On the fields of definition of genus-one covers of $\mathbb{P}^1$

Alexander Molyakov

Département de Mathématiques et Applications, École Normale Supérieure, Paris, France

Correspondence
Alexander Molyakov, Département de Mathématiques et Applications, École Normale Supérieure, 45 rue d’Ulm 75005 Paris, France.
Email: amolyakov1@gmail.com

Abstract
It is known that sometimes, a Belyi pair is not defined over its field of moduli. Instead, it is defined over a finite degree extension of its field of moduli, called a field of definition. We show that given a number $m$, there exists a Belyi pair such that the degree of a field of definition over the field of moduli is greater than $m$. As a by-product, we obtain a counterexample to the local-global principle for Belyi pairs.

MSC 2020
11G32, 14H30 (primary), 11G05, 12F10 (secondary)

1 | INTRODUCTION

The theory of covers of the projective line has been rapidly developing over the last 40 years. Covers unramified outside $\{0, 1, \infty\}$ are called Belyi functions, they are of special interest due to applications to the inverse Galois problem. The famous Belyi theorem asserts that a complex curve $X$ is defined over $\overline{\mathbb{Q}}$ if and only if there exists a Belyi function $\beta : X \to \mathbb{P}^1$ [1]. The category of Belyi pairs $(X, \beta)$ is equivalent to the category of dessins d’enfants, graphs embedded into surfaces in a particular way [18, p.188, Theorem]. Thus, the natural Galois-action on Belyi pairs induces a Galois-action on the set of dessins, which turns out to be exact.

The absolute field of moduli of a (ramified) cover $X \to \mathbb{P}^1$ is the fixed field of its stabilizer with respect to the natural action of the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Clearly, it is contained in each field of definition. Covers without automorphisms as well as regular covers are known to be defined over their field of moduli [7]. In fact, covers defined over the field of moduli form a Zariski-dense subset of the corresponding Hurwitz space [9]. However, there are examples of covers (and even of Belyi pairs) not defined over the field of moduli [3, 5, 12]. The examples presented in these papers give us covers that are defined over quadratic extensions of the corresponding field of moduli. It turns out that any cover of genus 0 is defined over a quadratic extension [3]. We
deal with the genus-one case where, as we show, the degree of a minimal field of definition over the field of moduli can be arbitrary large. Precisely, we prove the following result that appears as Theorem 2 below.

**Theorem.** Let $E$ be a non-CM elliptic curve over $\overline{\mathbb{Q}}$ and let $m$ be a positive integer. Then there exists a Belyi function $\beta : E \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ with the absolute field of moduli $M_{\text{abs}}$ and the following property: for any field of definition $L$ of the Belyi pair $(E, \beta)$, we have $[L : M_{\text{abs}}] \geq m$.

The construction proceeds as follows: using the idea of a reduced cover [10], models of the initial cover can be put in one-to-one correspondence with models of the regular cover $E \to E/\text{Aut}(E, \beta)$. The regular cover turns out to be an isogeny in the case we are interested. Afterward some analysis of cohomological obstructions demonstrates the existence of an isogeny with prescribed properties. Finally, the refined version of Belyi theorem from [4] is applied to complete the construction.

The cohomological obstructions for a field of moduli being a field of definition were introduced by P. Débes and J.-C. Douai in a more general context of arbitrary algebraic covers [7]. This obstruction consists of a family of elements in $H^2(G_M, C(\text{Aut}(X, f)))$ where $G_M$ is the absolute Galois group of a field of moduli $M$ and $C(\text{Aut}(X, f))$ stands for the center of the automorphisms group of a cover $(X, f)$. However, even in the case of covers with an abelian group of automorphisms when the obstruction reduces to a single element, it is generally unclear which elements in the cohomology group arise in this way. This makes constructing examples by means of purely cohomological techniques more difficult. The key observation in the genus-one case is that under some assumptions, each element of $H^2(G_M, E[m])$ appears as an obstruction for a Belyi pair (Lemma 3).

Our approach can also be applied to produce counterexamples to the Hasse principle for Belyi pairs in the following sense (see Corollary 5 below).

**Theorem.** There exists a genus-one Belyi pair $(X, f)$ over $\overline{\mathbb{Q}}$ which cannot be defined over its field of moduli $M$, yet which can be defined over the completion $M_\nu$ for all places $\nu$ of $M$.

While the local-to-global problem has a positive answer for $G$-covers with an exception of the special case of Grunwald–Wang theorem [7, 8], the Hasse principle fails to be true for mere covers. Though a counterexample is presented in [6], counterexamples for Belyi pairs seem to be absent in the literature. The method we use to obtain these examples does not immediately lead to explicit formulas but it is effective and appears to be computable in practice.

I would like to thank G. Shabat and other participants of the seminar “Graphs on surfaces and curves over number fields” for helpful discussions, fruitful remarks, and encouraging interest in the subject. I am also grateful to J.-M. Couveignes for his comments that helped to improve the exposition and to S. Gorchinskiy for pointing out to me the folklore fact that is stated as Proposition 5 below.

## 2 | PRELIMINARIES

### 2.1 | Base change and descent

**Notation.** Let $\mathbf{Sch}_L$ be the category of schemes over a field $L$. 
To an automorphism \( g : L \to L \), we can associate a base change functor \( g_* : \text{Sch}_L \to \text{Sch}_L \) which is defined as follows: for an \( L \)-scheme \( X \) with a structure morphism \( \psi : X \to \text{Spec}(L) \), the object \( g_*X \) is the scheme \( X \) with a modified structure morphism \( (g^*)^{-1} \circ \psi : X \to \text{Spec}(L) \) where \( g^* : \text{Spec}(L) \to \text{Spec}(L) \) is the automorphism induced by \( g \). In other words, \( g_* \) is the pullback functor \( \text{Sch}_L \to \text{Sch}_L \) under the map \( g^* : \text{Spec}(L) \to \text{Spec}(L) \).

If \( X \in \text{Sch}_K \) is a scheme given over a smaller field \( K \subset L \), then \( X_L \) stands for the \( L \)-scheme \( X \times_{\text{Spec}(K)} \text{Spec}(L) \), which is the extension of constants. By abuse of notations, we also write \( X_K \) for a \( K \)-model of a scheme \( X \) over the larger field \( L \) when it leads to no confusion.

We recall that when \( L \supset K \) is a Galois extension, \( X_L \) admits a descent datum consisting of a family of \( L \)-isomorphisms \( \rho_X(g) : \ g_*X_L \to X_L \) for each \( g \in \text{Gal}(L/K) \) satisfying the cocycle condition \( \rho_X(gh) = \rho_X(g) \circ \rho_X(h) \) [13, (14.17.1)]. A morphism of \( L \)-schemes with descent data is an \( L \)-morphism \( f : X \to Y \) compatible with the descent data in the sense that \( f \circ \rho_X(g) = \rho_Y(g) \circ g_*f \).

The category of quasi-projective varieties admits an effective Galois descent [13, Theorem 14.86]. This fact can be stated as follows:

**Fact 1.** Let \( K \subset L \) be a finite Galois extension. Then the category of quasi-projective varieties over \( L \) with descent data is equivalent to the category of quasi-projective varieties over the smaller field \( K \) where the functor in one direction is an extension of constants.

For another treatment of Galois descent in the classical language of algebraic varieties, see [15, Corollary 16.25] and the foundational paper of Weil [19].

### 2.2 Covers of curves and their fields of moduli

We will use the following notations and assumptions throughout this paper: all curves are assumed to be smooth, proper, and geometrically integral; we also fix a base field \( K \) of characteristic zero and a Galois extension \( F \supset K \); all fields are assumed to contain \( K \) and to be contained in \( F \).

**Definition 1.** Consider a curve \( B \) over a field \( L, K \subset L \subset F \).

(i) The category of (ramified) covers of \( B \) consists of pairs \( (X, f) \) where \( f : X \to B \) is a surjective \( L \)-morphism of curves over \( L \).

(ii) A morphism of covers \( h : (X_1, f_1) \to (X_2, f_2) \) is a morphism \( h : X_1 \to X_2 \) such that \( f_2 \circ h = f_1 \). In particular, an automorphism of a cover \( f : X \to B \) is an automorphism \( \sigma \in \text{Aut}(X) \) such that \( f \circ \sigma = f \).

There is a natural action of \( \text{Gal}(F/L) \) on the category of covers \( f : X \to B_F \). It is defined as follows:

\[
g_*(X, f) = \left( g_*X, \rho_B(g) \circ g_*f \right).
\]

Note that this action depends on the chosen \( L \)-model \( B \).

In the following proposition, a pointed cover is a surjective morphism of curves \( f : X \to B \) with marked rational points \( Q \in X, P \in B \) such that \( f(Q) = P \).
**Proposition 1.** Consider a finite Galois extension \( M \subset F \), a curve \( B \) over \( M \), and a (pointed) cover \( f : X \to B_F \). Then the cover \((X, f)\) admits a (pointed) \( M \)-model if and only if there exists a family of (pointed) cover isomorphisms \( \rho(g) : g_* (X, f) \to (X, f) \) defined for each \( g \in \text{Gal}(F/M) \) and satisfying the cocycle condition

\[
\rho(gh) = \rho(g) \circ g_* \rho(h).
\]

Furthermore, any such family of isomorphisms \( \{\rho(g)\}_g \) satisfying (1) defines a unique (pointed) \( M \)-model of the cover \((X, f)\).

**Proof.** This statement follows from the effective Galois descent for the category of quasi-projective varieties (Fact 1) because all curves are quasi-projective. A rational point on a curve over \( F \) can be viewed as a morphism from the one-point scheme \( \text{Spec}(F) \). Thus, in the case of pointed covers, it suffices to apply Galois descent to the following diagram:

\[
\begin{align*}
\xymatrix{
X \ar[dr]_f & \\
\text{Spec}(F) \ar[r]^P & B_F
}
\end{align*}
\]

**Definition 2.** Let \( B \) be a curve over \( K \).

(i) The absolute field of moduli of a cover \( f : X \to B_F \) is the fixed field \( F^{\text{Stab}(f)} \) where the stabilizer is taken with respect to the above action of \( \text{Gal}(F/K) \) on the set of equivalence classes of covers. We also use the notion of a relative field of moduli for any field containing the absolute field of moduli (“a field of moduli” will always refer to this case).

(ii) We say that \( f \) is defined over a field \( L \subset F \) if there exists an \( L \)-model \( f_L : X_L \to B_L \) isomorphic to \((X, f)\) over \( F \). In this case, \( L \) is called a field of definition.

In other words, a field \( M \) is said to be a field of moduli of a cover \( f : X \to B_F \) if \((X, f)\) is isomorphic to \( g_* (X, f) \) for each \( g \in \text{Gal}(F/M) \).

The two concepts we have just introduced are in the following relation as was demonstrated in [7].

**Proposition 2.**

(i) Every field of definition is a field of moduli.

(ii) The absolute field of moduli of a cover over \( \overline{\mathbb{Q}} \) is the intersection of all fields of definition. In particular, if there exists a minimal (by inclusion) field of definition, it coincides with the field of moduli.

The first part of Proposition 2 implies that the absolute field of moduli is a finite extension of \( K \). Indeed, every cover over \( F \) can be defined over a finite subextension \( L \supset K \) and the absolute field of moduli is contained in \( L \).

For some types of covers, a field of moduli is a field of definition.
Proposition 3. Let $B$ be a curve over $K$. Consider a cover $f : X \to B_F$ with a field of moduli $M$.

(i) If $\text{Aut}(X, f) = \{\text{id}\}$, then $(X, f)$ has a unique $M$-model.
(ii) If the cover $f$ is regular (i.e., $\text{Aut}(X, f)$ acts transitively on the fiber of a noncritical $F$-point) and $B$ has a noncritical $M$-point $P$, $f$ is defined over $M$. Assume furthermore that $X$ has an $F$-point $Q$ over $P$. Then $f$ has a unique $M$-model $X_M \to B_M$ such that $X_M$ possesses an $M$-point over $P$.

Proof (See also [7]). Without loss of generality, we may assume that $[F : K] < \infty$ since the infinite case reduces to the finite one as all covers over $F$ are defined over some finite subextension.

(i) If $f$ has no nontrivial automorphisms, there is a unique isomorphism of covers $\tilde{g} \cdot (X, f) \to (X, f)$ for each $g \in \text{Gal}(F/M)$. It satisfies the cocycle condition (1) because of the uniqueness and therefore gives a unique $M$-model of $f$ by Proposition 1.

(ii) Now suppose $f$ is regular and $P \in B(M)$ is noncritical. Choose an arbitrary geometric point $Q \in f^{-1}(P)$. Regularity of $f$ implies that for each $g \in \text{Gal}(F/M)$, there exists a unique isomorphism of covers $\rho : g \cdot (X, f) \to (X, f)$ such that $\rho(g, Q) = Q$. Similarly, this system of isomorphisms satisfies the cocycle condition (1) because of the uniqueness and defines an $M$-model of $f$ by Proposition 1. If furthermore $Q \in X(F)$, $(X, Q, f)$ is a pointed cover and there exists a unique isomorphism of pointed covers $g \cdot (X, Q, f) \to (X, Q, f)$ for each $g \in \text{Gal}(F/M)$. Applying Proposition 1 for pointed covers, we obtain a unique pointed $M$-model $X_M \to B_M$. □

Note that the last assumption of Proposition 3(ii) always holds if $F = \overline{K}$ is algebraically closed. In fact, the condition that the point $P$ in Proposition 3(ii) is noncritical can be weakened, see [17] for a more general result.

Proposition 4. Let $B$ be a curve over $K$. Consider a cover $f : X \to B_F$ with a field of moduli $M$. Then the following holds true:

(i) The cover can be decomposed as $f = f_0 \circ f_{\text{reg}}$ where $f_{\text{reg}} : X \to X/\text{Aut}(X, f)$ is the canonical projection and $f_0 : X/\text{Aut}(X, f) \to B$ is uniquely defined.
(ii) There exists a canonical $M$-model $X_0 \to B$ of $f_0$.
(iii) $M$ is a field of moduli of $f_{\text{reg}}$, the initial cover $f_0$ is defined over $M$ iff $f_{\text{reg}}$ has an $M$-model with the base $X_0$.

We call $(X_0, f_0)$ and $(X, f_{\text{reg}})$ the reduced and regular part of the cover $(X, f)$, respectively.

This result is stated in [10, Theorem 3.3]. Although the authors provide a complete proof only for a similar statement about curves, the case of covers can be established in the same manner. Here is a sketch of the proof.

Proof. We may restrict ourselves to the case of finite degree $[F : K] < \infty$ as in the proof of Proposition 3.

(i) Obvious.
(ii) Given an element $g \in \text{Gal}(F/M)$, we want to consider an isomorphism of covers

$$\tilde{\rho}(g) : g \cdot (X, f) \to (X, f).$$
It induces an isomorphism of the corresponding reduced covers

\[ \rho(g) : g_* (X/\text{Aut}(X, f)) \to X/\text{Aut}(X, f). \]

It is straightforward to check that this isomorphism is independent on the choice of \( \bar{\rho}(g) \) and therefore meets the cocycle condition of Proposition 1.

(iii) It is clear from the proof of (ii) that descent data on \((X, f)\) uniquely correspond to descent data on \((X, f^{\text{reg}})\). Thus, the result follows from Proposition 1. \(\square\)

**Corollary 1.** Using the notations introduced above, let \( L \supset M \) be an extension of the field of moduli such that \( X_0 \) has a noncritical \( L \)-point. Then \( f \) is defined over \( L \).

**Proof.** It follows from Propositions 4 (iii) and 3(ii). \(\square\)

As a consequence of the general results above, we can deduce that genus-zero covers are defined over a quadratic extension of their field of moduli [3, Theorem 5].

**Corollary 2.** Let \( f : \mathbb{P}^1_F \to \mathbb{P}^1_F \) be a cover with a field of moduli \( M \). Then there is an extension \( L \supset M \) such that \( f \) is defined over \( L \) and \([L : M] \leq 2\).

**Proof.** In this case, \( X_0 = \mathbb{P}^1_F/\text{Aut}(\mathbb{P}^1_F, f) \) is a curve of genus 0 over \( M \), and therefore, it has a point over some quadratic extension of \( M \). \(\square\)

### 2.3 The obstruction

In this section, we construct a cohomological obstruction for a cover being defined over its field of moduli. We start with the following folklore construction:

Let \( B \) be a curve over \( K \). Consider a cover \( f : X \to B_F \) with a field of moduli \( M \). Let \( G_{f,M} \) be the set of pairs \((g, \rho)\) where \( g \) is an element of \( \text{Gal}(F/M) \) and \( \rho \) is an isomorphism of covers \( g_*(X, f) \to (X, f) \). The group law on \( G_{f,M} \) is defined as follows:

\[ (g, \rho_1) \cdot (h, \rho_2) = (gh, \rho_1 \circ g_*(\rho_2)). \]

It can be easily checked that \( G_{f,M} \) is indeed a group with respect to this operation. There is a natural projection \( G_{f,M} \to \text{Gal}(F/M) \) whose kernel coincides with the group of automorphisms of \( f \). So, there exists an exact sequence of groups

\[ 1 \to \text{Aut}(X, f) \to G_{f,M} \to \text{Gal}(F/M) \to 1. \]  \hspace{1cm} (2)

**Proposition 5.** In the setting introduced above we assume furthermore that \([F : K] < \infty\). Then the sequence (2) splits iff \((X, f)\) is defined over \( M \).

**Proof.** The map \( G_{f,M} \to \text{Gal}(F/M) \) has a section iff a family of cover isomorphisms \( \rho(g) : g_*(X, f) \to (X, f) \) for each \( g \in \text{Gal}(F/M) \) can be chosen to fit the cocycle condition of Proposition 1. \(\square\)
Proposition 5 allows us to construct a cohomological obstruction for covers with an abelian group of automorphisms. For another cohomological approach in a more general context, see [7].

**Corollary 3.** Let $B$ be a curve over $K$. Consider a cover $f : X \to B_F$ with an abelian group of automorphisms. Then the obstruction for a field of moduli $M$ to be a field of definition is an element $\sigma \in H^2(Gal(F/M), Aut(X, f))$.

In the case of an infinite Galois extension $K \subset F$, Galois cohomology groups should be understood in the profinite sense.

**Proof.** If $K \subset F$ is finite, it is a standard fact that group extensions with abelian kernels are classified by the second cohomology group, see [2, Theorem 3.12]. In the infinite case, the statement follows from the definition of profinite cohomology groups

$$H^2(Gal(F/M), Aut(X, f)) := \lim_{\longrightarrow} H^2(Gal(L/M), Aut_L(X, f)),$$

where the limit is taken over all finite subextensions $L \supset K$.

**Remark 1.** Let $L \supset M$ be a larger field of moduli of the cover $f : X \to B_F$. Then $G_{f,L}$ coincides with the preimage of $Gal(F/L) \subset Gal(F/M)$ under the projection $G_{f,M} \to Gal(F/M)$. In other words, we have a commutative diagram

$$
\begin{array}{cccccc}
1 & \to & Aut(X, f) & \to & G_{f,L} & \to & Gal(F/L) & \to & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \to & Aut(X, f) & \to & G_{f,M} & \to & Gal(F/M) & \to & 1
\end{array}
$$

where the rows are exact and all squares are Cartesian. Hence, the group extension in the first row is the pullback of the group extension in the second row under the map $Gal(F/L) \to Gal(F/M)$. If the group of automorphisms $Aut(X, f)$ is abelian, this property implies that the obstruction $\sigma \in H^2(Gal(F/M), Aut(X, f))$ constructed in Corollary 3 is functorial in the following sense: the image of $\sigma$ under

$$res^M_L : H^2(Gal(F/M), Aut(X, f)) \to H^2(Gal(F/L), Aut(X, f))$$

is precisely the obstruction corresponding to the field of moduli $L$. In particular, the cover $f$ is defined over $L$ if and only if $res^M_L(\sigma) = 0$.

### 3 | COVERS OF GENUS ONE

By a cover of genus one, we understand a cover $X \to \mathbb{P}^1$ where $X$ is a curve of genus one. In this section, we focus on the absolute case $F = \overline{K} \supset K$.

**Notation.** $G_L = Gal(\overline{K}/L)$ is the absolute Galois group of a field $L$. 
Proposition 6. Let $f : X \to \mathbb{P}^1_K$ be a cover of genus one with a field of moduli $M$. Recall that $X_0 = X/\text{Aut}(X, f)$ is the canonical model of the reduced part of $f$ from Proposition 4. Then exactly one of the following holds true:

1. Either $\text{Aut}(X, f)$ acts freely on $X$ and $X_0$ has genus one (in this case, $\text{Aut}(X, f)$ may be viewed as a finite subgroup of the elliptic curve $X$ with a properly chosen basepoint); Or
2. $X_0$ has genus zero and $(X, f)$ is defined over a quadratic extension of $M$.

Proof. Let $d$ be the degree of $f^{\text{reg}}$, let $e_P$ be the ramification index of $f^{\text{reg}}$ at a point $P$, and let $g(X_0)$ stand for the genus. Then by Riemann–Hurwitz formula for $f^{\text{reg}}$

$$d(2 - 2g(X_0)) = \sum_{P \in X} (e_P - 1) \geq 0.$$ 

Hence, we deduce $g(X_0) \in \{0, 1\}$. The cover $f^{\text{reg}}$ is unramified (i.e., $e_P = 1$ at each $P \in X$) if and only if $\text{Aut}(X, f)$ acts on $X$ without fixed points, that is, freely.

If $X_0$ has genus one, the cover is a surjective morphism of genus-one curves which can be viewed as an isogeny of elliptic curves with properly chosen basepoints. Then $\text{Aut}(X, f)$ is the kernel of the corresponding isogeny.

Otherwise the cover is ramified and $X_0$ has genus zero. Then it has a point over a quadratic extension of the field of moduli and the statement follows from Corollary 1 of Proposition 4. □

As we are looking for covers with an arbitrary large degree of a field of definition over the field of moduli, we may restrict ourselves to the first case of Proposition 6. In the rest of this section, we show how the first case of Proposition 6 can be reduced to the lifting of some cohomological class.

Let $C$ be a curve over $\overline{K}$. In order to define an action of the Galois group $\text{Gal}(\overline{K}/M)$ on the category of covers of $C$, we need to fix an $M$-model of $C$ and the resulting action depends on the chosen model. Therefore, the absolute field of moduli of a cover $f : X \to C$ also depends on the chosen $M$-model of $C$. However, we prove that the absolute field of moduli of an isogeny of elliptic curves does not change when the base curve is replaced by any of its torsors.

Lemma 1. Let $E_0$ be an elliptic curve over a field $M$ and let $X_0$ be an $M$-torsor of $E_0$. Let us fix an arbitrary isomorphism of torsors $i : (E_0)_{\overline{K}} \to (X_0)_{\overline{K}}$. Consider an isogeny $\phi : E \to (E_0)_{\overline{K}}$. Then the absolute field of moduli of the cover $i \circ \phi : E \to (E_0)_{\overline{K}}$ coincides with the absolute field of moduli of the cover $i : (E_0)_{\overline{K}} \to (X_0)_{\overline{K}}$.

Proof. We denote the descent datum on $E_0$ by $\rho_{E_0}$. After the identification $i : (E_0)_{\overline{K}} \sim (X_0)_{\overline{K}}$, the descent datum on $E_0$ corresponding to the $M$-torsor $X_0$ has the form $\rho_{X_0}(g) = \rho_{E_0}(g) + \tau_0(g)$ where $\tau_0 \in H^1(\text{Gal}(\overline{K}/M), E_0)$. Let us consider an element $g \in \text{Gal}(\overline{K}/M)$. It is sufficient to demonstrate that $g \circ (E, \phi)$ and $(E, \phi)$ are isomorphic as covers with the $M$-base $E_0$ if and only if they are isomorphic as covers with the $M$-base $X_0$. The first condition is equivalent to the existence of a suitable isomorphism $\rho : g \circ E \to E$ such that the following diagram is commutative:

\[
\begin{array}{ccc}
g \circ E & \xrightarrow{\rho} & E \\
\downarrow g \circ \phi & & \downarrow \phi \\
g \circ E_0 & \xrightarrow{\rho \circ (g)} & E_0
\end{array}
\]
Similarly, the second condition is equivalent to the existence of another suitable isomorphism \( \tilde{\rho} : g_*E \to E \) such that the diagram below is commutative:

\[
\begin{array}{ccc}
g_*E & \xrightarrow{\rho} & E \\
\downarrow{g_*\phi} & & \downarrow{\phi} \\
g_*E_0 & \xrightarrow{\rho_0(g)+\tau_0(g)} & E_0
\end{array}
\] (4)

Let us pick some preimage \( \tau \) of \( \tau_0(g) \) under the isogeny \( \phi \). Then one easily verifies that given any \( \rho \) fitting into (3), \( \tilde{\rho} = \rho + \tau \) fits into (4):

\[
\phi \circ \tilde{\rho} = \phi \circ (\rho + \tau) = \phi \circ \rho + \phi(\tau) = \phi \circ \rho + \tau_0(g) = \rho_{E_0}(g) \circ g_*\phi + \tau_0(g).
\]

Similarly, given \( \tilde{\rho} \) fitting into (4), \( \rho = \tilde{\rho} - \tau \) fits into (3):

\[
\phi \circ \rho = \phi \circ (\tilde{\rho} - \tau) = \phi \circ \tilde{\rho} - \tau_0(g) = \rho_{E_0}(g) \circ g_*\phi + \tau_0(g) - \tau_0(g) = \rho_{E_0}(g) \circ g_*\phi.
\]

Now we prove a technical lemma.

**Lemma 2.** Let \( X_0 \) be a curve of genus one over a field \( M \), and consider a finite map of genus-one curves \( g : X \to (X_0)_{\overline{K}} \). Suppose that \( M \) is its field of moduli. Denote the Jacobian of \( X_0 \) by \( E_0 \). Then there exist an elliptic curve \( E \) over \( M \) and an isogeny \( \phi : E \to E_0 \) defined over \( M \) which is isomorphic to \( g \) over \( \overline{K} \) after an identification of \( (X_0)_{\overline{K}} \) and \( (E_0)_{\overline{K}} \), and the curve \( E \) and the isogeny \( \phi \) are uniquely determined. Moreover, if \( (X, g) \) has an \( M \)-model \( X_M \to X_0 \), then \( E \) is \( M \)-isomorphic to the Jacobian of \( X_M \).

**Proof.** From Lemma 1, we deduce that \( M \) is a field of moduli of \( \phi \) with respect to the \( M \)-base \( E_0 \). Then the first claim follows from Proposition 3(ii).

Let \( g_M : X_M \to X_0 \) be an \( M \)-model, we may consider the induced map on Jacobians \( J(X_0) \to J(X_M) \). It is defined over \( M \). Then the dual isogeny \( J(X_M) \to J(X_0) = E_0 \) is also defined over \( M \) and is isomorphic to \( (X, g) \) over \( \overline{K} \). From the uniqueness part of the first claim, it follows that \( J(X_M) \) is isomorphic to \( E \) over \( M \). 

Let \( f : X \to \mathbb{P}^1_{\overline{K}} \) be a cover of genus 1 with a field of moduli \( M \). We assume that \( \text{Aut}(X, f) \) acts freely on \( X \). The genus-one curve \( X_0 \) is defined over \( M \). Now we can apply Lemma 2 to obtain an \( M \)-isogeny of elliptic curves \( \phi : E \to E_0 = J(X_0) \), which is isomorphic to \( f_{\text{reg}} \) over \( \overline{K} \). Then there is an exact triple of \( G_M \)-modules:

\[
0 \to \text{Aut}(f) \to E \overset{\phi}{\to} E_0 \to 0.
\]

It induces an exact sequence of Galois cohomology groups

\[
H^1(G_M, E) \to H^1(G_M, E_0) \overset{\delta}{\to} H^2(G_M, \text{Aut}(f)).
\]
Proposition 7. In the setting introduced above, there is a canonically defined class \( \tau_0 \in H^1(G_M, E_0) \). The cover is defined over \( M \) if and only if \( \tau_0 \) can be lifted to \( \tau \in H^1(G_M, E) \). The image of \( \tau_0 \) under the boundary map \( \delta \) coincides with the obstruction of Corollary 3.

Proof. The class \( \tau_0 \in H^1(G_M, E_0) \) corresponds to \( X_0 \) which forms a principal homogeneous space of its Jacobian \( J(X_0) = E_0 \). Let \( \rho_E, \rho_{E_0} \) be the descend data corresponding to \( E, E_0 \). Then \( X_0 \) is defined by the descend datum \( \rho_{E_0} + \tau_0 \). If the cover \( f^\text{reg} \) has an \( M \)-model \( X_M \rightarrow X_0 \), we already know that \( E \) is the Jacobian of \( X_M \) (Lemma 2), so \( X_M \) is a torsor of \( E \) defined by a descend datum of the form \( \rho_E + \tau \) where \( \tau \in H^1(G_M, E) \). The cover \( f^\text{reg} \) should be compatible with the descent data. In other words, the following diagram is commutative:

\[
\begin{array}{ccc}
E & \xrightarrow{\phi} & E_0 \\
g^*E & \xrightarrow{\rho_E(g)+\tau(g)} & E \\
g^*E_0 & \xrightarrow{\rho_{E_0}(g)+\tau_0(g)} & E_0
\end{array}
\]

This means that the following equality holds for any \( x \in g^*E, g \in G_M \):

\[
\phi(\rho_E(g)(x) + \tau(g)) = \rho_{E_0}(g^*\phi(x)) + \tau_0(g).
\] (5)

Since \( \phi : E \rightarrow E_0 \) is defined over \( M \), it is compatible with \( \rho_E, \rho_{E_0} \), that is,

\[
\phi \circ \rho_E(g) = \rho_{E_0} \circ g^* \phi.
\] (6)

Hence, (5) is equivalent to the equality \( \phi(\tau(g)) = \tau_0(g) \). The latter equality implies that \( \tau_0 \) is the image of \( \tau \) under the map \( H^1(G_M, E) \rightarrow H^1(G_M, E_0) \).

The image of \( \tau_0 \) in \( H^2(G_M, \text{Aut}(f)) \) corresponds to the exact sequence

\[
0 \longrightarrow \text{Aut}(f) \longrightarrow G_M \times_{\tau_0} E \longrightarrow G_M \longrightarrow 0,
\]

where \( G_M \times_{\tau_0} E = \{(g, p) \in G_M \times E | \tau_0(g) = \phi(p)\} \). We need to show that this group coincides with \( G_{f,M} \) from the exact sequence (2). It suffices to verify that the condition \( \tau_0(g) = \phi(p) \) is equivalent to the fact that \( \rho_E(g) + p : g^*E \rightarrow E \) is an isomorphism of covers \( g^*E, \phi) \rightarrow (E, \phi) \). Indeed, \( \rho_E(g) + p \) is an isomorphism of covers when the following compatibility condition holds for any \( x \in g^*E \) (cf. the diagram above)

\[
\phi(\rho_E(g)(x) + p) = \rho_{E_0}(g^*\phi(x)) + \tau_0(g).
\]

From (6), we deduce that the latter is equivalent to \( \phi(p) = \tau_0(g) \).

\[ \square \]

4 | THE MAIN CONSTRUCTION

The aim of this section is to construct examples of Belyi functions such that the degree of a minimal field of definition over the field of moduli is large. In the previous section, we have seen that the problem of defining a genus-one cover over the field of moduli reduces to some isogeny
of elliptic curves. Here, we consider the case of the simplest isogeny, namely, multiplication by \(m\). First, we show that under some assumptions on a finite subgroup \(C\) of an elliptic curve \(E\), an element in \(H^2(G_M, C)\) can be obtained as the obstruction of Corollary 3. Then we demonstrate the existence of an appropriate element in \(H^2(G_M, E[m])\), which does not split over extensions of small degree.

The base field \(K\) is assumed to be a number field, \(K \subset F = \overline{Q}\). We need a fact from arithmetic geometry [16, Corollary 6.24, Corollary 3.4].

**Proposition 8.** For any elliptic curve \(E\) over a number field \(M\), there is a functorial isomorphism

\[
H^2(G_M, E) \xrightarrow{\sim} \prod_{\nu \text{ real}} H^2(G_{M_{\nu}}, E),
\]

where \(\nu\) runs through all real places of \(M\). For real places \(\nu\), we have

\[
H^2(G_{M_{\nu}}, E) = \begin{cases} 
\mathbb{Z}/2\mathbb{Z} & \text{if } \Delta(E) > 0 \\
0 & \text{if } \Delta(E) < 0.
\end{cases}
\]

**Corollary 4.** Consider an \(M\)-isogeny \(\phi : E \to E_0\) of elliptic curves over \(M\) such that \(\deg(\phi)\) is odd. Then it induces an isomorphism

\[
H^2(G_M, E) \to H^2(G_M, E_0).
\]

**Proof.** It is sufficient to show that \(\phi\) induces an isomorphism

\[
H^2(G_{M_{\nu}}, E) \to H^2(G_{M_{\nu}}, E_0)
\]

at each real place \(\nu\). Denote the dual isogeny by \(\hat{\phi} : E_0 \to E\). The composition \(\hat{\phi} \circ \phi\) induces a composite map

\[
H^2(G_{M_{\nu}}, E) \to H^2(G_{M_{\nu}}, E_0) \to H^2(G_{M_{\nu}}, E),
\]

which is the multiplication by an odd integer \(\deg(\phi)^2\). Therefore, it is an isomorphism. Similarly, the other composition \(\phi \circ \hat{\phi}\) induces an isomorphism. Then the first arrow is also an isomorphism since all the cohomology groups are either trivial or cyclic of order 2. \(\square\)

Recall that a Belyi function is a surjective morphism \(\beta : X \to \mathbb{P}^1\) unramified outside \(\{0, 1, \infty\}\), the cover \((X, \beta)\) is also called a Belyi pair. We quote a refined version of Belyi theorem from [4, p.2, Théorème] which we use to prove the key lemma below.

**Theorem 1.** For each curve \(X\) over a number field \(M\), there exists a Belyi function \(\beta : X \to \mathbb{P}^1_M\) over \(M\) such that \(\text{Aut}(X, \beta) = \{\text{id}\}\).

Recall that a non-CM elliptic curve is an elliptic curve \(E\) which does not have a complex multiplication or equivalently \(\text{End}(E) = \mathbb{Z}\). A \(G_M\)-submodule of an elliptic curve \(E\) over a field \(M\) is a subgroup \(C \subset E\), which is preserved by the action of \(G_M\), that is, \(gC \subset C\) for all \(g \in G_M\).
Lemma 3. Let $E$ be a non-CM elliptic curve over a number field $M$ and let $C \subset E$ be a finite subgroup such that $C$ is a $G_M$-submodule of $E$. Assume that at least one of the following holds true:

(i) The order of $C$ is odd.
(ii) The field $M$ is purely imaginary.

Then for each element $\sigma \in H^2(G_M, C)$, there exists a Belyi map $\beta : E_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\mathbb{Q}}$ with a field of moduli $M$ having $\sigma$ as the obstruction constructed in Corollary 3.

Proof. Let us denote the quotient curve $E/C = E_0$. It is defined over $M$ because $C$ is a $G_M$-submodule of $E$. Then the exact sequence of $G_M$-modules

$$0 \longrightarrow C \longrightarrow E \longrightarrow E_0 \longrightarrow 0$$

induces a long exact sequence

$$H^1(G_M, E) \longrightarrow H^1(G_M, E_0) \overset{\delta}{\longrightarrow} H^2(G_M, C) \longrightarrow H^2(G_M, E) \longrightarrow H^2(G_M, E_0).$$

In the case of an odd order of $C$, the latter arrow is an isomorphism by Corollary 4. Therefore, the boundary map $\delta$ is surjective. If $M$ is purely imaginary $H^2(G_M, E) = 0$ by Proposition 8, so $\delta$ is also surjective.

Choose $\sigma \in H^2(G_M, C)$ and lift it to an element $\tau_0 \in H^1(G_M, E_0)$. Then the element $\tau_0$ defines a principal homogeneous space $X_0$ of the elliptic curve $E_0$ over $M$.

Applying Theorem 1 to $X_0$, we obtain a Belyi map $\beta_0 : X_0 \to \mathbb{P}^1_M$ without nontrivial automorphisms. We next want to consider the composition $\beta = (\beta_0)_\overline{\mathbb{Q}} \circ \phi_{\overline{\mathbb{Q}}}$ where $\phi$ is the isogeny $E \to E_0$:

$$\beta : E_{\overline{\mathbb{Q}}} \overset{(\phi)_{\overline{\mathbb{Q}}}}{\longrightarrow} (E_0)_{\overline{\mathbb{Q}}} \sim (X_0)_{\overline{\mathbb{Q}}} \overset{(\beta_0)_{\overline{\mathbb{Q}}}}{\longrightarrow} \mathbb{P}^1_{\overline{\mathbb{Q}}}.$$ 

(We identify $(E_0)_{\overline{\mathbb{Q}}}$ with $(X_0)_{\overline{\mathbb{Q}}}$.) First note that $\beta$ is a Belyi function over $\overline{\mathbb{Q}}$ because $\phi$ is an unramified cover.

Let $h : E \to E$ be an automorphism of $\beta$. Since $E$ is non-CM, $h$ has the form $h(x) = \varepsilon \cdot x + a$ where $\varepsilon \in \{+1, -1\}, a \in E$. Then we deduce

$$\beta_0(\phi(x)) = \beta_0(\phi(\varepsilon x + a)) = \beta_0(\varepsilon \phi(x) + \phi(a)).$$

Therefore, $\varepsilon \cdot x + \phi(a)$ is an automorphism of $\beta_0$. Consequently, $\varepsilon = 1, \phi(a) = 0$ since $\beta_0$ is automorphisms free. Hence, $\text{Aut}(X, \beta) = \ker(\phi)$ and $\beta_0$ is the reduced part of $\beta$.

To see that $\beta$ fits our requirements, we only have to check that $M$ is a field of moduli of $\beta$. Since $M$ is a field of moduli (and even a field of definition) of $\phi$, Lemma 1 implies that $M$ is a field of moduli of $\phi$ with respect to the $M$-base $X_0$. Therefore, $M$ is a field of moduli of $\beta$ since $\beta_0 : X_0 \to \mathbb{P}^1_M$ is defined over $M$. 

\[\square\]

Proposition 9. Consider an elliptic curve $E$ over a number field $M$. Assume that $E[m] \subset E(M)$ and $\zeta_m \in M$ for a positive integer $m$ where $\zeta_m$ is a primitive $m$th root of unity. Then there exists an element $\sigma \in H^2(G_M, E[m])$ such that $\text{res}_L^M(\sigma) \neq 0$ for all $L \supset M$ with $[L : M] < m$. 

Proof. Under the hypothesis of the proposition, we have an isomorphism of $G_M$-modules

$$E[m] \cong \mu_m \times \mu_m$$

as both of them have trivial Galois action. In particular,

$$H^2(G_M, E[m]) \cong H^2(G_M, \mu_m) \times H^2(G_M, \mu_m).$$

The Kummer exact sequence

$$1 \longrightarrow \mu_m \longrightarrow \bar{K}^* \stackrel{m}{\longrightarrow} \bar{K}^* \longrightarrow 1$$

together with Hilbert 90 theorem lead to a canonical isomorphism

$$H^2(G_M, \mu_m) \sim \text{Br}(M)[m].$$

Therefore, it is sufficient to find an element in $\text{Br}(M)[m]$, which does not split over extensions of degree less than $m$. For example, one can take a cyclic algebra of order $m$ [14].

We are now ready to prove our first main result.

**Theorem 2.** Let $E$ be a non-CM elliptic curve over $\mathbb{Q}$ and let $m$ be a positive integer. Then there exists a Belyi function $\beta : E \to \mathbb{P}^1_{\mathbb{Q}}$ with the absolute field of moduli $M^{ab}$ and the following property: for any field of definition $L$ of the Belyi pair $(E, \beta)$, we have $[L : M^{ab}] \geq m$.

**Proof.** We may assume that $m$ is odd. The curve $E$ is defined over some number field $K$. Consider the field $M = K(E[m], \zeta_m)$. Apply Proposition 9 to get an element $\sigma \in H^2(G_M, E[m])$ which does not split over extensions of degree less than $m$. According to Lemma 3, $\sigma$ arises as an obstruction for some Belyi function $\beta : E_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$. Let $M^{ab}$ be the absolute field of moduli of $\beta$. Then $M^{ab}$ is contained in $M$ by definition. If $\beta$ is defined over an extension $L \supset M^{ab}$, then $\sigma$ vanish when restricted to $ML$. Therefore, we conclude

$$[L : M^{ab}] \geq [ML : M] \geq m.$$  \qed

## 5 A COUNTEREXAMPLE TO THE HASSE PRINCIPLE

Using the cohomological approach from the previous section, one may construct a Belyi pair defined everywhere locally though not globally.

**Definition 3.** Let $M$ be a number field and let $W$ be a $G_M$-module. We define the $i$th Tate–Shafarevich group of $W$ as the kernel of the corresponding local-global map:

$$\text{III}^i(G_M, W) = \ker \left( H^i(G_M, W) \to \prod \nu H^i(G_{M, \nu}, W) \right),$$

where the product is taken for all places $\nu$.  \qed
Theorem 3. Let $M$ be a number field, let $E$ be a non-CM elliptic curve over $M$, and let $m$ be a positive integer such that $m$ is odd or $M$ is purely imaginary. Additionally, assume that $\text{III}^1(G_M, E[m]) \neq 0$. Then there exists a Belyi function $\beta : E_{\mathbb{Q}} \rightarrow \mathbb{P}^1_{\mathbb{Q}}$ with a field of moduli $M$ such that $\beta$ is defined over $M_\nu$ for all places $\nu$ and $\beta$ is not defined over $M$.

Proof. By global Tate duality [16, Theorem 4.10], $\text{III}^2(G_M, E[m])$ is dual to $\text{III}^1(G_M, E[m])$, and therefore, it is nontrivial. Let us pick a nonzero element $\sigma \in \text{III}^2(G_M, E[m])$. By Lemma 3, it arises as an obstruction for some Belyi function $\beta : E_{\mathbb{Q}} \rightarrow \mathbb{P}^1_{\mathbb{Q}}$. Note that $\text{res}_\nu(\sigma) = 0$ is the obstruction corresponding to the local cover $(E_{K_\nu}, \beta_{K_\nu})$. So, $\beta$ is defined over $M_\nu$ for all places $\nu$; however, it is not defined over $M$. □

A numerical example. We present an example when the conditions of Theorem 3 are satisfied. The exact sequence

$$0 \longrightarrow E[m] \longrightarrow E \overset{m}{\longrightarrow} E \longrightarrow 0$$

induces a canonical injection

$$H^0(G_M, E/mE) = E(M)/mE(M) \hookrightarrow H^1(G_M, E[m]).$$

Therefore, $\text{III}^0(G_M, E/mE) \neq 0$ would imply $\text{III}^1(G_M, E[m]) \neq 0$. In [11], the authors provide the following example: a non-CM elliptic curve

$$E : y^2 = (x + 2795)(x - 1365)(x - 1430)$$

has a point

$$P = \left( \frac{5086347841}{1848^2}, -\frac{35496193060511}{1848^3} \right) \in E(\mathbb{Q})$$

such that $P$ is divisible by 4 at all places $\nu$ of $\mathbb{Q}$ but $P$ cannot be divided by 4 over $\mathbb{Q}$. In other words, $P$ gives a nontrivial class $[P] \in \text{III}^0(G_{\mathbb{Q}}, E/4E)$. Note that $\text{res}_{M_\nu}^M[P] \neq 0$ for some purely imaginary number field $M$. For instance, one can take any imaginary $M$ linearly disjoint from $\mathbb{Q}(P/4)$. Then the triple $(M, E, 4)$ fits the requirements.

Corollary 5. There exists a genus-one Belyi pair $(X, f)$ over $\overline{\mathbb{Q}}$ which cannot be defined over its field of moduli $M$, yet which can be defined over the completion $M_\nu$ for all places $\nu$ of $M$.
REFERENCES

1. G. V. Belyi, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), 267–276, 479.
2. K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer, New York-Berlin, 1982.
3. J.-M. Couveignes, *Calcul et rationalité de fonctions de Belyi en genre 0*, Ann. Inst. Fourier (Grenoble) **44** (1994), no. 1, 1–38.
4. J.-M. Couveignes, *À propos du théorème de Belyi*, J. Théor. Nombres Bordeaux **8** (1996), no. 1, 93–99.
5. J.-M. Couveignes and L. Granboulan, *Dessins from a geometric point of view*, The Grothendieck theory of dessins d’enfants (Luminy, 1993), pp. 79–113.
6. J.-M. Couveignes and N. Ros, *Des obstructions globales à la descente des revêtements*, Acta Arith. **114** (2004), no. 4, 331–348. London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, Cambridge, 1994.
7. P. Débes and J.-C. Douai, *Algebraic covers: field of moduli versus field of definition*, Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338.
8. P. Débes and J.-C. Douai, *Local-global principles for algebraic covers*, Israel J. Math. **103** (1998), 237–257.
9. P. Débes, J.-C. Douai, and L. Moret-Bailly, *Descent varieties for algebraic covers*, J. Reine Angew. Math. **574** (2004), 51–78.
10. P. Débes and M. Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56.
11. R. Dvornicich and U. Zannier, *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Math. Acad. Sci. Paris **338** (2004), no. 1, 47–50.
12. V. O. Filimonenkov and G. B. Shabat, *Fields of definition of rational functions of one variable with three critical values*, Fundam. Prikl. Mat. **1** (1995), no. 3, 781–799.
13. U. Görtz and T. Wedhorn, *Algebraic Geometry I: Schemes with examples and exercises*, 2nd ed., Springer Studium Mathematik—Master, Springer Spektrum, Wiesbaden, 2020, pp. vii+625.
14. J. S. Milne, *Class field theory*, Course notes (unpublished). Available at https://www.jmilne.org/math/ CourseNotes/CFT.pdf
15. J. S. Milne, *Algebraic geometry, descent theory*, Course notes (unpublished). Available at https://www.jmilne. org/math/CourseNotes/AG16.pdf
16. J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006, pp. viii+339.
17. J. Sijsling and J. Voight, *On explicit descent of marked curves and maps*, Res. Number Theory, **2** (2016), no. 27, pp. 35.
18. G. Shabat, *Calculating and drawing Belyi pairs*, J. Math. Sci. (N.Y.) **226** (2017), no. 5, 667–693.
19. A. Weil, *The field of definition of a variety*, Am. J. Math. **78** (1956), no. 3, 509–524.