Q}$-scheme S, with the correct definition of the right hand side. But for us, fields will suffice.

Let me explain what "natural" means. The left and right hand sides of the equation in Proposition 3.2 are functors in K. Given $K \to L$, we have a natural induced maps

$$\mathcal{H}_{d,g}(K) \to \mathcal{H}_{d,g}(L),$$

obtained by treating a K-point as an L-point, and

$$\{\phi_K\colon X_K \to \mathbf{P}^1_K\} \to \{\phi_L\colon X_L \to \mathbf{P}^1_L\}$$

obtained by applying $- \times_K L$. The propostion asserts a natural isomorphism of these functors.

Similarly, there is a moduli space that parametrizes degree b divisors on $\mathbf{P}^1$.

Proposition 3.3 (Literally true)**.** *There is a scheme $\mathcal{P}_b$ of finite type over $\mathbf{Q}$ with a natural isomorphism*

$$\mathcal{P}_b(K) \cong \{\text{Divisors of degree } b \text{ on } \mathbf{P}^1_K\}$$

for every field extension $K/\mathbf{Q}$.

In fact, it is easy to see what $\mathcal{P}_b$ is: it is just the projective space $\mathbf{P}^b$. To be precise, let V be the degree b homogeneous component of $\mathbf{Q}[X, Y]$. Then $\mathcal{P}_b = \mathbf{P}V$.

Recall that we have a rule $\phi \mapsto \operatorname{Br}\phi$ that takes a finite cover and gives a branch divisor. This rule can be used to define a morphism of schemes

$$\operatorname{Br}\colon \mathcal{H}_{d,g} \to \mathcal{P}_b.$$

Proposition 3.4. *The morphism* Br *is quasi-finite. That is, it has finite fibers.*

Proof. It is enough to check that given any $\mathbf{C}$-point of $\mathcal{P}_b$, there are only finitely many $\mathbf{C}$ points of $\mathcal{H}_{d,g}$ in its pre-image. That is, given a divisor $B \subset \mathbf{P}^1_{\mathbf{C}}$ of degree b, we must prove that there are only finitely many $\phi\colon X \to \mathbf{P}^1_{\mathbf{C}}$ with $\operatorname{Br}\phi = B$, up to isomorphism. Any such ϕ gives a covering space $X^o \to U$, where $U = \mathbf{P}^1_{\mathbf{C}} \setminus B$. By the theory of covering spaces in complex analysis, covering spaces $X^\circ \to U$ are equivalent to branched covers of Riemann surfaces $X \to \mathbf{P}^1$ unbranched outside B (and all such covers are algebraic). On the other hand, a degree d covering space of U is determined by its monodromy, which is a homomorphism

$$\pi_1(U) \to S_d.$$

The group $\pi_1(U)$ is finitely generated and the group S_d is finite, so there are only finitely many such homomorphisms. □

We now have the tools to finish the proof of Proposition 3.1. Consider $\phi\colon X \to \mathbf{P}^1_{\mathbf{C}}$ whose branch divisor $\operatorname{Br}\phi \subset \mathbf{P}^1_{\mathbf{C}}$ is K-rational. The branch divisor corresponds to a $\mathbf{C}$-point of $\mathcal{P}_b$. Saying that it is K-rational is equivalent to saying that this point arises from a K-point $\operatorname{Spec} K \to \mathcal{P}_b$. Then $\phi\colon X \to \mathbf{P}^1_{\mathbf{C}}$ corresponds a $\mathbf{C}$-point of the fiber product

$$\mathcal{H}_{d,g} \times_{\mathcal{P}_b} \operatorname{Spec} K.$$

Since $\mathcal{H}_{d,g} \to \mathcal{P}_b$ is quasi-finite, this fiber product is a finite K-scheme, that is, it is the spectrum of a K-algebra A of finite length. As a result, any homomorphism $A \to \mathbf{C}$ factors as $A \to A/m \to \mathbf{C}$, where $m \subset A$ is a maximal ideal (this uses that A is of finite length; in general m is only prime). By the Nullstellensatz, $L = A/m$ is a finite extension of K. So the $\mathbf{C}$-point $\phi\colon X \to \mathbf{P}^1_{\mathbf{C}}$ of $\mathcal{H}_{d,g}$ arises from an L-point, where L/K is a finite extension. In particular, X is obtained by base-change from a curve defined over L.

It is now time to come clean. As I confessed, Proposition 3.2 is not true. But it *is* true if we replace "scheme" by "Deligne–Mumford stack". The rest of the argument goes through almost verbatim. Alternatively, we can use a weaker notion of moduli space called a 'coarse' moduli space. It is perhaps not wise to go into the details, but the key point is that then Proposition 3.2 is literally true (with the word "scheme" in place) but only for algebraically closed $K/\mathbf{Q}$. But this suffices for our purposes. The same argument as before implies that $\phi\colon X \to \mathbf{P}^1_{\mathbf{C}}$ arises from a $\overline{K}$ point, which is just as good.

3.1.1. *References for this section.* The space $\mathcal{H}_{d,g}$ is called the *Hurwitz space*. Its existence and properties over $\mathbf{C}$ have been known at least since Riemann. Fulton in Fulton [1969] constructs it over $\mathbf{Z}[1/d!]$ but with an additional condition of simple branching. Romagny and Wewers Romagny and Wewers [2006] construct it more generally. But both of these references deal with mixed characteristics, where the theory is harder. In characteristic 0, the space we want also follows from the existence of the Kontsevich space of maps treated, for example, in Fulton and Pandharipande [1997] (over $\mathbf{C}$, but the arguments should work at least over $\overline{\mathbf{Q}}$ if not $\mathbf{Q}$). But they also treat the case of singular curves, making it harder than it needs to be. It can be a good exercise to just write your own proof of Proposition 3.2 using the existence of the moduli stack of curves $\mathcal{M}_g$. There is an obvious forgetful map $\mathcal{H}_{d,g} \to \mathcal{M}_g$, and it is not too hard to show that this map is representable by schemes.

3.2. **A more direct argument.** Let us sketch a more direct argument for Proposition 3.1 that does not rely on the existence of the moduli space. It will bring up some ideas that may be helpful. The proof is based on Hammer and Herrlich [2003].

Let $X/\mathbf{C}$ be a $\mathbf{C}$-scheme with the structure map $X \xrightarrow{\pi} \operatorname{Spec}\mathbf{C}$. Let $\sigma\colon \mathbf{C} \to \mathbf{C}$ be a field automorphism. Denote by $X^\sigma/\mathbf{C}$ the $\mathbf{C}$-scheme $X \xrightarrow{\pi'} \operatorname{Spec}\mathbf{C}$ where $\pi' = \sigma \circ \pi$. It is useful to think of this procedure for affine schemes, say for example $X = \operatorname{Spec} A$ where A is a $\mathbf{C}$-algebra. Take, for example $A = \mathbf{C}[x,y]/f(x,y)$, where

$$f(x,y) = \sum a_{i,j} x^i y^j, \text{ for } a_{i,j} \in \mathbf{C}.$$

Then $X^\sigma = \operatorname{Spec} A^\sigma$, where A^σ is the same ring as A but the embedding $\mathbf{C} \to A^\sigma$ is different. As a $\mathbf{C}$-algebra, A^σ is in fact isomorphic to $\mathbf{C}[x,y]/f^\sigma(x,y)$, where

$$f^\sigma(x,y) = \sum \sigma^{-1}(a_{i,j}) x^i y^j.$$

Thus, we may think $X^\sigma/\mathbf{C}$ as the $\mathbf{C}$-scheme obtained from $X/\mathbf{C}$ where the coefficients of the defining equations have been changed by applying σ^{-1}.

Remark 3.5. Consider the sets of complex points $X(\mathbf{C})$ versus $X^\sigma(\mathbf{C})$. We have a bijection between these two sets obtained by applying σ. But $\sigma\colon \mathbf{C} \to \mathbf{C}$ will not be holomorphic (except for $\sigma = \mathrm{id}$) or even continuous (except for $\sigma = \mathrm{id}$ or complex conjugation). So it *will not* give a biholomorphism between $X(\mathbf{C})$ and $X^\sigma(\mathbf{C})$.

Suppose X can be defined over a subfield $K \subset \mathbf{C}$ and $\sigma \in \mathrm{Aut}(\mathbf{C}/K)$. Then the coefficients of a set of defining equations of X are fixed by σ, so $X/\mathbf{C}$ and $X^\sigma/\mathbf{C}$ are isomorphic.

Definition 3.6. Let X be a scheme over $\mathbf{C}$. Let $G(X) \subset \mathrm{Aut}(\mathbf{C}/\mathbf{Q})$ be the subgroup consisting of σ such that $X/\mathbf{C}$ and $X^\sigma/\mathbf{C}$ are isomorphic. The *field of moduli* of X, denoted by $M(X)$, is the subfield of $\mathbf{C}$ fixed by $G(X)$

$$M(X) = \mathbf{C}^{G(X)}.$$

Strictly speaking, $G(X)$ and $M(X)$ depend on $X/\mathbf{C}$—that is, X along with the structure map and not just X—but this is usually dropped from the notation.

Suppose X can be defined over $K \subset \mathbf{C}$. Then $\mathrm{Aut}(\mathbf{C}/K) \subset G(X)$. The fixed field of $\mathrm{Aut}(\mathbf{C}/K)$ is K (not obvious, but true; the proof needs the axiom of choice because the extension $K/\mathbf{C}$ can be infinite, but this is ultimately true because $\mathbf{C}$ is algebraically closed). So we get the inclusion $M(X) \subset K$. It is not always possible to have equality—it may not be true that X can be defined over $M(X)$—but it is only a finite extension away.

Proposition 3.7. *Let $X/\mathbf{C}$ be a smooth projective curve and let $M = M(X)$ be its field of moduli. Then there exists a finite extension K/M such that X can be defined over K.*

Proof. We want to exhibit a finite extension K/M and a K-scheme Y such that X is isomorphic to $Y \times_K \mathbf{C}$ as a $\mathbf{C}$-scheme.

It may be helpful to keep a running example in mind, such as the X defined by the (homogenisation) of

$$y^2 = (x^3 - \pi).$$

Then the field of moduli is $\mathbf{Q}$ and our proof will in fact show that X is isomorphic to a curve defined over $\mathbf{Q}$. This is easy to see directly, but it is instructive to see how it comes about in the proof.

Since $X/\mathbf{C}$ is of finite type, it is defined over a subfield $L \subset \mathbf{C}$ which is finitely generated over M. We can write $L = \operatorname{frac} A$ where A is a finitely generated M-algebra. Then we can "spread out" $X \to \operatorname{Spec} L$ to a $\pi\colon \mathcal{X} \to \operatorname{Spec} A$. By shrinking A if necessary, we may assume that π is smooth and proper. Then, by construction, we have

$$X = \mathcal{X} \times_A \mathbf{C},$$

along the map $A \to \mathbf{C}$ that is the composite of $A \to L$ and $L \to \mathbf{C}$.

In our running example, we can take $L = \mathbf{Q}(t)$ with the map $L \to \mathbf{C}$ given by $t \mapsto \pi$ and $A = \mathbf{Q}[t, t^{-1}]$ and $\mathcal{X}$ to be the A-scheme defined by (the homogenisation of) $y^2 = x^3 - t$.

Now consider the set of $\mathbf{C}$ points of $\operatorname{Spec} A$ over M, or equivalently, M-homomorphisms $A \to \mathbf{C}$. The fiber of π over every $\mathbf{C}$ point is a $\mathbf{C}$-scheme. Consider the point $p\colon A \to \mathbf{C}$ corresponding to the composite $A \to L \to \mathbf{C}$. The fiber over this point is, by construction, $X/\mathbf{C}$. For $\sigma \in G(X)$, the fiber over $\sigma(p)$ is $X^\sigma/\mathbf{C}$, which is isomorphic to $X/\mathbf{C}$.

The point p represents a closed point of $\operatorname{Spec} A_{\mathbf{C}}$, where $A_{\mathbf{C}} = A \times_M \mathbf{C}$. But since $p\colon A \to \mathbf{C}$ is injective, this point lies over the generic point of $\operatorname{Spec} A$. Using this, it is not hard to show that the $G(X)$ orbit of $p \in \operatorname{Spec} A_{\mathbf{C}}$ is Zariski dense in $\operatorname{Spec} A_{\mathbf{C}}$.

In our running example, this orbit consists of the points of $\operatorname{Spec} \mathbf{C}[t, t^{-1}]$ corresponding to any transcendental value of t.

Set

$$\mathbb{X} = \mathcal{X} \times_M \mathbf{C}.$$

Then $\mathbb{X} \to \operatorname{Spec} A_{\mathbf{C}}$ is a proper smooth morphism whose fibers over a Zariski dense subset are isomorphic to a single $X/\mathbf{C}$. With a little bit of argument (for example, by invoking the Isom scheme, which is proper;

see), this implies that *all* fibers are isomorphic to $X/\mathbf{C}$. But $\operatorname{Spec} A_{\mathbf{C}}$ includes closed points that lie over closed points of $\operatorname{Spec} A$. Let q be one such point. Then the kernel of $q\colon A \to \mathbf{C}$ is a maximal ideal $m \subset A$, whose residue field $K = A/m$ is a finite extension of M by the Nullstellensatz. Take $Y = \mathcal{X} \times_A K$. Then Y is a K-scheme such that $Y \times_K \mathbf{C}$ is isomorphic to X.

In our running example, we can take q to be any point of $\operatorname{Spec} \mathbf{C}[t, t^{-1}]$ corresponding to an algebraic value of t. □

The only place in the proof where we used that $X/\mathbf{C}$ is a smooth projective curve is in the parenthetical remark invoking Isom. In fact, in any situation where constancy of the isomorphism class over a dense set implies constancy over the whole base, the argument should hold.

Remark 3.8. It is possible that X cannot be defined over the field of moduli and a finite extension is really required. However, if X has no non-trivial automorphisms, then we can use descent to show that X can be defined over the field of moduli. See Shimura [1972, Theorems 2 and 3] for examples where a finite extension is required.

Using Proposition 3.7, it is now quite easy to deduce Proposition 3.1. Let $X/\mathbf{C}$ be a smooth projective curve and $\phi\colon X \to \mathbf{P}^1_{\mathbf{C}}$ a finite map such that $\operatorname{Br}\phi$ is K-rational. Let $\sigma \in \operatorname{Aut}(\mathbf{C}/K)$. Then $\phi^\sigma\colon X^\sigma \to \mathbf{P}^1_{\mathbf{C}}$ is a map of the same degree with the same branch divisor. But there are only finitely many isomorphism classes of covers with this branch divisor. Hence, there is a finite index subgroup $H \subset \operatorname{Aut}(\mathbf{C}/K)$ such that for every $\sigma \in H$, the curves $X/\mathbf{C}$ and $X^\sigma/\mathbf{C}$ are isomorphic. A bit of Galois theory (handled with care due to the infinite nature of extensions) shows that $\mathbf{C}^H/K$ is a finite extension. Thus, the field of moduli of X is contained in a finite extension of K. By Proposition 3.7, we conclude that X can be defined over a finite extension of K.

References

W. Fulton and R. Pandharipande. Notes on stable maps and quantum cohomology. In *Algebraic geometry—Santa Cruz 1995*, volume 62 of *Proc. Sympos. Pure Math.*, pages 45–96. Amer. Math. Soc., Providence, RI, 1997. doi: 10.1090/pspum/062.2/1492534. URL `http://dx.doi.org/10.1090/pspum/062.2/1492534`.

William Fulton. Hurwitz schemes and irreducibility of moduli of algebraic curves. *Ann. of Math. (2)*, 90: 542–575, 1969. ISSN 0003-486X. doi: 10.2307/1970748.

Horst Hammer and Frank Herrlich. A remark on the moduli field of a curve. *Arch. Math.*, 81(1):5–10, 2003. ISSN 0003-889X. doi: 10.1007/s00013-003-4649-5.

Bernhard Köck. Belyi's theorem revisited. *Beitr. Algebra Geom.*, 45(1):253–265, 2004. ISSN 0138-4821.

Matthieu Romagny and Stefan Wewers. Hurwitz spaces. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Sémin. Congr.*, pages 313–341. Soc. Math. France, Paris, 2006.

Goro Shimura. On the field of rationality for an Abelian variety. *Nagoya Math. J.*, 45:167–178, 1972. ISSN 0027-7630. doi: 10.1017/S0027763000014720.