ON EXPLICIT DESCENT OF MARKED CURVES AND MAPS

JEROEN SIJSLING AND JOHN VOIGHT

Abstract. We revisit a statement of Birch that the field of moduli for a marked three-point ramified cover is a field of definition. Classical criteria due to Dèbes and Emsalem can be used to prove this statement in the presence of a smooth point, and in fact these results imply more generally that a marked curve descends to its field of moduli. We give a constructive version of their results, based on an algebraic version of the notion of branches of a morphism and allowing us to extend the aforementioned results to the wildly ramified case. Moreover, we give explicit counterexamples for singular curves.

In his *Esquisse d'un Programme* [12], Grothendieck embarked on a study of $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$, the absolute Galois group of $\mathbb{Q}$, via its action on a set with a geometric description: the set of finite morphisms $f : X \to \mathbb{P}^1$ of smooth projective curves over $\overline{\mathbb{Q}}$ unramified away from $\{0, 1, \infty\}$, known as Belyĭ maps. The heart of this program is to understand over what number fields a Belyĭ map is defined and when two Galois-conjugate Belyĭ maps are isomorphic. One of the more subtle aspects of this investigation is the issue of *descent*: whether or not a Belyĭ map is defined over its field of moduli, which is then necessarily a minimal field of definition. Some concrete descent problems were studied by Couveignes [6] and Couveignes–Granboulan [7]; a more general theoretical approach to the subject of descent of (maps of) curves was developed by Dèbes–Douai [8] and Dèbes–Emsalem [9].

By the classical theory of Weil descent, a Belyĭ map with trivial automorphism group descends to its field of moduli. As such, one typically tries to eliminate descent obstructions by a simple rigidification that eliminates as many non-trivial automorphisms as possible. In his article on dessins, Birch claims [3, Theorem 2] that by equipping a Belyĭ map $f : X \to \mathbb{P}^1$ with a point $P \in X(\overline{\mathbb{Q}})$ satisfying $f(P) = \infty$, the marked tuple $(X, f; P)$ descends to its field of moduli [3, Theorem 2]. Birch provides several references to more general descent results, but upon further reflection we could not see how these implied his particular statement. Obtaining a proof or counterexample was not merely of theoretical importance: indeed, in order to determine explicit equations for Belyĭ maps, one needs a handle on their field of definition [28, §7]. Moreover, if the descent obstruction indeed vanishes, then it is desirable to have general methods to obtain an equation over the field of moduli. The issue under consideration is therefore also very relevant for practical purposes—whence our interest in the problem.

Fortunately, it turned out that general results of Dèbes–Emsalem [9, §5] imply that a marked projective curve $(X; P)$ descends to its field of moduli as long as the marked point P is *smooth*, something that holds by definition for a Belyĭ map $f : X \to \mathbb{P}^1$ (as X itself is required to be smooth). Their argument then shows equally well that Birch's statement holds true: a marked Belyĭ map $(X, f; P)$ descends to its field of moduli.

In this paper, we revisit the results of Dèbes–Emsalem [9] from a slightly different point of view that is more explicit from the point of view of Weil cocycles.

Date: June 26, 2015.

Our main theorem (Theorem 1.10) is as follows. A marked map $(Y, f; Q_1, \ldots, Q_n; P_1, \ldots, P_m)$ over F is a map $f : Y \to X$ of curves over F equipped with distinct points $Q_1, \ldots, Q_n \in Y(F)$ and $P_1, \ldots, P_m \in X(F)$.

Theorem A. *Let*

$$(Y, f : Y \to X; Q_1, \ldots, Q_m; P_1, \ldots, P_n) = (Y, f; \mathcal{R})$$

be a marked map of curves over a separably closed field $F = F^{\mathrm{sep}}$ such that $m \geq 1$ and at least one of the points $Q_1, \ldots Q_m$ is smooth. Then $(Y, f; \mathcal{R})$ descends to its field of moduli.

Theorem A extends the results of Dèbes–Emsalem [9], where the curve X was assumed to be of genus at least 2 and where moreover the order of $\mathrm{Aut}(X)$ was assumed to be coprime to the characteristic of the base field.

Our approach to proving Theorem A is essentially self-contained, and we recover the result of Birch on descent of marked Belyĭ maps (Theorem 1.12). We define the *branches* of a morphism, replacing the choice of a tangential base point with something canonical. This approach has several advantages. First, it provides a more unified treatment, extending results to the wildly ramified (but separable) case. Second, the notion is more conducive to constructive applications: by using branches it becomes straightforward to read off a Weil cocycle from the given rigidification, without having to calculate the canonical model of $\mathrm{Aut}(X)\backslash X$. From the point of view of a computational *Esquisse* [28], this gain is quite important. Finally, our approach leads us to construct some explicit counterexamples to descent in the case where the marked point P is not smooth, as follows.

Theorem B. *There exists marked curves $(X; P)$ and marked maps $(X, f : X \to \mathbb{P}^1; P; 0, 1, \infty)$ with X projective and f unramified outside $\{0, 1, \infty\}$ whose field of moduli for the extension $\mathbb{C} \,|\, \mathbb{R}$ equal $\mathbb{R}$ but that do not descend to $\mathbb{R}$.*

Our paper is organized as follows. In section 1, we introduce the relevant background and notions under consideration, and we give precise statements of the main results of this article. After a review of the classical Weil descent criterion in section 2, we present our theory of branches in section 3. We give some concrete examples in section 4; these include the explicit descent of marked hyperelliptic curves to their field of moduli as well as the descent a marked Klein quartic $(X; P)$ using branches. In section 5, we conclude the paper by presenting our counterexamples in the singular case. In an appendix, we consider descent of marked Galois Belyĭ maps in genus 0.

Acknowledgments. We would like to thank Bryan Birch, Enric Nart, Andrew Obus, and the anonymous referee for their valuable comments on previous versions of this article. The second author was supported by an NSF CAREER Award (DMS-1151047).

1. Background, notation, and statements of main results

In this section, we set up the basic background and notation we will use in the rest of the paper.

Let F be a field with separable closure F^{sep} and absolute Galois group $\Gamma_F = \mathrm{Gal}(F^{\mathrm{sep}} \,|\, F)$. When $\mathrm{char}\, F = 0$, we will also write $F^{\mathrm{sep}} = \overline{F}$. A curve X over F is a geometrically integral, separated scheme of finite type over F of dimension 1. A map $f : Y \to X$ of curves over F is

a nonconstant morphism defined over F. If X, Y are projective, this implies that f is finite, hence proper.

An isomorphism of maps $f : Y \to X$ and $f' : Y' \to X'$ of curves over F is a pair (ψ, φ) of isomorphisms of curves $\psi : Y \xrightarrow{\sim} Y'$ and $\varphi : X \xrightarrow{\sim} X'$ over F such that $\varphi f = f'\psi$, i.e., such that the diagram

$$\begin{array}{ccc} Y & \xrightarrow{\psi} & Y' \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ X & \xrightarrow{\varphi} & X' \end{array} \tag{1.1}$$

commutes; if f is isomorphic to f' we write $f \xrightarrow{\sim} f'$.

The absolute Galois group Γ_F acts naturally on the set of curves and the set of maps between curves defined over F^{sep}—in both cases, applying the Galois action of the automorphism σ comes down to applying σ to the defining equations of an algebraic model of X (resp. f) over F^{sep}. The conjugate of a curve X over F^{sep} by an automorphism $\sigma \in \Gamma_F$ is denoted by $\sigma(X)$, and similarly that of a map f by $\sigma(f)$.

Given a curve X over F and an extension $K \mid F$ of fields, we will denote by X_K the base extension of X to K. We denote the group of of automorphisms of X_K over K by $\mathrm{Aut}(X)(K)$. This latter convention reflects the fact that $\mathrm{Aut}(X)$ is a scheme over F, the K-rational points of which are the K-rational automorphisms of X (by work of Grothendieck on the representability of the Hilbert scheme and related functors [14, 4.c]). As in the introduction, we occasionally write $\mathrm{Aut}(X)$ for the group of points $\mathrm{Aut}(X)(F^{\mathrm{sep}})$ when no confusion is possible, and for curves Y and X over K, we will often speak of an isomorphism between Y and X over K when more precisely an isomorphism between Y_K and X_K over K is meant.

We call a map of curves $f : Y \to X$ over F geometrically generically Galois if the group $G = \mathrm{Aut}(Y)(F^{\mathrm{sep}})$ acts transitively on the fibers of f, or equivalently if the extension of function fields $F^{\mathrm{sep}}(Y) \,|\, F^{\mathrm{sep}}(X)$ is Galois. (This terminology reflects the fact that the usual Galois torsor property is only required to hold on the generic points, and that the elements of the group G need only be defined over F^{sep}.) In what follows, we abbreviate *geometrically generically Galois* to simply Galois. If $f : Y \to X$ is a Galois cover, then it can be identified with a quotient $q_H : Y \to H\backslash Y$ of Y by a finite F-rational subgroup H of G. (This quotient by G exists by work of Grothendieck [13, §6].)

Given a geometrically generically Galois map $f : Y \to X$ branching over a point $P \in X(F^{\mathrm{sep}})$, the ramification indices of the points $Q \in f^{-1}(P)(F^{\mathrm{sep}})$ are all equal, and we call this common value the branch index of the point x on X.

We will now define certain rigidifications of the maps and curves considered above.

Definition 1.2. Let $n \in \mathbb{Z}_{\geq 0}$. An n-marked curve (or n-pointed curve) $(X; P_1, \ldots, P_n)$ over F is a curve X equipped with distinct points $P_1, \ldots, P_n \in X(F)$. An isomorphism of n-marked curves $(X; P_1, \ldots, P_n) \xrightarrow{\sim} (X'; P'_1, \ldots, P'_n)$ over F is an isomorphism $\varphi : X \xrightarrow{\sim} X'$ over F such that $\varphi(P_i) = P'_i$ for $i = 1, \ldots, n$.

We will often use the simpler terminology marked curve for a 1-marked curve.

Definition 1.3. For $n, m \in \mathbb{Z}_{\geq 0}$, an n, m-marked map $(Y, f; Q_1, \ldots, Q_n; P_1, \ldots, P_m)$ over F is a map $f : Y \to X$ of curves over F equipped with distinct points $Q_1, \ldots, Q_n \in Y(F)$ and

$P_1, \dots, P_m \in X(F)$. An isomorphism between n, m-marked maps over F is an isomorphism of maps $(\psi, \varphi) : f \xrightarrow{\sim} f'$ over F such that $\psi(Q_i) = Q_i'$ for $j = 1, \dots, n$ and $\varphi(P_i) = P_i'$ for $i = 1, \dots, m$.

In the definition of an n, m-marked map, no relationship between the points Q_j and P_i under f is assumed; moreover, the points Q_j may or may not be branch points and the points P_i may or may not be ramification points.

We recover the case of marked curves from marked maps by taking $Y = X$ and choosing $f : X \to X$ to be the identity. To avoid cumbersome notation, we will sometimes abbreviate

$$(Y, f; Q_1, \dots, Q_n; P_1, \dots, P_m) = (Y, f; \mathcal{R})$$

and refer to $\mathcal{R}$ as the rigidification data. We use similar notation $(X; \mathcal{R})$ for marked curves.

We will be especially interested in the following special class of maps.

Definition 1.4. Suppose $\operatorname{char} F = 0$. A Belyĭ map over F is a marked map

$$(X, f : X \to \mathbb{P}^1; -; 0, 1, \infty)$$

over F such that X is projective and f is unramified outside $\{0, 1, \infty\}$. A marked Belyĭ map $(X, f : X \to \mathbb{P}^1; P; 0, 1, \infty)$ over F is a Belyĭ map that is marked. A Belyĭ map with a marked cusp over F is a marked Belyĭ map $(X, f : X \to \mathbb{P}^1; P; 0, 1, \infty)$ over F such that $f(P) = \infty$; the width of the marked point P is the ramification index of P over ∞.

Remark 1.5. Replacing f by $1/f$ or $1/(1-f)$, one may realize any marked Belyĭ map whose marking lies above 0 or 1 as a Belyĭ map with a marked cusp.

An isomorphism (ψ, φ) of Belyĭ maps fixes the target $\mathbb{P}^1$: since the automorphism φ of $\mathbb{P}^1$ has to fix each of the points $0, 1, \infty$ by definition, φ is the identity. When no confusion can result, we will often abbreviate a (marked) Belyĭ map by simply f.

Remark 1.6. Relaxing the notion of isomorphism of Belyĭ maps by removing the marked points $0, 1, \infty$ on $\mathbb{P}^1$ typically leads one to consider covers of conics instead of $\mathbb{P}^1$, as in work of van Hoeij–Vidunas [29, §§3.3–3.4]; we discuss this setup further in the appendix.

Let $f : X \to \mathbb{P}^1$ be a Belyĭ map of degree d over $\overline{\mathbb{Q}} \subset \mathbb{C}$. Numbering the sheets of f by $1, \dots, d$, we define the monodromy group of f to be the group $G \leq S_d$ generated by the monodromy elements s_0, s_1, s_∞ of loops around $0, 1, \infty$; the monodromy group is well-defined up to conjugation in S_d, as are the conjugacy classes C_0, C_1, C_∞ in S_d of the monodromy elements, specified by partitions of d. We organize this data as follows.

Definition 1.7. The passport of f is the tuple $(g; G; C_0, C_1, C_\infty)$, where g is the geometric genus of X and $G \leq S_d$ and C_0, C_1, C_∞ are the monodromy group and S_d-conjugacy classes associated to f. The size of a passport is the cardinality of the set of $\overline{\mathbb{Q}}$-isomorphism classes of Belyĭ maps with given genus g and monodromy group G generated by monodromy elements in the S_d-conjugacy classes C_0, C_1, C_∞, respectively.

For all $\sigma \in \operatorname{Aut}(\mathbb{C})$, the Belyĭ map $\sigma(f)$ has the same ramification indices and monodromy group (up to conjugation) as f. Therefore the index of the stabilizer of f in $\operatorname{Aut}(\mathbb{C})$ is bounded by the size of its passport. The size of a passport is finite and can be computed by combinatorial or group-theoretic means [27, Theorem 7.2.1]; thus the field of moduli of f over $\overline{\mathbb{Q}}$ is a number field of degree at most the size of the passport.

We analogously define a marked passport associated to a Belyĭ map with a marked cusp to be the tuple $(g; G; C_0, C_1, C_\infty; \nu)$ where ν is the width of the marked cusp, corresponding to a cycle in the partition associated to C_∞. Once more the field of moduli of a Belyĭ map with a marked cusp over $\overline{\mathbb{Q}}$ is a number field of degree at most the size of its marked passport.

Now let $K \,|\, F$ be a Galois field extension, let X be a curve over K, and let $\Gamma = \mathrm{Gal}(K \,|\, F)$. The field of moduli $M_F^K(X)$ of X with respect to $K \mid F$ is the subfield of K fixed by the subgroup

$$\{\sigma \in \Gamma = \mathrm{Gal}(K \,|\, F) : \sigma(X) \simeq X\}\,. \tag{1.8}$$

In a similar way, one defines the field of moduli $M_F^K(Y; f; \mathcal{R})$ of a marked map. In this paper we will usually only consider the case where $K = F^{\mathrm{sep}}$, and we simply call $M(X) = M_F^K(X)$ the field of moduli of X, and similarly for maps and marked variants.

The central question that we consider in this article is the following.

Question 1.9. *What conditions ensure that a curve, map, or one of its marked variants is defined over its field of moduli?*

For brevity, when an object is defined over its field of moduli with respect to a separable extension $K \,|\, F$, we will say that the object descends (to its field of moduli).

We are now in a position to give a precise formulation of the results motivating this paper.

Theorem 1.10. *Let*

$$(Y, f : Y \to X; Q_1, \ldots, Q_m; P_1, \ldots, P_n) = (Y, f; \mathcal{R})$$

be a marked map of curves over a separably closed field $F = F^{\mathrm{sep}}$ with $m \geq 1$ such that at least one of the points $Q_1, \ldots Q_m$ is smooth. Then $(Y, f; \mathcal{R})$ descends to its field of moduli.

We will prove Theorem 1.10 as a consequence of Theorems 3.12 and 3.19 (the latter dealing with the case of genus zero); it is a special instance of a more general geometric result that shows how to extract a Weil cocycle from the rigidification provided in the theorem. By contrast, marked curves can fail to descend if the marked point is singular: in section 5 we construct two explicit counterexamples, one on a curve X that descends to $\mathbb{R}$ and another on a curve that does not.

Before proceeding, we deduce several important corollaries.

Corollary 1.11. *Let $(X; P)$ be a curve with a smooth marked point over a separably closed field $F = F^{\mathrm{sep}}$. Then $(X; P)$ descends.*

Another corollary is the following theorem.

Theorem 1.12. *A marked Belyĭ map $(X, f : X \to \mathbb{P}^1; P; 0, 1, \infty)$ over $\overline{\mathbb{Q}}$ descends.*

Theorem 1.12 was claimed by Birch [3, Theorem 2] in the special case of a Belyĭ map with a marked cusp; but his proof is incomplete. In work of Dèbes–Emsalem [9, §5], a proof of Theorem 1.12 is sketched using a suitable embedding in a field of Puiseux series. The following corollary of Theorem 1.12 then follows immediately.

Corollary 1.13. *A Belyĭ map $f : X \to \mathbb{P}^1$ is defined over a number field of degree at most the minimum of the sizes of the marked passports $(X, f; P; 0, 1, \infty)$, where $P \in f^{-1}(\{0, 1, \infty\})$.*

Corollary 1.13 often enables one to conclude that the Belyĭ map itself descends, as the following result shows.

Corollary 1.14. *Let $f : X \to \mathbb{P}^1$ be a Belyĭ map over $\overline{\mathbb{Q}}$ with a marked cusp P whose ramification index is unique in its fiber $f^{-1}(\infty)$. Then the Belyĭ map $(X, f; -; 0, 1, \infty)$ descends.*

Proof. Let F be the field of moduli of the marked map $(X, f; -; 0, 1, \infty)$ with respect to the extension $\overline{\mathbb{Q}} \,|\, \mathbb{Q}$. Let $\sigma \in \Gamma_F$ and consider the conjugate Belyĭ map $(\sigma(f); -; 0, 1, \infty)$ with source $\sigma(X)$. Since F is the field of moduli, there exists an isomorphism

$$(\psi_\sigma, \varphi_\sigma) : (\sigma(f); -; 0, 1, \infty) \xrightarrow{\sim} (X, f; -; 0, 1, \infty)$$

with φ_σ the identity map (as noted after Definition 1.4). We see that

$$f(\psi_\sigma(\sigma(P))) = \sigma(f)(\sigma(P)) = \sigma(\infty) = \infty = f(P) \tag{1.15}$$

so $\psi_\sigma(\sigma(P)) \in f^{-1}(\infty)$. The ramification index of $f = \sigma(f)\psi_\sigma^{-1}$ at $\psi_\sigma(\sigma(P))$ is equal to the ramification of $\sigma(f)$ at $\sigma(P)$, which in turn equals that of f at P. By the uniqueness hypothesis, we must have $(\psi_\sigma, \varphi_\sigma)$ sends $\sigma(P)$ to P.

Since σ was arbitrary, this means that the field of moduli of the marked Belyĭ map $(X, f; P; 0, 1, \infty)$ coincides with that of $(X, f; -; 0, 1, \infty)$. By Theorem 1.12, $(X, f; P; 0, 1, \infty)$ descends to this common field of moduli and thus so does $(X, f; -; 0, 1, \infty)$. □

Remark 1.16. The hypothesis of Corollary 1.14 is very often satisfied. When it is not, one can still try to obtain a model of a Belyĭ map over a small degree extension of its field of moduli by ensuring that marking a point does not make the size of the passport grow too much; for example, if P is a point of maximal ramification index then the automorphism group of the marked tuple $(X, f; P; 0, 1, \infty)$ may be of small index in that of $(X, f; -; 0, 1, \infty)$.

2. Weil cocycles

Our main tool for the construction of examples and counterexamples is the *Weil cocycle criterion*, which we will give in Theorem 2.1. For more details, we refer to Serre [25, Ch. V, 20, Cor.2] and to Huggins's thesis [16], which is an excellent exposition on descent of curves.

Throughout this section, we let $K \,|\, F$ be a (possibly infinite) Galois extension, and we let X be a curve over K whose field of moduli with respect to the extension $K \,|\, F$ equals F.

Theorem 2.1 (Weil cocycle criterion)**.** *The curve X descends if and only if there exist isomorphisms*

$$\{\varphi_\sigma : \sigma(X) \xrightarrow{\sim} X\}_{\sigma \in \Gamma} \tag{2.2}$$

over K such that

$$\{\sigma \in \Gamma : \sigma(X) = X \text{ and } \varphi_\sigma = \mathrm{id}_X\} \text{ has finite index in } \Gamma \tag{2.3}$$

and moreover the cocycle condition

$$\varphi_{\sigma\tau} = \varphi_\sigma \sigma(\varphi_\tau) \text{ for all } \sigma, \tau \in \Gamma \tag{2.4}$$

holds.

More precisely, if isomorphisms (2.2) *satisfy conditions* (2.3)–(2.4)*, then there exists a descent X_0 of X to F and an isomorphism $\varphi_0 : X \xrightarrow{\sim} X_0$ over K such that φ_σ is given as the coboundary*

$$\varphi_\sigma = \varphi_0^{-1} \sigma(\varphi_0). \tag{2.5}$$

Remark 2.6. We warn the reader not to confuse the descent φ_0 with the isomorphisms φ_σ for $\sigma \in \Gamma$.

An important corollary of Theorem 2.1, obtained by an immediate uniqueness argument, is the following.

Corollary 2.7. *If* $\mathrm{Aut}(X)(K)$ *is trivial, then* X *descends.*

The Weil cocycle criterion is especially concrete when the base field F equals $\mathbb{R}$. In this case we only have to find an isomorphism $\varphi : \overline{X} \xrightarrow{\sim} X$ between X and its complex conjugate $\overline{X}$ and test the single cocycle relation

$$\varphi\overline{\varphi} = 1 \tag{2.8}$$

that corresponds to the complex conjugation being an involution. Given any φ as above, all other are of the form $\alpha\varphi$, where $\alpha \in \mathrm{Aut}(X)(\mathbb{C})$.

Remark 2.9. More generally, if the extension $K \,|\, F$ is finite, there is a method to find all possible descents of X with respect to the extension $K \,|\, F$; see Method 4.1.

In general, using Theorem 2.1 requires some finesse; when the extension $K \,|\, F$ is infinite, it is not immediately clear through which finite subextensions a descent cocycle could factor. However, in Corollary 3.14 below we shall see that for marked curves or marked Belyĭ maps it is possible to reduce considerations to an explicitly computable finite subextension of $K \,|\, F$.

Now let $(Y; \mathcal{R})$ be a marked curve or map, with $\mathcal{R}$ the rigidification data, and suppose again that the field of moduli of $(Y; \mathcal{R})$ with respect to the extension $K \,|\, F$ equals F. In this case (as mentioned by Dèbes–Emsalem [9, §5]), Theorem 2.1 still applies to the marked curve $(Y; \mathcal{R})$ after replacing $\mathrm{Aut}(Y)$ by the subgroup $\mathrm{Aut}(Y; \mathcal{R})$. Moreover, in case a Weil cocycle exists the marked data then descend along with Y to give a model $(Y_0; \mathcal{R}_0)$ of $(Y; \mathcal{R})$ over F. We give a simple example of this general principle.

Example 2.10. Let $(X; P)$ be a marked curve over K. Suppose that X has field of moduli F, with $\varphi_\sigma : \sigma(X) \xrightarrow{\sim} X$ in (2.4) having the additional property that $\varphi_\sigma(\sigma(P)) = P$. Let X_0 be a descent of X to F, with $\varphi_0 : X \xrightarrow{\sim} X_0$ over K. Let $P_0 = \varphi_0(P) \in X_0(K)$. Then by (2.5), for all $\sigma \in \Gamma$ we have

$$\sigma(P_0) = \sigma(\varphi_0)(\sigma(P)) = \varphi_0\varphi_\sigma(\sigma(P)) = \varphi_0(P) = P_0. \tag{2.11}$$

By Galois invariance, we see that $P_0 \in X_0(F)$. Therefore the marked curve $(X; P)$ descends.

The following special case of Theorem 1.10, an analogue of Corollary 2.7, is then clear from Example 2.10.

Corollary 2.12. *If the group* $\mathrm{Aut}(Y, f; \mathcal{R})(K)$ *is trivial, then* $(Y, f; \mathcal{R})$ *descends.*

Corollary 2.13. *Suppose that* $(Y, f; \mathcal{R})$ *is given by*

$$(Y, f; Q_1, \ldots, Q_n; P_1, \ldots, P_m) = (Y, f; \mathcal{R})$$

with $n \geq 1$*, and moreover suppose that* Q_1 *is* not *a ramification point of* f*. Then* $(Y, f; \mathcal{R})$ *descends.*

Proof. We have $\mathrm{Aut}(Y, f; \mathcal{R})(K) \leq \mathrm{Aut}(Y, f; P_i)(K) \leq \mathrm{Aut}(Y, f)(K)$ and the latter group acts freely on those orbits that contains a non-ramifying point, so indeed $\mathrm{Aut}(Y, f; \mathcal{R})(K)$ is trivial. □

The moral is that when rigidification trivializes the automorphism group, then the obstruction to descent vanishes. At the other extreme, when the original curve descends and the marked curve has the same automorphism group, then the marked curve descends as well.

Proposition 2.14. *Suppose that* $\mathrm{Aut}(Y, f; \mathcal{R})(K) = \mathrm{Aut}(Y)(K)$. *Let* F *be the field of moduli of* $(Y, f; \mathcal{R})$. *Then* $(Y, f; \mathcal{R})$ *descends if* Y *descends, and any descent datum for* Y *gives rise to one for* $(Y, f; \mathcal{R})$.

Proof. Let Y_0 be a descent of Y to F with isomorphism $\psi_0 : Y \xrightarrow{\sim} Y_0$ over K, and let $\sigma \in \mathrm{Gal}(K \mid F)$. We now interpret the map f as a further rigidification of the curve Y, and correspondingly write $(Y; \mathcal{R}')$ for $(Y, f; \mathcal{R})$. By hypothesis, there exists an isomorphism $\psi_\sigma : \sigma(Y) \xrightarrow{\sim} Y$ over K that sends the conjugate rigidification $\sigma(\mathcal{R}')$ to $\mathcal{R}'$. Composing, we get an isomorphism

$$\psi'_\sigma = \sigma(Y_0) \xrightarrow{\sigma(\psi_0^{-1})} \sigma(Y) \xrightarrow{\psi_\sigma} Y \xrightarrow{\psi_0} Y_0. \tag{2.15}$$

Moreover, if we let $\mathcal{R}'_0 = \psi_0(\mathcal{R}')$, then the cocycle relation $\psi_\sigma = \psi_0^{-1}\sigma(\psi_0)$ shows that ψ'_σ sends $\sigma(\mathcal{R}'_0)$ to $\mathcal{R}'_0$: we have

$$\psi'_\sigma(\mathcal{R}'_0) = \psi_0(\psi_\sigma(\sigma(\psi_0^{-1})(\psi_0(\mathcal{R}')))) = \psi_0(\psi_\sigma(\psi_\sigma^{-1}(\mathcal{R}'))) = \psi_0(\mathcal{R}') = \mathcal{R}'_0. \tag{2.16}$$

Now we have assumed that Y_0 is defined over F. Therefore $\sigma(Y_0) = Y_0$, which shows that ψ'_σ actually belongs to $\mathrm{Aut}(Y_0)(K)$. Since $\mathrm{Aut}(Y; \mathcal{R}')(K) = \mathrm{Aut}(Y)(K)$ we equally well have $\mathrm{Aut}(Y_0; \mathcal{R}'_0)(K) = \mathrm{Aut}(Y_0)(K)$. Hence in fact $\sigma(\mathcal{R}'_0) = (\psi'_\sigma)^{-1}(\mathcal{R}'_0) = \mathcal{R}'_0$. Since σ was arbitrary, we see that the rigidification $\mathcal{R}'_0$ is rational on Y_0, as desired. □

Remark 2.17. In case of proper inclusions $\{1\} \subsetneq \mathrm{Aut}(X; \mathcal{R})(K) \subsetneq \mathrm{Aut}(X)(K)$, it is possible for X to descend to F while this is not possible for $(X; \mathcal{R})$: we will see an example of this in Section 5 which is minimal in the sense that the chain of inclusions

$$\{1\} \subsetneq \mathrm{Aut}(X; \mathcal{R})(\mathbb{C}) \simeq \mathbb{Z}/2\mathbb{Z} \subsetneq \mathrm{Aut}(X)(\mathbb{C}) \simeq \mathbb{Z}/4\mathbb{Z}$$

is as small as possible.

3. Branches

The geometric equivalent of a fundamental tool of Dèbes–Emsalem [9] is the consideration of what we will define as the *branches* of a morphism of curves over a point P. For a map tamely ramified at P, branches can be interpreted by embeddings into certain rings of Puiseux series. We revisit this definition in a more general geometric context, which will extend to the wildly ramified case.

Let X be a curve over F, and let $P \in X(F^{\mathrm{sep}})$ be a geometric point of X. Let $\mathscr{O}_{X_{\text{ét}},P}$ be the local ring of X at P for the étale topology. Using idempotents, we have a canonical decomposition

$$\mathscr{O}_{X_{\text{ét}},P} = \prod_i \mathscr{O}_{X_{\text{ét}},P,i} \tag{3.1}$$

into a finite product of domains. Let $\mathscr{P}_{X_{\text{ét}},P,i}$ be the integral closure of the domain $\mathscr{O}_{X_{\text{ét}},P,i}$ in $\mathrm{Frac}(\mathscr{O}_{X_{\text{ét}},P,i})^{\mathrm{sep}}$, the separable closure of its quotient field. We get a ring

$$\mathscr{P}_{X_{\text{ét}},P} = \prod_i \mathscr{P}_{X_{\text{ét}},P,i} \tag{3.2}$$

along with a canonical morphism $\operatorname{Spec} \mathscr{P}_{X_{\text{ét}},P} \to X$.

Definition 3.3. Let $f : Y \to X$ be a separable map of curves over F. A branch of f over P is a morphism $b : \operatorname{Spec} \mathscr{P}_{X_{\text{ét}},P} \to Y$ such that the following diagram commutes:

$$\begin{array}{ccc} & & Y \\ & \overset{b}{\nearrow} & \downarrow f \\ \operatorname{Spec} \mathscr{P}_{X_{\text{ét}},P} & \longrightarrow & X \end{array} \tag{3.4}$$

The set of branches of f over P is denoted $B(f, P)$.

Remark 3.5. Geometrically, a branch of f can be seen as an equivalence class of sections $V \to Y \xrightarrow{f} X$, where the composition $V \to X$ is a "separable neighborhood" of P in the sense that it factors as $V \to U \to X$, where $V \to U$ is separable and where $U \to X$ is an étale neighborhood of P.

Definition 3.3 is most concrete when P is a smooth point of X. In this case $\mathscr{P}_{X_{\text{ét}},P}$ is the closure of $\mathscr{O}_{X_{\text{ét}},P}$ in $\operatorname{Frac}(\mathscr{O}_{X,P})^{\text{sep}}$. The ring $\mathscr{O}_{X_{\text{ét}},P}$ is isomorphic to the integral closure of the polynomial ring $F^{\text{sep}}[t]$ in the ring of power series $F^{\text{sep}}[[t]]$, for t a uniformizer at P [22, Prop. 4.10]. Therefore, if $\operatorname{char} F = 0$, then $\mathscr{P}_{X_{\text{ét}},P}$ is isomorphic to the valuation ring of the field of Puiseux series $F^{\text{sep}}((t^{1/\infty}))$, consisting of those elements of $F^{\text{sep}}((t^{1/\infty}))$ whose monomials all have non-negative exponent. (This isomorphism explains our notation for the ring $\mathscr{P}_{X_{\text{ét}},P}$.) If $\operatorname{char} F = p$, then wild ramification can occur, as for example when considering Artin–Schreier extensions; in this case the ring $\mathscr{P}_{X_{\text{ét}},P}$ is no longer simply a Puiseux series ring (see e.g. the discussion surrounding (4.43)).

Remark 3.6. By taking the fiber over the closed point of $\operatorname{Spec} \mathscr{P}_{X_{\text{ét}},P}$ (in the case of a valuation ring in a field of Puiseux series, we are setting $t = 0$), we recover a lift of the point $P \in X(F^{\text{sep}})$. We can see b as an infinitesimal thickening of this lift; the fact that we cannot use the local ring for the étale topology reflects that we need slightly thinner thickenings than that in this topology to obtain enough sections.

In general, the decomposition in (3.1) has more than one factor. Using the categorical properties of products we see that giving a branch amounts to specifying, for every i, a morphism b_i making the following diagram commute:

$$\begin{array}{ccc} \operatorname{Spec} \mathscr{P}_{X_{\text{ét}},P,i} & \overset{b_i}{\dashrightarrow} & Y \\ \downarrow & & \downarrow f \\ \operatorname{Spec} \mathscr{P}_{X_{\text{ét}},P} & \longrightarrow & X \end{array} \tag{3.7}$$

In this way, we have effectively passed to the normalization of X. For the identity map $X \to X$, the b_i give what is classically called the set of branches of X at P.

Remark 3.8. Alternatively, one can first define branches in the case of a smooth point and then for a general morphism $f : Y \to X$ at a point P to be a branch of the induced map $\widetilde{f} : \widetilde{Y} \to \widetilde{X}$ of normalizations at some point $\widetilde{P} \in \widetilde{X}(F^{\text{sep}})$ over P.

From here on, we will restrict to the case where $P \in X(F^{\text{sep}})$ is a smooth point.

Given an element σ of the absolute Galois group $\mathrm{Gal}(F^{\mathrm{sep}} \mid F)$, there is a canonical map of sets

$$\begin{aligned} B(f,P) &\to B(\sigma(f),\sigma(P)) \\ b &\mapsto \sigma(b) \end{aligned} \tag{3.9}$$

Here $\sigma(f)$ is the morphism $\sigma(Y) \to \sigma(X)$ induced by the action of σ on the coefficients of f. The map on branches is defined as follows. Given a branch $b : \operatorname{Spec} \mathscr{P}_{X_{\text{ét}},P} \to Y$ of f over P, we can conjugate it to obtain a morphism $\sigma(b) : \operatorname{Spec} \sigma(\mathscr{P}_{X_{\text{ét}},P}) \to \sigma(Y)$. We compose with the canonical isomorphism

$$\sigma(\mathscr{P}_{X_{\text{ét}},P}) \simeq \mathscr{P}_{\sigma(X)_{\text{ét}},\sigma(P)} \tag{3.10}$$

where the F^{sep}-algebra structure on this ring has been changed by conjugation with σ.

In the upcoming proposition, we show that the set $B(f,P)$ has two very pleasant properties, which should be thought of as generalizing the properties of usual fibers over non-branch points (cf. Corollary 2.13).

Proposition 3.11. *Let $f : Y \to X$ be a proper map of curves of degree d, and let $P \in X(F^{\mathrm{sep}})$ be a smooth geometric point of X. Then the set $B(f,P)$ has cardinality d, and the action of $\mathrm{Aut}(Y,f)$ on $B(f,P)$ is faithful.*

Proof. Let $R = \mathscr{O}_{X_{\text{ét}},P}$ and $S = \mathscr{P}_{X_{\text{ét}},P}$ be as above. Since P is smooth, the rings R and S are integral domains; we denote their quotient fields by K and L. By definition, L is a separable closure of K, and the point P yields canonically a point $P_K \in X(K)$. Pulling back the map f by P_K, we obtain another separable map of degree d, corresponding to a field extension of K. By Galois theory, there are d points $Q_1, \ldots, Q_d$ in $Y(L)$ that lie over P.

We claim that the points $Q_1, \ldots, Q_d$ are specializations of unique points in $Y(S)$. To see this, note that every point Q_i is in fact defined over a finite subextension K_i of K contained in L. Let R_i be the integral closure of the strictly henselian discrete valuation ring R in K_i. Then R_i is again a discrete valuation ring. The morphism f is proper because Y and X both are. Therefore, by the valuative criterion of properness applied to the morphism f, the points $Q_i \in Y(K_i)$ extend uniquely to points in $Y(R_i)$, proving our claim.

To conclude, we show that the action of $\mathrm{Aut}(Y,f)$ is faithful: this follows since it is a base extension of the action of the automorphism group on the generic fiber. □

The following theorem can then be applied to give a constructive proof of Theorem A (Theorem 1.10) in the case where the automorphism group of the marked map is finite. We finish the proof below.

Theorem 3.12. *Let $(Y,f;\mathcal{R})$ be a marked curve over F^{sep} with finite automorphism group $G = \mathrm{Aut}(Y,f;\mathcal{R})(F^{\mathrm{sep}})$. Let $\pi : Y \to G\backslash Y = W$ be the quotient map.*

(a) *Let $Q \in Y(F^{\mathrm{sep}})$ be smooth. Then $S = \pi(Q)$ is a smooth point of W, and the set of branches $B(\pi,S)$ is a torsor under G.*

(b) *Suppose that $\mathcal{R}$ contains at least one smooth point Q on Y. Then $(Y,f;\mathcal{R})$ descends.*

More precisely, let $S = \pi(Q)$. Given $b \in B(\pi,S)$, for all $\sigma \in \Gamma = \mathrm{Gal}(F^{\mathrm{sep}} \mid F)$ there exists a unique morphism $\varphi_\sigma : \sigma(Y) \xrightarrow{\sim} Y$ such that $\sigma(b)$ is sent to b, and the collection $\{\varphi_\sigma\}_{\sigma\in\Gamma}$ defines a Weil cocycle.

Proof. First, part (a). The smoothness of the point S follows from the fact that a quotient of the power series ring $F^{\mathrm{sep}}[[x]]$ by a finite group action is isomorphic to this same ring by the structure theorem for complete discrete valuation rings [26, II, Th. 2]. That the set $B(\pi, S)$ is a G-torsor then follows from Proposition 3.11, since the map $Y \to W$ is (generically) Galois. Note that the quotient morphism π is finite, hence proper.

Now we prove (b). The existence of φ_σ follows because choosing just *any* $\varphi'_\sigma : \sigma(Y) \to Y$ maps $\sigma(b)$ to *some* branch over S, which we can then modify to be b by invoking the transitivity part of being a torsor. The φ_σ give a Weil cocycle because of the uniqueness part of being a torsor; both $\varphi_{\sigma\tau}$ and $\varphi_\sigma\sigma(\varphi_\tau)$ send b to $\sigma\tau(b)$. □

Remark 3.13. Theorem 3.12 in fact shows that there exists a descent $(Y_0; f_0; \mathcal{R}_0)$ with a branch at the image S_0 of S that is defined over F. Indeed, the coboundary corresponding to the Weil cocycle φ_σ maps b to a F-rational branch by a similar argument as that in (2.11).

The proof of Theorem 3.12 also shows how to obtain a finite extension of F over which a Weil cocycle can be constructed.

Corollary 3.14. *Let $(Y, f; \mathcal{R})$ be a marked map with a smooth point P as part of the rigidification data. Let G be the automorphism group of $(Y, f; \mathcal{R})$. Let K be the Galois closure of the field generated over F by the coefficients of defining equations of $(Y, f; \mathcal{R})$, the elements of the group G, and the branches of the canonical morphism $\pi : Y \to G\backslash Y$ at $\pi(P)$. Then a Weil cocycle for $(Y, f; \mathcal{R})$ can be constructed relative to the extension $K \,|\, F$.*

Remark 3.15. As we will see explicitly later, computing the splitting field of the branches at a given point requires no more than determining the leading term of a certain fractional power series, which in turn has known order.

Remark 3.16. The counterexamples in Section 5 all share the property that the number of branches over the points of the base curve is not constant, because of the merging of these branches over the singular points, which are (crucially) the only rational points of the base curve. This makes it impossible to read off a uniquely determined cocycle as in Theorem 3.12.

Remark 3.17. As in Birch's original article [3] we can consider the case where X is a modular curve associated with a subgroup $\mathrm{SL}_2(\mathbb{Z})$, which we suppose to be defined over some number field F. Using a cusp of X then allows one to use q-expansions with respect to a uniformizer q of the appropriate width with respect to the cusp.

Echelonizing a basis of modular forms gives a defining equation for X over F; this does indeed turn out to lead to F-rational q-expansions, with the slight subtlety that one may need to twist X to have a rational branch over F.

To finish the proof of Theorem 1.10, it remains to deal with the case where the automorphism group of the marked curve $(Y, f; \mathcal{R})$ is infinite. In this case the map f has to be the identity map, so we are reduced to considering marked curves $(X; \mathcal{R}) = (X; P_1, \dots P_n)$ with $n \geq 1$ for which one of the P_i, say P_1, is smooth.

Lemma 3.18. *Let $(X; \mathcal{R}) = (X; P_1, \dots P_n)$ be a marked projective curve with P_1 smooth and $\#\operatorname{Aut}(X; \mathcal{R}) = \infty$. Let $\Sigma = X_{\mathrm{sing}}(F^{\mathrm{sep}})$ be the set of singular points of X. Then the following statements hold.*

(a) *The geometric genus g of X is equal to* 0.

(b) *We have* $n+\#\Sigma \leq 2$*, and the inverse image of* $\mathcal{R}\cup\Sigma$ *with respect to the normalization* $\widetilde{X} \to X$ *has cardinality at most* 2*.*

Proof. An automorphism of X extends to a unique automorphism of the normalization $\widetilde{X}$, so $\mathrm{Aut}(X;\mathcal{R}) \leq \mathrm{Aut}(X) \leq \mathrm{Aut}(\widetilde{X})$. If $g \geq 2$ then $\mathrm{Aut}(\widetilde{X})$ is infinite, so immediately we have $g = 0, 1$.

Since P_1 is smooth, it lifts to a unique point $\widetilde{P}_1$ on $\widetilde{X}$, and any automorphism of X fixing P_1 lifts to a unique automorphism of $\widetilde{X}$ fixing $\widetilde{P}_1$. If $g = 1$, then $(\widetilde{X}, \widetilde{P}_1)$ has the structure of an elliptic curve so $\mathrm{Aut}(\widetilde{X}, \widetilde{P}_1)$ is finite, and so $\mathrm{Aut}(X;\mathcal{R}) \leq \mathrm{Aut}(X;P_1) \leq \mathrm{Aut}(\widetilde{X}, \widetilde{P}_1)$. So $g = 0$, proving (a).

Statement (b) then follows, since an automorphism of a curve of genus 0 is determined by the image of three distinct points on this curve. □

Theorem 3.19. *Let* $(X;\mathcal{R})$ *be a marked curve over* F^{sep} *such that* $\mathcal{R}$ *contains at least one smooth point on* X*. Then* $(X;\mathcal{R})$ *descends.*

Proof. Let $G = \mathrm{Aut}(X;\mathcal{R})$. If $\#G < \infty$, we can apply Theorem 3.12. If $\#G = \infty$, we apply Lemma 3.18 and have two cases.

First suppose X is projective and that $(X;\mathcal{R}) = (X;P_1)$ for a smooth point P_1. By Lemma 3.18(b), X has at most one singular point. If X is smooth, we can then take $(\mathbb{P}^1;\infty)$ as a descent (cf. Lemma 4.5). This leaves the case where X has a unique singular point P_2, and again by Lemma 3.18(b), P_2 has a unique inverse image $\widetilde{P}_2$ on $\widetilde{X}$. The automorphism group $\mathrm{Aut}(X;\mathcal{R})$ is contained in the group of automorphisms $\mathrm{Aut}(\widetilde{X};\widetilde{P}_1,\widetilde{P}_2) \simeq \mathbb{G}_m$ since P_2 is the unique singular point on X. Moreover, this inclusion is functorial. Therefore $\mathrm{Aut}(X;\mathcal{R})$ is isomorphic to a subvariety of $\mathbb{G}_m$, and since we assumed that it was infinite, it coincides with $\mathrm{Aut}(\widetilde{X};\widetilde{P}_1,\widetilde{P}_2)$. Now $(\widetilde{X};\widetilde{P}_1,\widetilde{P}_2)$ descends by the argument above. Let $\{\varphi_\sigma\}_{\sigma\in\Gamma}$ be a set of isomorphisms of $(X;P_1,P_2)$ with its conjugates. By the property of the normalization, these lift to yield a set of isomorphisms $\{\widetilde{\varphi}_\sigma\}_{\sigma\in\Gamma}$ of $(\widetilde{X};\widetilde{P}_1,\widetilde{P}_2)$. Because $(\widetilde{X};\widetilde{P}_1,\widetilde{P}_2)$ descends we can modify this latter set by automorphisms $\{\widetilde{\alpha}_\sigma\}_{\sigma\in\Gamma}$, to obtain a Weil cocycle $\{\widetilde{\varphi}\widetilde{\alpha}_\sigma\}_{\sigma\in\Gamma}$ for $(\widetilde{X};\widetilde{P}_1,\widetilde{P}_2)$. Our statement on automorphism groups above means that the set of automorphisms $\{\widetilde{\alpha}_\sigma\}_{\sigma\in\Gamma}$ descends to a set of automorphisms $\{\alpha_\sigma\}_{\sigma\in\Gamma}$, and by construction $\{\varphi_\sigma\alpha_\sigma\}_{\sigma\in\Gamma}$ is then a Weil cocycle for $(X;P_1,P_2)$.

Now suppose that X is projective with two marked points $(X;\mathcal{R}) = (X;P_1,P_2)$. Again we are done if X is smooth, since then a descent is given by $(\mathbb{P}^1;\infty,0)$. In the case where we admit singular points, we are reduced to the same case as that in the previous paragraph: P_2 is singular and has a unique inverse image $\widetilde{P}_2$ on $\widetilde{X}$.

The case where X is not projective follows by taking its smooth completion and applying the results above. □

Remark 3.20. In the proof above it is indeed possible for the automorphism group of $\mathrm{Aut}(X;P_1,P_2)$ to be finite and non-trivial. An example is given by the smooth completion of the embedding

$$t \mapsto (t^3(1-t^2), t^4(1-t^2), t^7), \tag{3.21}$$

which has an automorphism group of order 2 as long as the characteristic of F is odd.

To conclude this section, we phrase our results in terms of a classical notion from Dèbes–Emsalem [9]. Let $(Y, f;\mathcal{R})$ be a marked map over F^{sep} with field of moduli F and finite

automorphism group $G = \mathrm{Aut}(Y, f; \mathcal{R})$, and let $W = G\backslash Y$. Then by construction any choice of isomorphisms (2.2) gives rise to a Weil cocycle on W.

Definition 3.22. The canonical model W_0 is the model of W defined over F determined by the cocycle on W induced by any choice of isomorphisms (2.2).

The canonical model depends only on the isomorphism class of $(Y, f; \mathcal{R})$ over F^{sep}. In the canonical model, we denote the quotient morphism $\pi : Y \to G\backslash Y$ and let $\psi_0 : W \xrightarrow{\sim} W_0$ be a coboundary corresponding to the uniquely determined collection of isomorphisms $\{\psi_\sigma\}_{\sigma\in\Gamma}$ induced by (2.2). Set $\pi_0 = \psi_0\pi$.

Proposition 3.23. *Let $Q \in Y(F^{\mathrm{sep}})$ be smooth. Then the field of moduli of $(Y, f; \mathcal{R}; Q)$ is the field of definition of the point $\pi_0(Q)$ on W_0.*

Proof. Let $F' = F(\pi_0(Q))$ be the field of definition of $\pi_0(Q)$ on W_0.

First, we claim that F' is contained in the field of moduli M of $(Y, f; \mathcal{R}; Q)$. By Theorem 1.10, we may assume without loss of generality that $(Y, f; \mathcal{R}; Q) = (Y_0; f_0; \mathcal{R}_0; Q_0)$ is defined over M. Thus $Q \in Y(M)$. This implies $\pi_0(Q) \in W_0(M)$: we have $W_0 = G\backslash Y$ where $G = \mathrm{Aut}(Y, f; \mathcal{R})$ so that π_0 coincides with the natural projection $Y \to W = G\backslash Y$ defined over M. Thus $M \supseteq F' = F(\pi_0(Q))$.

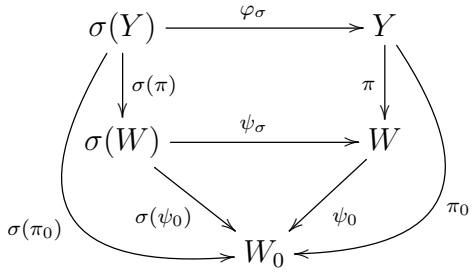
To conclude, we show $M \subseteq F'$. We then have to show that for all $\sigma \in \Gamma' = \mathrm{Gal}(F^{\mathrm{sep}} \,|\, F')$, there exist isomorphisms

$$\varphi_\sigma : (\sigma(Y); \sigma(f); \sigma(\mathcal{R}); \sigma(P)) \xrightarrow{\sim} (Y, f; \mathcal{R}; P) \tag{3.24}$$

so that M is contained in F'. We are given that $(Y, f; \mathcal{R})$ has field of moduli F, so we have isomorphisms $\varphi_\sigma : (\sigma(Y); \sigma(f); \sigma(\mathcal{R})) \xrightarrow{\sim} (Y, f; \mathcal{R})$ for all $\sigma \in \mathrm{Gal}(F^{\mathrm{sep}} \,|\, F)$.

Let $\sigma \in \Gamma'$. We will show that φ_σ can be chosen in such a way that additionally $\varphi_\sigma(\sigma(Q)) = Q$. Let $\psi_\sigma = \psi_0^{-1}\sigma(\psi_0)$. Then by construction of the canonical Weil cocycle for W we know that $\pi\varphi_\sigma = \psi_\sigma\sigma(\pi)$. We obtain the following commutative diagram:

(3.25)



The rationality of $\pi_0(Q)$ over F' implies that

$$\pi_0(Q) = \sigma(\pi_0(Q)) = \sigma(\pi_0)(\sigma(Q)). \tag{3.26}$$

We claim that $Q, \varphi_\sigma(\sigma(Q)) \in Y(F^{\mathrm{sep}})$ are in the same fiber of the map π_0. Indeed, from (3.26) and tracing through the diagram (3.25), we obtain

$$\pi_0(Q) = \sigma(\pi_0)(\sigma(Q)) = \pi_0(\varphi_\sigma(\sigma(Q))). \tag{3.27}$$

Because $\mathrm{Aut}(Y, f; \mathcal{R})$ acts transitively on the fibers of π and thus on those of π_0, we see that we can compose the chosen φ_σ with an element of this group to obtain an isomorphism as in (3.24). □

Theorem 3.28. *Let $Q \in Y(K)$ be smooth. Then Q is F-rational on* some *descent of $(Y, f; \mathcal{R})$ to F if and only if $\pi_0(Q)$ is F-rational.*

As a corollary, we obtain the following theorem, alluded to by Dèbes–Emsalem [9, §5].

Theorem 3.29. *Suppose that W_0 admits a smooth F-rational point. Then $(Y, f; \mathcal{R})$ descends.*

Proof. Let $Q \in Y(F^{\mathrm{sep}})$ be such that $\pi_0(Q) \in V_0(F)$. Then the field of moduli of $(Y, f; \mathcal{R}; Q)$ equals F by Qroposition 3.23. We get a descent $(Y_0; f_0; \mathcal{R}_0; Q_0)$ of $(Y, f; \mathcal{R}; Q)$ to F by Theorem 1.10, which also gives a descent of $(Y, f; \mathcal{R})$ to F. □

Remark 3.30. Theorem 3.29 applies in particular when Y is not equipped with a rigidification. Consider for example the marked curve case $Y = X$ where X is hyperelliptic, with hyperelliptic involution ι; one can then show [20] that a descent to F induced by a point P as in Theorem 3.28 always exists, except possibly if $g(X)$ and $\#\operatorname{Aut}(X)/\langle\iota\rangle$ are both odd. That is, except in these special cases any descent can be obtained by marking a point on X.

Remark 3.31. The results in this section can also be obtained by using a tangential base point (a germ of a regular function at a given point) as in Deligne [10, §15] by splitting an exact sequence of fundamental groups, as explained by Dèbes–Emsalem [9]. We prefer our new approach for two reasons. First, a choice of tangential base point is noncanonical, so it is cleaner (and more intuitive) to instead refine points into branches, which does not require such a choice. Second, the formalism of tangential base points has not been extended to the wildly ramified case to our knowledge, whereas our definition immediately covers this case.

4. Descent of marked curves

This section focuses on the explicit descent on marked curves, notably hyperelliptic curves and plane quartics. Before treating these examples, we indicate a general method for descending marked curves.

Determining a Weil descent. Let $K \mid F$ be a Galois extension, and let $(Y, f; \mathcal{R})$ be a marked map over K. Suppose that the extension $K \mid F$ and the automorphism group $\operatorname{Aut}(Y, f; \mathcal{R})$ are both finite. Then the following method finds all possible descents of $(Y, f; \mathcal{R})$ with respect to the extension $K \mid F$.

Method 4.1. This method takes as input a marked map $(Y, f; \mathcal{R})$ over K and produces as output all descents $(Y_0, f_0; \mathcal{R}_0)$ of $(Y, f; \mathcal{R})$ to F up to isomorphism over F.

1. Compute a presentation $\Gamma = \langle \Sigma \mid \Pi \rangle$ of the Galois group $\Gamma = \operatorname{Gal}(K \mid F)$ in finitely many generators Σ and relations Π.
2. Compute $G = \operatorname{Aut}(Y, f; \mathcal{R})(K)$.
3. For all $\sigma \in \Sigma$, compute an isomorphism $\psi_\sigma : (\sigma(Y), \sigma(f); \sigma(\mathcal{R})) \xrightarrow{\sim} (Y, f; \mathcal{R})$ over K. If for one of these generators no such isomorphism exists, output the empty set and terminate.
4. For all tuples $(\varphi_\sigma)_{\sigma\in\Sigma}$ in the product $\prod_{\sigma\in\Sigma} G\psi_\sigma$, use the relation (2.4) to determine the value of the corresponding cocycle on the relations in Π; retain a list $\mathcal{L}$ of those tuples for which the corresponding cocycle is trivial on all elements of Π.
5. For the tuples $(\varphi_\sigma)_{\sigma\in\Sigma}$ in $\mathcal{L}$, construct a coboundary morphism $\varphi_0 : (Y, f; \mathcal{R}) \xrightarrow{\sim} (Y_0, f_0; \mathcal{R}_0)$ to obtain a descent of $(Y, f; \mathcal{R})$. Output this set of descents.

Remark 4.2. Method 4.1 applies to smoothly marked maps $(Y, f; \mathcal{R})$ over the separable closure F^{sep} to detect the existence of a descent: by Corollary 3.14, we can always reduce the existence of a descent from F^{sep} to a finite extension $K \mid F$. (There may be infinitely many descents of $(Y, f; \mathcal{R})$ over F^{sep}, but only finitely many coming from a given finite extension $K \mid F$.)

Remark 4.3. In step 1 of the above method, one can work instead with the full group Γ itself rather than generators and relations; then one loops over the elements of the group and checks compatibility with products.

The correctness of this method follows by the general approach in the previous section. For now, we present only a 'method' rather than a true algorithm, as each of these steps may involve a rather difficult computer algebra problem in general; however, efficient algorithms for finding isomorphisms exist for smooth hyperelliptic or plane curves, , making all but the final step of the method are algorithmic. The construction of a coboundary is somewhat more involved but can be obtained in the aforementioned cases as well, essentially by finding points on a certain variety over the ground field. We do not go into the general problem here, as they form a substantial challenge of their own, but we do indicate how to proceed in special cases below.

Remark 4.4. If $(Y, f; \mathcal{R})$ is already defined over F, the method above will find the twists of $(Y, f; \mathcal{R})$ over K, that is, the set of F-isomorphism classes of marked maps curves over F that become isomorphic to $(Y, f; \mathcal{R})$ over K. In this case the isomorphisms φ_σ are themselves already in G, so this computation is slightly easier.

Descent of marked smooth curves of genus at most one. We begin by disposing of two easy cases in low genus.

Lemma 4.5. *Let $(X; P)$ be marked curve over F^{sep} with X smooth of genus ≤ 1. Then $(X; P)$ has field of moduli F. If $g = 0$, a descent to F is given by $(X_0; P_0) = (\mathbb{P}^1; \infty)$; if $g = 1$, then the field of moduli is equal to $F(j(\mathrm{Jac}(X)))$.*

Proof. The case $g = 0$ is immediate. So suppose $g = 1$. By translation on the genus 1 curve X, we can take $(X_0; P_0) = (J; \infty)$, where $J = \mathrm{Jac}(X)$ is the Jacobian of X with origin ∞, which is defined over $F(j)$ where j is the j-invariant of J. □

Hyperelliptic curves. We now pass to a class of examples that can be treated in some generality, namely that of smooth hyperelliptic curves of genus at least 2. Throughout, we suppose that the base field F does not have characteristic 2.

Let X be a smooth hyperelliptic curve over F^{sep} and let $\iota : X \to X$ be the hyperelliptic involution. Let $W = \langle \iota \rangle \backslash X$ and $V = \mathrm{Aut}(X) \backslash X$. We get a sequence of natural projection maps

$$X \xrightarrow{q} W \xrightarrow{p} V; \tag{4.6}$$

the map p is the quotient of W by the reduced automorphism group $G = \mathrm{Aut}(X)(F^{\text{sep}})/\langle \iota \rangle$ of W (or of X, by abuse).

We can identify G with a subgroup of $\mathrm{PGL}_2(F^{\text{sep}}) = \mathrm{Aut}(W)(F^{\text{sep}})$. For simplicity, we also suppose that G *does not contain any non-trivial unipotent elements*. This hypothesis implies that G is isomorphic to one of the finite groups C_n, D_n, A_4, S_4 and A_5.

The reduced automorphism group G is also described as $G = \mathrm{Aut}(W; D)(F^{\mathrm{sep}})$, where D is the branch divisor of q, or equivalently, the image on W of the divisor of Weierstrass points on X; thus X can be recovered from $(W; D)$ over F^{sep} by taking a degree 2 cover of W ramified over D.

Remark 4.7. Even if $(W; D) = (W_0; D_0)$ is defined over F, it is *not* always possible to construct a cover X_0 of $(W_0; D_0)$ over F whose branch divisor equals D_0. Indeed, let X be a hyperelliptic curve with field of moduli F and $\mathrm{Aut}(X)(F^{\mathrm{sep}}) = \langle \iota \rangle$. Then $W = V$, and there exists a canonical descent W_0 of W. Moreover, by the same argument that we used to obtain (2.11), D transforms to a F-rational divisor D_0. If the aforementioned cover could be constructed over F, then X_0 would be a descent of X. But as is known classically (see also Remark 5.9), there exist hyperelliptic curves of genus 2 with generic automorphism group that do not descend.

Let $R \in X(F^{\mathrm{sep}})$ and consider the marked curve $(X; R)$ over F^{sep}. Let $Q = q(R)$ be the image of R on W, and similarly let $P = p(q(R))$ be its image on V. Then we can also reconstruct $(X; R)$ from the datum $(W; Q; D)$ obtained by rigidifying $(W; Q)$ with the branch divisor D of q.

Proposition 4.8. *With the above notation, let X' be a curve over F^{sep} obtained as a degree 2 cover of W ramifying over D, and let R' be any preimage of Q under the corresponding covering map. Then (X', R') is isomorphic to (X, R) over F^{sep}.*

Proof. This follows from the fact that a hyperelliptic curve over F^{sep} is uniquely determined by the branch locus of its hyperelliptic involution ι, combined with the fact that ι acts transitively on the fibers of the quotient $X \to W$. □

We now suppose that $(X; R)$ has field of moduli F, which we can do without loss of generality. By Theorem 1.10, we know that $(X; R)$ descends to a marked curve $(X_0; R_0)$ over F, which upon taking quotients by normal subgroups gives rise to a sequence of marked curves and morphisms

$$(X_0; R_0) \xrightarrow{p_0} (W_0; Q_0) \xrightarrow{q_0} (V_0; P_0). \tag{4.9}$$

over F. In what follows, we will show how to calculate the descent $(X_0; R_0)$ explicitly. Our methods do not yet need branches; for pointed hyperelliptic curves, it suffices to use more elementary techniques involving morphisms between curves of genus 0.

We will first construct the descent $(V_0; P_0)$ of (V, P). This is done as in Dèbes–Emsalem [9]; we start with any collection of isomorphisms $\{\varphi_\sigma : \sigma(X) \to X\}_{\sigma \in \Gamma_F}$ and consider the induced maps $\chi_\sigma : \sigma(V) \xrightarrow{\sim} V$. By construction, the collection $\{\chi_\sigma\}_{\sigma \in \Gamma_F}$ satisfies the Weil cocycle relation. Therefore there exists a map $\chi_0 : V \xrightarrow{\sim} V_0$ to a descent V_0 of F such that $\chi_\sigma = \chi_0^{-1} \sigma(\chi_0)$. By the same argument that we used to obtain (2.11), we see that $P_0 = \chi_0(P)$ becomes an F-rational point on V_0.

The isomorphisms $\varphi_\sigma : \sigma(X) \xrightarrow{\sim} X$ can be explicitly calculated [19]. After determining the induced maps $\chi_\sigma : \sigma(V) \xrightarrow{\sim} V$ between genus 0 curves, we can explicitly calculate the map χ_0, and with it the point P_0 [15, 24]. We therefore assume the descent $\chi_0 : (V; P) \xrightarrow{\sim} (V_0; P_0)$ to be given, and will now discuss how to reconstruct a descent $(X_0; R_0)$ of $(X; R)$ from it.

In one case, determining $(X_0; R_0)$ turns out to be particularly easy. Let $G_0 = \mathrm{Aut}(W_0; Q_0)$. Suppose that G_0 is trivial, so that $(W_0; Q_0) = (V_0; P_0)$. Then the image D_0 of the branch

divisor D on W_0 is defined over F. Since V_0 admits the point P_0 over F, it is isomorphic to $\mathbb{P}^1$ over F.

Suppose the reduced automorphism group of the pair $(X;R)$ is trivial. Let $W_0 \xrightarrow{\sim} \mathbb{P}^1$ be any isomorphism over F that sends R_0 to ∞, and let p_0 be a monic polynomial cutting out the image of $\mathrm{Supp}(D_0)\backslash\infty$. Let

$$X_0 : y^2 = p_0(x) \tag{4.10}$$

If R is not a Weierstrass point of X, then $\infty \notin \mathrm{Supp}(D_0)$, so that p_0 is of even degree. In this case we let R_0 be the point at infinity corresponding to the image of $(0,1)$ under the change of coordinates $(x,y) \leftarrow (1/x, y/x^{g+1})$. On the other hand, if R is a Weierstrass point of X, then $\infty \in \mathrm{Supp}(D_0)$ and p_0 is of odd degree, in which case we let R_0 be the point corresponding to $(0,0)$ under the aforementioned change of coordinates.

The following proposition is then immediate.

Proposition 4.11. *Let $(X;R)$ be a marked hyperelliptic curve over F^{sep} whose reduced automorphism group is trivial. Then the pair $(X_0;R_0)$ defined in (4.10) is a descent of $(X;R)$.*

Remark 4.12. In Proposition 4.11, the indicated point P_0 on X_0 admits a rational branch. In the case when R is a not a Weierstrass point of X, this is because P_0 is unramified, whereas in the latter case we get a rational branch for the map $(x,y) \mapsto x$. This follows from a local power series expansion at infinity; since $y^2 = x + O(x^2)$, we get the rational branch corresponding to the root $y = \sqrt{x} + O(x)$.

The quadratic twist defined by $c_0 y^2 = p_0(x)$ also gives a descent of the marked curve $(X;R)$; but if $c_0 \in F^\times \setminus F^{\times 2}$, the map $(x,y) \to x$ does not admit a rational branch at the point at infinity, rather the morphism $(x,y) \mapsto c_0 x$ gives a rational branch. In general, the passage from points to branches gives rise to further cohomological considerations, and any branch on a descended curve $(X_0;R_0)$ for the quotient map $\mathrm{Aut}(X_0;R_0)\backslash(X_0;R_0)$ becomes rational on some uniquely determined twist of $(X_0;R_0)$.

Now suppose that the pair $(X;R)$ has nontrivial reduced automorphism group $G = \mathrm{Aut}(X)/\langle\iota\rangle$. This automorphism group is then cyclic, of order $n = \#G$. We will now show how to obtain a descent of $(X;R)$ in this case.

Let α be a generator of G, and let $Q = q(R)$ be the image of R on the quotient $W = \langle\iota\rangle\backslash X$. Since we assumed that α was not unipotent, we can identify W with a projective line $\mathbb{P}^1$ with affine coordinate x in such a way that Q corresponds to the point $\infty \in \mathbb{P}^1(F^{\mathrm{sep}})$ and such that α is defined by

$$\alpha(x) = \zeta_n x \tag{4.13}$$

with ζ_n a primitive nth root of unity in F^{sep}. Let p be the polynomial defining X as a cover of W. Then because of our normalizations, we either have

$$p(x) = \pi(x^n) \tag{4.14}$$

or

$$p(x) = x\pi(x^n). \tag{4.15}$$

for some polynomial π. In the latter case, there is a single point at infinity that is a Weierstrass point of X, whereas in the former there are two ordinary points at infinity.

We normalize π to be monic by applying a scaling in x (which does not affect the above assumptions on α and Q) and denote its degree by d. By our assumption that the reduced automorphism group is of order n, if we write

$$\pi(x) = \sum_{i=0}^{d} \pi_i x^{d-i} = x^d + \pi_1 x^{d-1} + \pi_2 x^{d-2} + \cdots + \pi_{d-1} x + \pi_d \tag{4.16}$$

then the subgroup of $\mathbb{Z}$ generated by $\{i : \pi_i \neq 0\}$ equals $\mathbb{Z}$.

Given a monic polynomial π as above, we define the hyperelliptic curves X_π and X'_π by

$$X_\pi : y^2 = \pi(x) \tag{4.17}$$

and

$$X'_\pi : y^2 = x\pi(x). \tag{4.18}$$

The former curve admits a distinguished point $R_\pi = (0 : 1)$ at infinity after the coordinate change $(x, y) \leftarrow (1/x, y/x^{g+1})$, whereas the latter admits a Weierstrass point at infinity (which corresponds to $R'_\pi = (0, 0)$ under the same coordinate transformation).

Our only freedom left to modify the coefficients of π is scaling in the x-coordinate: this induces an action of F^{sep} on the coefficients π_i, given by

$$\alpha(\pi_1, \pi_2, \ldots, \pi_d) = (\alpha^1 \pi_1, \alpha^2 \pi_2, \ldots, \alpha^d \pi_d). \tag{4.19}$$

We can interpret the coefficients of π as a representative of a point in the corresponding weighted projective space. Now there is a notion of a normalized representative of such a point [18]. We call a polynomial π normalized if its tuple of coefficients is normalized.

The uniqueness of the normalized representative then shows the following theorem.

Theorem 4.20. *Let $(X; R)$ be a marked hyperelliptic curve over F^{sep} whose reduced automorphism group is tamely cyclic of order n. Then $(X; R)$ admits a unique model of the form (X_π, R_π) or (X'_π, R'_π), with π normalized, depending on whether R is a Weierstrass point of X or not.*

Proof. It is clear from the above that $(X; R)$ admits a model of the indicated form. On the other hand, let $\sigma \in G_F$ and consider the polynomial $\sigma(\pi)$ obtained by conjugating the coefficients of π by σ. If the coefficients of p_π were not stable under Galois, then we would find two distinct normalized representatives of the same weighed point, a contradiction. Therefore $\sigma(\pi) = \pi$, and since σ was arbitrary, our theorem is proved. □

Remark 4.21. If we do not happen to know the field of moduli of the pair $(X; R)$, then the approach above calculates it as well. Indeed, $M_F^{F^{\mathrm{sep}}}(X; R)$ is generated by the coordinates of the normalized representative $c_{I,0}$. A similar remark applies to the upcoming Proposition 5.33.

The Klein quartic. We now apply the method of branches to a plane quartic, namely the Klein quartic, defined by the equation

$$x^3 y + y^3 z + z^3 x = 0. \tag{4.22}$$

By classical results (see the complete exposition by Elkies [11]), this curve admits Belyĭ map of degree 168 that realizes the quotient map by its full automorphism group. In what follows, we will determine a model of the Klein quartic that admits a rational ramification

point for this morphism that is of index 2. The geometry of the Klein quartic is exceedingly well-understood due to its moduli interpretation. As such, our result is not new; it can be found in a different form in work of Poonen–Schaefer–Stoll [23]. However, what makes our method new is the purely algebraic approach to the problem, which is available in rather greater generality.

Before starting, we modify our model slightly and instead consider the rational S_3 model from Elkies [11], which is given by

$$X : x^4 + y^4 + z^4 + 6(xy^3 + yz^3 + zx^3) - 3(x^2y^2 + y^2z^2 + z^2x^2) + 3xyz(x + y + z) = 0. \tag{4.23}$$

Consider the field $K = \mathbb{Q}(i, \theta)$ where $\theta^4 = -7$. Over K, the curve X admits the involution defined by the matrix

$$\begin{pmatrix} 2 & -3 & -6 \\ -3 & -6 & 2 \\ -6 & 2 & -3 \end{pmatrix} \in \mathrm{PGL}_3(\mathbb{Q}) = \mathrm{Aut}(\mathbb{P}^2)(\mathbb{Q}) \tag{4.24}$$

This involution has the fixed point

$$P = ((i+1)\theta^3 + 12i\theta^2 - 21(i-1)\theta + 66 : 3(i+1)\theta^3 + 36i\theta^2 - 63(i-1)\theta - 50 : 124). \tag{4.25}$$

Using branches, we will construct an isomorphism between the curve $(X; P)$ and its conjugates that satisfies the cocycle relation.

Let σ be the automorphism of K such that $\sigma(\theta) = i\theta$ and $\sigma(i) = i$; and similarly let $\tau(\theta) = \theta$ and $\tau(i) = -i$. Then σ and τ satisfy the standard relations for the dihedral group of order 8, the Galois group of the extension K.

One surprise here is that it is impossible to construct a Weil cocycle for the full extension $K \mid \mathbb{Q}$. In fact there exist isomorphisms $\varphi_\sigma : (\sigma(X); \sigma(P))$ and $\varphi_\tau : (\tau(X); \tau(P))$ but no matter which we take, the automorphism

$$\sigma^3(\varphi_\sigma)\sigma^2(\varphi_\sigma)\sigma(\varphi_\sigma)\varphi_\sigma \tag{4.26}$$

of X that corresponds to the cocycle relation for σ is never trivial, but always of order 2. This strongly suggests that we should find an extension L of $\mathbb{Q}$ with Galois group dihedral of order 16 into which K embeds. Such extensions do indeed exist; one can be found in the ray class field of $\mathbb{Q}(i)$ of conductor 42, obtained as the splitting field of the polynomial $63t^8 - 70t^4 - 9$ over $\mathbb{Q}$.

The above extension is exactly the one that shows up when considering the branches of the Belyĭ map $q : X \to \mathrm{Aut}(X)\backslash X$, which can be calculated by using the methods in Poonen–Schaefer–Stoll [23]. Note that it would have sufficed for our purposes to quotient out by the involution fixing P; however, we use the Belyĭ map to show that it, too, can be used for purposes of descent.

We use $x = s$ as a local parameter at the point P, and modify the coordinate on $\mathrm{Aut}(X)\backslash X$ such that P is sent to 0. After dehomogenizing by putting $z = 1$ and determining $y = y(s)$ as a power series in s, we obtain a power series expression in s for q by composition. This power series looks like

$$s \to c_2 s^2 + O(s^3) \tag{4.27}$$

The leading coefficient c_2 of this power series has minimal polynomial

$$27889t^4 - 1869588t^3 - 18805122t^2 + 1869795900t - 25658183943 \tag{4.28}$$

over the rationals. Since the branch is an inverse of the power series above under composition, it will look like

$$s \to (1/\sqrt{c_2})s^{1/2} + O(s). \tag{4.29}$$

The field generates by its leading coefficient can therefore be obtained as the splitting field of the polynomial (4.28) evaluated at t^2. This is indeed the extension L constructed above: we have

$$\frac{1}{\sqrt{c_2}} = \frac{1}{16032}(211239\eta^7 - 66339\eta^5 - 163835\eta^3 + 98343\eta) \tag{4.30}$$

where η is a root of $63t^8 - 70t^4 - 9$.

We now evaluate all fractional power series for x, y, z involved at the branch $(1/\sqrt{c_2})s^{1/2} + O(s)$ instead of s. This allows us to study the Galois action; by dehomogenizing and comparing the conjugated fractional power series $(\sigma(X)(s), \sigma(y)(s))$ with the fractional linear transformation of (x, y) under the automorphisms of X, we can read off which α_σ maps the former branch to the latter.

There exist elements $\widetilde{\sigma}, \widetilde{\tau}$ satisfying the relations for the dihedral group of order 16, generating the Galois group of L, and restricting to σ, τ on K. For these elements, the conjugate branch $(\widetilde{\sigma}(x)(s), \widetilde{\sigma}(y)(s))$, respectively $(\widetilde{\tau}(x)(s), \widetilde{\tau}(y)(s))$, is sent to $(x(s), y(s))$ by the ambient transformation

$$\alpha_{\widetilde{\sigma}} = \begin{pmatrix} -6 & -2\theta^2 + 2 & \theta^2 + 11 \\ 2\theta^2 + 2 & -10 & 3\theta^2 + 1 \\ -\theta^2 + 11 & -3\theta^2 + 1 & 2 \end{pmatrix}, \tag{4.31}$$

respectively

$$\alpha_{\widetilde{\tau}} = \begin{pmatrix} -6 & 2\theta^2 + 2 & -\theta^2 + 11 \\ -2\theta^2 + 2 & -10 & -3\theta^2 + 1 \\ \theta^2 + 11 & 3\theta^2 + 1 & 2 \end{pmatrix}. \tag{4.32}$$

In particular $\sigma(P)$, respectively $\tau(P)$, is sent to P by $\alpha_{\widetilde{\sigma}}$, respectively $\alpha_{\widetilde{\tau}}$. By uniqueness of $\alpha_{\widetilde{\sigma}}$ and $\alpha_{\widetilde{\tau}}$ when considering its action on the branches, we do get a Weil cocycle this time. Moreover, the corresponding descent leads to a rational branch of the Belyĭ map q. After calculating a coboundary and polishing the result, we get the model

$$X_0 : x^4 + 2x^3y + 3x^2y^2 + 2xy^3 + 18xyz^2 + 9y^2z^2 - 9z^4 = 0 \tag{4.33}$$

as in Poonen–Schaefer–Stoll [23]. The curve X_0 admits the point $(0 : 1 : 0)$, which is a rational branch for the quotient map $(x : y : z) \mapsto (x : y : z^2)$ to the curve

$$x^4 + 2x^3y + 3x^2y^2 + 2xy^3 + 18xyz + 9y^2z - 9z^2 = 0 \tag{4.34}$$

in $\mathbb{P}(1, 1, 2)$.

We do not give explicit isomorphisms with the models (4.22) and (4.23) here, as they are slightly unwieldy to write down; a matrix α_0 inducing an isomorphism $X \xrightarrow{\sim} X_0$ can be found by solving the equations

$$\begin{aligned} \alpha_0\alpha_\sigma &= \sigma(\alpha_0) \\ \alpha_0\alpha_\tau &= \sigma(\alpha_0) \end{aligned} \tag{4.35}$$

up to a scalar, where $\alpha_\sigma, \alpha_\tau \in \mathrm{PGL}_3(L) = \mathrm{Aut}(\mathbb{P}^2)(L)$ induce the isomorphisms σ, τ, respectively. The equations 4.35 are none other than (2.5). Once we lift the $\mathrm{PGL}_3(L)$-cocycle $\sigma \mapsto \alpha_\sigma$ to $\mathrm{GL}_3(L)$, then we can forget about the scalar factor, so that (4.35) can be solved by expressing the entries of α_0 as combinations of a $\mathbb{Q}$-basis of L. This in turn reduces solving (4.35) to solving a system of linear equations; it then remains to find a solution of relatively small height to find a reasonable descent morphism.

Remark 4.36. Lifting the cocycle $\sigma \mapsto \alpha_\sigma$ mentioned above to $\mathrm{GL}_3(L)$ is not trivial; for general plane curves it requires modifying an arbitrary set-theoretic lift by suitable scalars, which in turn comes down to determining the rational points on a certain conic. For plane quartics, however, things are slightly easier, since we can consider the morphism on the space of differentials that our cocycle induces.

The case of a ramification point of index 3 is considerably easier and yields the model

$$7x^3z + 3x^2y^2 - 3xyz^2 + y^3z - z^4 = 0, \tag{4.37}$$

on which the points $(1:0:0)$ and $(0:1:0)$ are fixed for the automorphism $(x:y:z) \mapsto (\omega^2 x : \omega y : z)$ where ω is a primitive cube root of unity. In this case, we do not insist on the branch being rational in order to get a nicer model for the marked curve.

Finally, the original model (4.22) already admits the rational point $(0:0:1)$, which is stable under the automorphism $(x:y:z) \to (\zeta_7^4 x : \zeta_7^2 y : \zeta_7 z)$ of order 7.

Remark 4.38. Yet another way to find the descent above is to diagonalize the automorphism 4.24 to the standard diagonal matrix with diagonal $(1, 1, -1)$, which can be done by a $\mathbb{Q}$-rational transformation. The 4 fixed points of the involution are then on the line $z = 0$. By transforming the coordinates x and y over $\overline{\mathbb{Q}}$ we can ensure that the involution remains given by the diagonal matrix $(1, 1, -1)$ and the set 4 points remains still defined over $\mathbb{Q}$, while also putting one of these points at $(0:1:0)$. This normalization reduces the automorphism group sufficiently to make the rest of the descent straightforward.

Wild branches and wild descent. Determining branches in the wild case is less intuitive than in the tame case. It turns out that branches can still be represented by certain power series, but this time the denominators of the exponents involved are unbounded—so although the branch belongs to the separable closure of the power series ring, it cannot be represented by a Puiseux series. We illustrate this principle by considering two examples.

Example 4.39. We start off with the standard Artin–Schreier extension

$$y^p - y = x. \tag{4.40}$$

The projection $f : (y, x) \to x$ is then unramified outside ∞, and in fact this is a Galois cover, with automorphism group generated by $(x, y) \mapsto (x, y + 1)$. Transforming coordinates to interchange 0 and ∞, the extension (4.40) becomes

$$y^p - yz^{p-1} = z^{p-1}. \tag{4.41}$$

Now the map f has $(y, z) \mapsto z$ is a Galois cover, unramified outside 0. Its automorphism group is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and a generator is given by $(y, z) \mapsto (y + z, z)$.

We want to find a solution to (4.41) in fractional power series with positive exponents. For this, we first set $y = cz^e$. This gives the equation

$$c^p z^{pe} - cz^{p-1+e} = z^{p-1}. \tag{4.42}$$

To get cancellation with z^{p-1}, the smallest among the exponents pe and $p-1+e$ has to equal $p-1$. Now since $e>0$ we can never have that the latter exponent does the job. We get that $e=1-p^{-1}$ and $c^p=1$, so we have our leading monomial $z^{1-p^{-1}}$ of y. Writing $y=z^{1-p^{-1}}+cz^e$ and continuing iteratively, we can expand the branch if we allow rational exponents of z with arbitrarily large powers of p in the denominator. We are tempted to write the formal expansion

$$y=\sum_{n=1}^{\infty} z^{1-p^{-n}}; \tag{4.43}$$

to be precise, we think of (4.43) as encoding a sequence given by its partial sums, each of which belongs to a ring $k(t^{1/p^n})$ for $n\in\mathbb{Z}_{\geq 0}$. These partial sums "converge" to a root of (4.41), but only in a formal sense.

The exponents pe and $p-1+e$ cancel mutually precisely when $e=1$, confirming Proposition 3.11 and recovering exactly the images of (4.43) under the automorphism group, to wit

$$y=cz+\sum_{n=1}^{\infty} z^{1-p^{-n}},\ c\in\mathbb{F}_p. \tag{4.44}$$

We see that the wildness of the ramification is reflected in the denominators of the exponents $1-p^{-n}$ being unbounded.

Example 4.45. As a second illustration, we use a family of hyperelliptic curves in characteristic 2 considered by Igusa [17], namely

$$y^2-y=x^3+ax+bx^{-1}. \tag{4.46}$$

This curve has a distinguished point at infinity. Igusa [17] proved that the family (4.46) contains duplicates; more precisely, modifying $(a,b)\mapsto(\zeta_3 a,\zeta_3^{-1}b)$ does not change the isomorphism class. The corresponding invariant subfield of $\mathbb{F}_2(a,b)$ is $\mathbb{F}_2(a^3,ab)$, and we will use the marked point at infinity to descend to this subfield.

Transforming projectively as before, we get the equation

$$X: x-xz=(b+abx^2+x^4)z^2. \tag{4.47}$$

The hyperelliptic quotient map is given by $(x,z)\mapsto x$, and the automorphism group (of either the curve or the marked curve) is generated by $(x,z)\mapsto(x,z/(z+1))$. Determining a branch, we obtain one fractional power series that starts as

$$z=b^{-1/2}x^{1/2}+b^{-3/4}x^{3/4}+\ldots; \tag{4.48}$$

this is again just a formal expression, and by "starts" we mean that we have written a partial sum (as in the previous example) containing the terms whose exponent has denominator at most 4.

Now note that from (4.47) it follows that the second branch can be obtained by replacing z by $z+c$, where

$$c=\frac{x}{b+ax^2+x^4}=b^{-1}x+ab^{-2}x^3+\ldots \tag{4.49}$$

Regardless, note that if we let σ be the automorphism sending (a,b) to $(\zeta_3 a,\zeta_3^{-1}b)$, there is an obvious isomorphism $\varphi_\sigma: X^\sigma\to X$ given by $(x,z)\mapsto(\zeta_3 x,z)$. There is of course a

second isomorphism $(x, z) \to (\zeta_3 x, z/(z+1))$. However, the first isomorphism respects the branches, as can indeed be seen by looking at the exponents in the corresponding expansions alone; since only the second branch above contains a multiple of x, only φ_σ can send it to its conjugate.

Taking a corresponding coboundary corresponding to the cocycle generated by σ is easy and comes down to substituting bx for x in (4.47). We get a descent

$$x - xz = (1 + abx^2 + b^3x^4)z^2 \tag{4.50}$$

in which the rational branch is clearly visible. Transforming back to Igusa's form, we get the representative family

$$y^2 - y = b^3x^3 + abx + x^{-1}. \tag{4.51}$$

Of course this family can also be obtained by immediate inspection; our purpose was to show that branches can still be used perfectly and explicitly as a tool for descent. Finding more general families of hyperelliptic curves in this way is a topic for future work.

5. Counterexamples

In this final section, we prove Theorem B and consider two (counter)examples that show that for general (non-singular) marked curves the conclusion of Theorem 1.10 is false. That is, we exhibit pointed curves (and associated pointed Belyĭ maps) that are defined over $\mathbb{C}$ and have field of moduli $\mathbb{R}$ with respect to the extension $\mathbb{C} \mid \mathbb{R}$, yet do not descend to $\mathbb{R}$. In the first example, neither the singular curve nor its normalization descends to $\mathbb{R}$; thus one can equip extra rigidification data that can be compatibly identified by the complex conjugate that maintains the obstruction to descent. In the second example, the curve itself is defined over $\mathbb{R}$ but the marked curve is not, so rigidifying by marking a point creates a descent problem where previously none existed.

First example: the curve does not descend. We will employ the criterion (2.8) of Weil descent with respect to the extension $\mathbb{C}|\mathbb{R}$.

Lemma 5.1. *Let W be a variety over $\mathbb{R}$ and let $\varrho \in \mathrm{Aut}(W)(\mathbb{R})$ have order 4. Suppose that $X \subseteq W$ is a curve over $\mathbb{C}$ such that $\varrho(\overline{X}) = X$ and $\mathrm{Aut}(X)(\mathbb{C}) = \langle \varrho^2|_X \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Suppose $P \in W(\mathbb{R}) \cap X(\mathbb{C})$ has $\varrho(P) = P$. Then both X and $(X; P)$ have field of moduli $\mathbb{R}$ with respect to the extension $\mathbb{C} \mid \mathbb{R}$ but neither descends to $\mathbb{R}$.*

Proof. By hypothesis, the map $\varphi = \varrho|_{\overline{X}}$ gives an isomorphism $\varphi : \overline{X} \xrightarrow{\sim} X$, and $\varphi(P) = \varrho(\overline{P}) = \overline{P} = P$ since $P \in W(\mathbb{R})$ and ϱ is defined over $\mathbb{R}$. We have $\overline{\varphi}\varphi = (\varrho^2)|_{\overline{X}} \neq 1$ on both W and X. Therefore φ does not give rise to a descent of X to $\mathbb{R}$. Neither does $\varphi' = \varrho^3|_{\overline{X}}$, since again it similarly satisfies $\overline{\varphi}'\varphi' = (\varrho^2)|_{\overline{X}} \neq 1$.

To show that $(X; P)$ does not descend to $\mathbb{R}$, it is enough to show that X does not descend to $\mathbb{R}$. Suppose that X_0 is a descent; then we would have an isomorphism $\varphi_0 : X \xrightarrow{\sim} (X_0)_{\mathbb{C}}$. Let $\omega = \varphi_0^{-1}\overline{\varphi_0}$, defined via the composition

$$\overline{X} \xrightarrow{\overline{\varphi_0}} \overline{(X_0)_{\mathbb{C}}} = (X_0)_{\mathbb{C}} \xrightarrow{\varphi_0^{-1}} X. \tag{5.2}$$

Then the cocycle condition $\overline{\omega}\omega = 1$ is satisfied, since $\overline{\omega} = \overline{\varphi_0}^{-1}\varphi_0$. But we also have $\varrho|_{\overline{X}}^{-1}\omega \in \mathrm{Aut}(X)(\mathbb{C})$, and by hypothesis, we have $\mathrm{Aut}(X)(\mathbb{C}) = \langle \varrho^2|_{\overline{X}} \rangle \simeq \mathbb{Z}/2\mathbb{Z}$; so either

$\omega = \varrho|_{\overline{X}} = \varphi$ or $\omega = \varrho^3|_{\overline{X}} = \varphi'$, and in either case we obtain a contradiction from the first paragraph. □

To give an explicit example of Lemma 5.1, we take $W = \mathbb{P}^2$ and the automorphism

$$\begin{aligned} \varrho : \mathbb{P}^2 &\to \mathbb{P}^2 \\ (x : y : z) &\to (y : -x : z). \end{aligned} \tag{5.3}$$

Lemma 5.4. *We have*

$$\{P \in \mathbb{P}^2(\mathbb{C}) : \varrho(P) = P\} = \{(0 : 0 : 1), (\pm i : 1 : 0)\}. \tag{5.5}$$

Proof. In the affine open where $z = 1$ we get the equations $y = x = -x$, whose unique solution is given by $x = y = 0$. On the other hand, when $z = 0$ we find $(x : y) = (y : -x) \in \mathbb{P}^1(\mathbb{C})$. This implies $x = iy$, and the result follows. □

By Lemma 5.4, the only point $P \in \mathbb{P}^2(\mathbb{R})$ with $\varrho(P) = P$ is $P = (0 : 0 : 1)$. Our curve $X \subseteq \mathbb{P}^2$ is a projective plane curve, defined by a homogeneous polynomial $h(x, y, z) \in \mathbb{R}[x, y, z]$ with $h(0 : 0 : 1) = 0$. The condition that $\varrho(\overline{X}) = X$ is equivalent to the condition that $h(y : -x : z)$ is a scalar multiple of $\overline{h}(x : y : z)$; for simplicity, we assume that

$$h(y : -x : z) = \overline{h}(x : y : z).$$

The condition that $\varrho^2|_X \in \mathrm{Aut}(X)(\mathbb{C})$ implies that

$$h(x : y : -z) = h(x : y : z).$$

We take $\deg h = 4$ so that $\mathrm{Aut}(X)(\mathbb{C})$ is finite. The above conditions then imply that

$$h(x, y, z) = ax^4 + \overline{a}y^4 + (bx^2 - \overline{b}y^2)xy + (cx^2 + \overline{c}y^2)z^2 + rx^2y^2 + sixyz^2 \tag{5.6}$$

with $a, b, c \in \mathbb{C}$ and $r, s \in \mathbb{R}$. We observe that $P = (0 : 0 : 1)$ is a singular point of X and P is a nodal double point if and only if $s^2 \neq -4|c|^2$.

To apply Lemma 5.1, we need to select coefficients of h such that X has no automorphisms beyond $\varrho^2|_X$; we will show this is true for a particular choice, which will then in fact imply that the resulting computations are true for a general choice, i.e., for the curve defined by equation (5.6) over $\mathbb{C}[a, b, c, r, s, \Delta^{-1}]$ where Δ is the discriminant of h. We consider the curve with

$$(a, b, c, r, s) = (0, i, 1 + i, 1, 2)$$

so that X is described by the homogeneous equation

$$X : i(x^2 + y^2)xy + ((1 + i)x^2 + (1 - i)y^2)z^2 + x^2y^2 + 2ixyz^2 = 0. \tag{5.7}$$

Standard techniques in computational algebraic geometry (we performed our computation in Magma [4]) show that P is the only singular point of X, so that X has geometric genus 2. We verify that $\mathrm{Aut}(X)(\mathbb{C}) \simeq \mathbb{Z}/2\mathbb{Z}$ by computing that the normalization of X over $\mathbb{R}$ is given by

$$Y : y^2 = (i + 1)x^5 + (-i - 1)x^4 + 4x^3 + (-i + 1)x^2 + (-i + 1)x \tag{5.8}$$

and by a computation using invariant theory (again a computation in Magma [19]) we see that indeed Y has automorphism group $\mathbb{Z}/2\mathbb{Z}$ generated by the hyperelliptic involution. Since every automorphism group of a singular curve lifts to its normalization, we see that indeed $\mathrm{Aut}(X)(\mathbb{C}) \simeq \mathbb{Z}/2\mathbb{Z}$. Lemma 5.1 therefore applies to show that 5.7 is an explicit counterexample.

Alternatively, one can compute that the Igusa–Clebsch invariants of Y are defined over $\mathbb{R}$, so that the field of moduli is $\mathbb{R}$, but that there is an obstruction to the curve Y being defined over $\mathbb{R}$, as described by Mestre [21]. On the other hand, one shows that the existence of a descent of Y is equivalent with that for X since P is the unique singular point of X.

Remark 5.9. With the equation (5.8) in hand, one sees how to recover this class of examples in a different way, as follows. Let W_0 be the conic defined by $x^2 + y^2 + z^2 = 0$ in $\mathbb{P}^2$ over $\mathbb{R}$. Then $W_0(\mathbb{R}) = \emptyset$. Let $S \subseteq W_0(\mathbb{C})$ be a subset of 6 distinct points over $\mathbb{C}$ forming 3 complex conjugate pairs. Then there exists a smooth hyperelliptic curve X' over $\mathbb{C}$ branched over the set S that does not descend to $\mathbb{R}$: this follows from work of Mestre [21], but it is also a rephrasing of the results by Shimura and Earle reviewed by Huggins [16, Chapter 5].

Now let $Q_1, Q_2 \in S$ be such that $Q_2 = \overline{Q_1}$ and let $P_1, P_2 \in X'(\mathbb{C})$ be their ramified preimages. By the cocycle condition, the points $\overline{P_1}, \overline{P_2} \in \overline{X'}(\mathbb{C})$ are mapped to $P_1, P_2 \in X'(\mathbb{C})$ under the isomorphism between $\overline{X'}$ and X'. Now pinch together the points P_1, P_2 to obtain a curve X over $\mathbb{C}$ with a double point P. Then $\overline{P} \in \overline{X}(\mathbb{C})$ is mapped to its conjugate P on X ("itself" on W_0) by construction, and so $(X; P)$ also has field of moduli $\mathbb{R}$.

To obtain a map $f : X \to \mathbb{P}^1$ unramified away from $\{0, 1, \infty\}$, thereby completing the first proof of Theorem , we first choose a function π on W defined over $\mathbb{R}$ that is invariant under ϱ and that is nonconstant on X. This yields a morphism $\pi|_X : X \to \mathbb{P}^1$, and because ϱ maps X to $\overline{X}$ and π is invariant under ϱ, the branch locus of $\pi|_X$ is invariant under complex conjugation.

In the specific example (5.7) above, we take $\pi = x^2 + y^2$ and compute that the branch locus is described by the vanishing of the homogeneous polynomial

$$3072u^7v + 4352u^6v^2 + 5840u^5v^3 + 3424u^4v^4 + 920u^3v^5 + 104u^2v^6 + 5uv^7, \tag{5.10}$$

which shows that it is in fact even stable under $\mathrm{Gal}(\overline{\mathbb{Q}}\,|\,\mathbb{Q})$.

We can now apply the following slight strengthening of the result of Belyĭ.

Theorem 5.11 (Belyĭ [2])**.** *Let $g : X \to \mathbb{P}^1$ be a map of curves over $\overline{\mathbb{Q}}$ whose branch locus in $\mathbb{P}^1(\overline{\mathbb{Q}})$ is defined over a number field $F \subset \overline{\mathbb{Q}}$. Then there exists a morphism $\alpha : \mathbb{P}^1 \to \mathbb{P}^1$ defined over F such that $f = \alpha \circ g$ is a Belyĭ map.*

Theorem 5.11 applies equally well to the extension $\mathbb{C}\,|\,\mathbb{R}$, essentially since every Belyĭ map is already defined over $\overline{\mathbb{Q}}$. We apply the above for $g = \pi$, whose branch locus is $\mathbb{R}$-rational, and let $f = \alpha\pi : X \to \mathbb{P}^1$ be the map thus obtained, unramified away from $\{0, 1, \infty\}$. Now f is ϱ-invariant since π is, and because we have $\overline{\pi} = \pi\varrho = \pi$ on W we also have

$$\overline{f}\,\varrho = \overline{\alpha\pi}\,\varrho = \alpha\overline{\pi}\,\varrho = \alpha\pi\varrho^2 = \alpha\pi = f. \tag{5.12}$$

So indeed the field of moduli of the pointed map $(X; f : X \to \mathbb{P}^1; P; 0, 1, \infty)$ with respect to the extension $\mathbb{C}\,|\,\mathbb{R}$ equals $\mathbb{R}$. However, because X does not descend to $\mathbb{R}$, neither does $(X; f; P; 0, 1, \infty)$.

Second example: the curve descends. In this second example, the curve itself descends but the marked curve does not. The setup is described by the following lemma.

Lemma 5.13. *Let X be a curve over $\mathbb{R}$ such that*

$$\mathrm{Aut}(X)(\mathbb{C}) = \mathrm{Aut}(X)(\mathbb{R}) = \langle\varrho\rangle \simeq \mathbb{Z}/4\mathbb{Z}. \tag{5.14}$$

Suppose that $P \in X(\mathbb{C}) \setminus X(\mathbb{R})$ satisfies $\overline{P} = \varrho(P)$. Then $(X_{\mathbb{C}}; P)$ has field of moduli $\mathbb{R}$ with respect to the extension $\mathbb{C}|\mathbb{R}$ but does not descend to $\mathbb{R}$.

Proof. The field of moduli claim follows by taking $\varphi = \varrho$ to be the identity map, since $\overline{X} = X$ and $\varrho(\overline{P}) = P$ as ϱ is defined over $\mathbb{R}$. Moreover, we have

$$P = \overline{\overline{P}} = \overline{\varrho(P)} = \varrho(\overline{P}) = \varrho^2(P). \tag{5.15}$$

It remains to show that $(X; P)$ does not descend to $\mathbb{R}$. For purposes of contradiction, suppose that $(X_0; P_0)$ is a descent. Then we have an isomorphism $\varphi_0 : X_{\mathbb{C}} \xrightarrow{\sim} (X_0)_{\mathbb{C}}$ such that $\varphi_0(P) = P_0$ satisfies $\overline{P_0} = P_0$. The composition $\varphi_0^{-1}\overline{\varphi_0} = \omega$ gives a map

$$X_{\mathbb{C}} = \overline{X}_{\mathbb{C}} \xrightarrow{\overline{\varphi_0}} \overline{(X_0)_{\mathbb{C}}} = (X_0)_{\mathbb{C}} \xrightarrow{\varphi_0^{-1}} X_{\mathbb{C}} \tag{5.16}$$

so $\omega \in \mathrm{Aut}(X)(\mathbb{C})$, and since $\overline{\omega} = \overline{\varphi_0}^{-1}\varphi_0$ we have $\omega\overline{\omega} = 1$. But since $\mathrm{Aut}(X)(\mathbb{C}) = \mathrm{Aut}(X)(\mathbb{R})$, we have that $\omega = \overline{\omega}$. Therefore the cocycle condition implies that ω is an involution. If $\omega = 1$ then $\overline{\varphi_0} = \varphi_0$ is defined over $\mathbb{R}$ so that under this isomorphism

$$\varphi_0(\overline{P}) = \overline{\varphi_0}(\overline{P}) = \overline{\varphi_0(P)} = \overline{P_0} = P_0 = \varphi_0(P), \tag{5.17}$$

a contradiction with our hypothesis $P \in X(\mathbb{C}) \setminus X(\mathbb{R})$. So we must have $\overline{\varphi_0} = \varphi_0\varrho^2$. But then by (5.15) and rationality of ϱ we would again have

$$\varphi_0(\overline{P}) = \varphi_0(\overline{\varrho^2(P)}) = \varphi_0(\overline{\varrho^2}(\overline{P})) = \varphi(\varrho^2(\overline{P})) = \overline{\varphi_0}(\overline{P}) = \overline{\varphi_0(P)} = P_0 = \varphi_0(P). \tag{5.18}$$

Therefore no descent of $(X; P)$ exists. □

Remark 5.19. Admitting for a moment that curves as in Lemma 5.13 do exist, we see that rigidifying by marking a point may very well lead to a descent problem where previously none existed: while both $(X_{\mathbb{C}}, P)$ and *a fortiori* $X_{\mathbb{C}}$ have field of moduli $\mathbb{R}$ with respect to the extension $\mathbb{C} \mid \mathbb{R}$, the obstruction vanishes for the non-marked curve $X_{\mathbb{C}}$, whereas it is non-trivial for the pair $(X_{\mathbb{C}}, P)$. So while non-marked curves $X_{\mathbb{C}}$ may not descend, as was noted by Birch [3], neither may a given rigidification of $X_{\mathbb{C}}$, as we saw in the last subsection, and in fact it may even complicate descent matters further when the automorphism group remains nontrivial.

To exhibit an explicit curve meeting the requirements of Lemma 5.13, we first construct a smooth curve Y defined over $\mathbb{R}$ with

$$\mathrm{Aut}(Y)(\mathbb{R}) = \mathrm{Aut}(Y)(\mathbb{C}) \simeq \mathbb{Z}/4\mathbb{Z}.$$

To do this, we choose distinct $x_1, x_2 \in \mathbb{C}$ and let

$$p(x) = (x^2 + 1)\prod_{i=1}^{2}(x - x_i)(x - \overline{x}_i)(x + 1/x_i)(x + 1/\overline{x}_i) \in \mathbb{R}[x]. \tag{5.20}$$

We see that $p(-1/x) = p(x)/x^{10}$. One then expects that generically the hyperelliptic curve

$$Y : y^2 = p(x)$$

will have automorphism group generated by $\varrho(x, y) = (-1/x, y/x^5)$. It is indeed possible to verify [19] that this indeed happens for the choice $x_1 = 1 + i, x_2 = 2 + i$, which (after scaling) yields the genus 4 hyperelliptic curve

$$Y : y^2 = 10x^{10} - 42x^9 + 67x^8 - 36x^7 + 23x^6 + 23x^4 + 36x^3 + 67x^2 + 42x + 10. \tag{5.21}$$

Consider the point $Q = (1+i, 0) \in Y(\mathbb{C})$. To get Lemma 5.13 to apply, we need $\overline{Q} = \varrho(Q)$. Of course this cannot be the case on Y in light of Theorem 1.10, but we can make it true by construction if we pinch together the points $\overline{Q}$ and $\varrho(Q)$. Moreover, if we take care to pinch Q with $\varrho(\overline{Q})$ similarly, then the resulting contraction morphism $c : Y \to X$ will be defined over $\mathbb{R}$. If we let $P = c(Q)$, then by construction, the pair $(X; P)$ will satisfy the conditions of Lemma 5.13. Indeed, any automorphism of a singular curve lifts to its normalization, and conversely the automorphisms of Y all transfer to X because of our construction of the contraction, so that indeed

$$\mathrm{Aut}(X)(\mathbb{R}) = \mathrm{Aut}(X)(\mathbb{C}) \simeq \mathrm{Aut}(Y)(\mathbb{C}) \simeq \mathbb{Z}/4\mathbb{Z};$$

the stabilizer of P again corresponds to the subgroup of $\mathbb{Z}/4\mathbb{Z}$ of order 2.

A contraction morphism c can be constructed in many different ways, none of which is particularly pleasing from the point of view of finding an equation. The first approach is to find a sufficiently ample linear system and extract the sublinear system of sections whose values at $\overline{Q}$ and $\varrho(Q)$ (resp. Q and $\varrho(\overline{Q})$) coincide. This leads to ambient spaces that are too large to give rise to attractive equations.

An alternative approach is as follows. Define

$$\begin{aligned} q(x) &= (x - x_1)(x - \overline{x}_1)(x + 1/x_1)(x + 1/\overline{x}_1) = x^4 - x^3 + \frac{1}{2}x^2 + x + 1, \\ r(x) &= \frac{2}{3}x^3 - 2x^2 + x. \end{aligned} \tag{5.22}$$

and let $c : \mathbb{A}^2 \to \mathbb{A}^4$ be given by

$$c(x, y) = (q(x), xq(x), r(x), y) = (t, u, v, w). \tag{5.23}$$

Given a point in the image of c, we can always read off the original y-coordinate from w. We can also recover the x-coordinate u/t as long as $t \neq 0$. The latter only occurs if x is a root of q; these roots all have the property that $t = u = w = 0$. On the other hand, one verifies that r assumes exactly two distinct values on this set of roots; moreover, the preimage of one of these values is given by $\{Q, \varrho(\overline{Q})\}$, and the other by $\{\overline{Q}, \varrho(Q)\}$. We see that the morphism c constracts the pairs $\{Q, \varrho(\overline{Q})\}$ and $\{\overline{Q}, \varrho(Q)\}$ exactly in the way that we wanted.

Of course this method gives only an affine open of X, but this open contains all the singular points that we are interested in, so that completing the corresponding model smoothly at infinity will give the model of X that is desired. On the patch $t \neq 0$ we can describe the image of c by the following equations:

$$\begin{aligned} t^5 - t^4 - t^3u - 1/2t^2u^2 + tu^3 - u^4 &= 0, \\ t^3v - t^2u + 2tu^2 - 2/3u^3 &= 0, \\ 10t^{10}w^2 - 10t^{10} - 42t^9u - 67t^8u^2 - 36t^7u^3 - 23t^6u^4 & \\ -23t^4u^6 + 36t^3u^7 - 67t^2u^8 + 42tu^9 - 10u^{10} &= 0. \end{aligned} \tag{5.24}$$

Adding a few more coordinates, we can also describe the automorphism ϱ: using the contraction

$$\begin{aligned} c(x, y) &= (q(x), xq(x), r(x), y, q(-1/x), -1/xq(-1/x), r(-1/x), y/x^5) \\ &= (t, u, v, w, t', u', v', w'), \end{aligned} \tag{5.25}$$

it can be described by

$$\varrho(t,u,v,w,t',u',v',w') = (t',u',v',w',t,u,v,-w). \tag{5.26}$$

In both cases, the full ideal of the image of c can be recovered by using Gröbner bases.

To conclude our argument; by Theorem 5.11, we can find a map $f : X \to \mathbb{P}^1$ unramified outside $\{0,1,\infty\}$ such that $(X,f;P)$ has the same automorphism group: one takes any function φ defined over $\mathbb{R}$ that is invariant under $\mathrm{Aut}(X,P)$ and postcompose with a function h following Belyĭ to get a map $\varphi = h\varphi_0$ with the same field of moduli and the same obstruction.

Remark 5.27. The curve in the first counterexample had exactly one singular point—in a sense, it was "marked" anyway. By contrast, the curve in this subsection has two singular points, which makes it important to keep track of the chosen marking.

Remark 5.28. There should be many more ways to construct singular curves over $\mathbb{R}$ for whom the field of moduli is no longer a field of definition after rigidification by a singular point.

For example, if we take the automorphism $\varrho : \mathbb{P}^3 \to \mathbb{P}^3$ given by the cyclic permutation of the coordinates $\varrho(x : y : z : w) = (y : z : w : x)$ and considers the generic complete intersection X of two polynomials invariant under ϱ containing the point $P = (1 : i : 1 : i)$ with $\varrho(P) = \overline{P}$, then we expect that the curve X will satisfy the hypotheses above. For example, if we define

$$\varrho(m) = m + \varrho^*(m) + (\varrho^{*2})(m) + (\varrho^{*3})(m) \tag{5.29}$$

for $m \in k[x,y,z,w]$ a monomial, then we believe that the curve X of genus 7 defined by

$$\begin{gathered} \varrho(x^2) = x^2 + y^2 + z^2 + w^2 = 0 \\ 5\varrho(x^4) + \varrho(x^3y) + \varrho(x^3z) - 4\varrho(x^2yw) - 2\varrho(x^2zw) + 3\varrho(x^2y^2) + 7\varrho(xyzw) = 0 \end{gathered} \tag{5.30}$$

has this property, as we can verify that $\mathrm{Aut}(X)(\mathbb{F}_p) \simeq \mathbb{Z}/4\mathbb{Z}$ for a number of large primes p; however, it is much more involved to provably compute the automorphism group for such a curve, which is why we have preferred to stick with this admittedly more special case.

Appendix: Descent of marked Galois Belyĭ maps in genus zero

In this appendix, we show how branches can be used to provide explicit descent of marked Galois Belyĭ maps in genus zero. The results are classical, but the method to derive them is quite pleasing so we provide it here.

As mentioned in the previous section, in the absence of unipotent automorphisms a geometrically generically Galois map $W \to V$ between curves of genus 0 over F^{sep} is always a quotient by one of the groups C_n, D_n, A_4, S_4, A_5. In fact all of these quotients are Belyĭ maps over F^{sep}, and in what follows we wish to consider some special descents of these maps. This will expand on the results in Couveignes–Granboulan [7], in which quite pleasing forms of these Belyĭ maps were already given.

We will slightly broaden our notion of Belyĭ maps over F in order to allow their branch divisor to be an arbitrary F-rational divisor instead of merely consisting of multiples of points individually defined over F.

Definition 5.31. A lax Belyĭ map over F is a map $f : X \to \mathbb{P}^1$ of curves defined over F that is ramified above at most three points. A marked lax Belyĭ map over F is a pair $(X;f;P)$, where $f : X \to \mathbb{P}^1$ is a lax Belyĭ map over F and $P \in X(F)$ is a point of X over F.

By Birch's theorem, any marked lax Belyĭ map descends to its field of moduli. In principle we could once more use the methods of branches to descend marked lax Belyĭ maps. However, it turns out that if we consider the case where X has genus 0, then things are much easier, essentially because we have an obvious descent $(\mathbb{P}^1, \infty)$ of $(X; P)$ that we can exploit. This leads to a useful and easily memorizable trick that resembles our approach to hyperelliptic curves in the previous section.

In what follows, we suppose that $f : X \to \mathbb{P}^1$ is a lax Belyĭ map with X of genus 0 such that f is geometrically generically Galois with field of moduli F with respect to the extension $F^{\mathrm{sep}} \,|\, F$. We suppose P is a ramification point of f of *non-trivial* order $n \in \mathbb{Z}_{\geq 2}$, which we suppose maps to $0 \in \mathbb{P}^1$ for the sake of simplicity. Our reasoning will now be very similar to that in section 4.

Using an automorphism of $\mathbb{P}^1$ if necessary, we can obtain a model $\mathbb{P}^1$ of X such that not only does P correspond to the point $(1 : 0)$ of X at infinity but additionally the automorphism group of $(X, f; P)$ is generated by $(x : z) \mapsto (\zeta_n x : z)$ with ζ_n a primitive nth root of unity. This means that if we let t be the affine coordinate z/x the function f can be identified with a power series expansion

$$f(t) = \sum_{i=1}^{\infty} c_i t^{in}. \tag{5.32}$$

Because $f(P) = 0$, we have $c_i = 0$ for $i \leq 0$.

Since $\mathrm{Aut}(X, f; P)(F^{\mathrm{sep}}) \simeq \mathbb{Z}/n\mathbb{Z}$, the set $\{i \geq 1 : c_i \neq 0\}$ generates $\mathbb{Z}$ as a group. So there exists a finite subset I of this set with this property as well. Let $c_I = (c_i)_{i \in I}$ be the corresponding point in the projective space weighted by its indices, and choose a normalized representative $c_{I,0}$ of c_I [18]. There exists a scaling $t \mapsto \alpha t$ of t that transforms c_I into $c_{I,0}$, which is uniquely determined up to a power of the automorphism $t \mapsto \zeta_n t$ since the elements in I generate $\mathbb{Z}$.

Proposition 5.33. *With notations as above, let*

$$f_0(t) = f(\alpha t) = \sum_{i=1}^{\infty} c_{i,0} t^{in}. \tag{5.34}$$

Then f_0 has coefficients in F and $(X, f_0; \infty)$ is a descent of $(X, f; P)$.

Proof. Any isomorphism between f_0 and its conjugate $\sigma(f_0)$ normalizes the group of automorphisms generated by $(x : z) \mapsto (\zeta_n x : z)$ and fixes $(1 : 0) \in \mathbb{P}^1(x : z)$. Therefore it is given by a scaling $t \mapsto \alpha_\sigma t$. The subset c_I is defined over F, and in particular it is fixed by Galois conjugation. By uniqueness of the normalized representative, we therefore see that α_σ is a power of ζ_n, and in particular that f_0 is stable under conjugation by σ. Since σ was arbitrary, we see that indeed f_0 is defined over F. □

In what follows, we exhibit descents of all the geometrically generically Galois lax Belyĭ maps of genus 0, ordered by their automorphism group G under the hypothesis that G does not contain any unipotent elements. We impose an ordering of the corresponding branch indices b_0, b_∞, b_1. Then we give a number of equalities of the form

$$f_0 - f_\infty = f_1.$$

These equations will represent a rational function $f = f_0/f_\infty$ that is ramified over three individually F-rational points, which we may and do put at $0, \infty, 1$. The polynomial functions f_0, f_∞, f_1 will show the ramification behavior over these three points, which will be uniform of branch index b_0, b_∞, b_1. In some cases, we will only give a single triple, usually when that triple already has obvious rational points over $0, \infty, 1$. But when normalizing requires more work, we will give three triples f_0, f_∞, f_1.

The branch point on $\mathbb{P}^1$ that is the image of the marked point P will always be rational over the field of moduli; this was also the reason that we did not consider conics as the target space in our Definition 5.31. However, by our relaxation of the condition in Definition 5.31 it is possible that the other two branch points are conjugate over F if they have the same branch indices, which leads to further twists. In this case, we put the points with coinciding branch indices at 0 and ∞ in the first triples. We then change f to $\sqrt{d}(f+1)/(f-1)$, which moves the branch point 1 to ∞ and the pair $0, \infty$ to $\pm\sqrt{d}$. Normalizing again, we get our twists.

Case $G \simeq C_n$. We have the obvious triple with branch indices $n, n, 1$:

$$t^n - 1 = (t^n - 1). \tag{5.35}$$

Twisting this map to get it to ramify over $\pm\sqrt{d}$ is actually not so straightforward as the procedure above, essentially because there is no branching over 1, so that we cannot apply our normalization argument. However, a corresponding lax Belyĭ map was constructed by Lercier–Ritzenthaler–Sijsling [20, Proposition 3.16]. We pass over this case here since the corresponding points have trivial ramification index.

Case $G \simeq D_n$. The branch indices are now equal to $n, 2, 2$. Putting the indices 2 at $0, \infty$ and n at 1, we get the triples

$$f(t) = \frac{(t^n - 1)^2}{(t^n + 1)^2}. \tag{5.36}$$

This map admits two rational points $0, \infty$ over 1. Moreover, there is the rational point 1 over 0, and by exchanging the roles of 0 and ∞ we get a rational point over ∞. Twisting gives the function

$$f(t) = \frac{dt^{2n} + 1}{2t^n} \tag{5.37}$$

which indeed branches of index n over ∞ and moreover of index 2 over $\pm\sqrt{d}$ since

$$(dt^{2n} + 1) \pm 2\sqrt{d}t^n = (\pm\sqrt{d}t^n + 1)^2. \tag{5.38}$$

Case $G \simeq A_4$. This case has branch indices $2, 3, 3$. We put the indices 3 at $0, \infty$ and 2 at 1 to get

$$(t(t^3 + 8))^3 - 2^6(t^3 - 1)^3 = (t^6 - 20t^3 - 8)^2. \tag{5.39}$$

Permuting f_0 and f_∞ gives rise to a rational point over 0, while a triple that has the rational point ∞ over 1 is given by

$$(3t^4 - 6t^2 - 1)^3 - (3t^4 + 6t^2 - 1)^3 = -2^2 3^2 (t(3t^4 + 1))^2. \tag{5.40}$$

The corresponding family of twists branching over ∞ and $\pm\sqrt{d}$ is given by

$$f(t) = \frac{-d^3t^{12} - 99d^2t^8 + 297dt^4 + 27}{18(d^2t^{10} + 6dt^6 + 9t^2)}. \tag{5.41}$$

Case $G \simeq S_4$. For this case, the branch indices $2, 3, 4$ are distinct, so we do not get extra twists, but only the three following triples:

$$(t^8 + 14t^3 + 1)^3 - 2^2 3^3 (t(t^4 - 1))^4 = (t^{12} - 33t^8 - 33t^4 + 1)^2, \tag{5.42}$$

$$-2^8(t^7 + 7t^4 - 8t)^3 - (t^6 - 20t^3 - 8) = (t^{12} + 88t^9 + 704t^3 - 64)^2, \tag{5.43}$$

and

$$\begin{aligned}(3t^8 + 28t^6 - 14t^4 + 28t^2 + 3)^3 - 3^3(t^6 - 5t^4 - 5t^2 + 1)^4 \\ = 2^4(9t^{11} + 11t^9 + 66t^7 - 66t^5 - 11t^3 - 9t)^2.\end{aligned} \tag{5.44}$$

Case $G \simeq A_5$. Once more the branch indices $2, 3, 5$ are distinct. We get the following triples:

$$\begin{aligned}(t^{20} + 228t^{15} + 494t^{10} - 228t^5 + 1)^3 - 2^6 3^3 (t(t^{10} - 11t^5 - 1)) \\ = t^{30} - 522t^{25} - 10005t^{20} - 10005t^{10} + 522t^5 + 1,\end{aligned} \tag{5.45}$$

and

$$\begin{aligned}- 5^3(t(5t^6 - 5t^3 + 8)(40t^6 + 5t^3 + 1)(5t^6 + 40t^3 - 1))^3 \\ - 2^6(25t^{12} - 275t^9 - 165t^6 + 55t^3 + 1)^5 \\ = -\big(5t^6 + 1)(200t^{12} + 500x^9 + 2055t^6 - 100t^3 + 8)\cdot \\ (25t^2 + 1750t^9 - 2190t^6 - 350t^3 + 1)\big)^2,\end{aligned} \tag{5.46}$$

and finally

$$\begin{aligned}\big((3t^4 - 10t^2 + 15)(t^8 - 60t^6 - 370t^4 - 300t^2 + 25)(t^8 + 70t^4 + 25)\big)^3 \\ - 2^2\big(t(t^4 - 5)(9t^4 + 10t^2 + 5)(t^4 + 10t^2 + 45)\cdot \\ (t^8 - 20t^6 + 470t^4 - 500t^2 + 625)(5t^8 - 20t^6 + 94t^4 - 20t^2 + 5)\big)^2 \\ = 3^3\big((t^4 + 2t^2 + 5)(t^8 + 20t^6 - 210t^4 + 100t^2 + 25)\big)^4.\end{aligned} \tag{5.47}$$

The above method extends to curves and Belyĭ maps of genus 0 with unipotent automorphism group, and to higher genus (hyperelliptic or not). We expect this will be useful in building databases of Belyĭ maps with small defining equations, a topic for future work.

References

[1] G.V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Math. USSR-Izv. **14** (1980), no. 2, 247–256.

[2] G.V. Belyĭ, *A new proof of the three-point theorem*, translation in Sb. Math. **193** (2002), no. 3–4, 329–332.

[3] Bryan Birch, *Noncongruence subgroups, covers and drawings*, in *The Grothendieck theory of dessins d'enfants (Luminy, 1993)*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge Univ. Press, Cambridge, 1994, 25–46.

[4] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (3–4), 1997, 235–265.

[5] Kevin Coombes and David Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), no. 4, 821–839.

[6] Jean-Marc Couveignes, *Calcul et rationalité de fonctions de Belyi en genre 0*, Annales de l'Institut Fourier (Grenoble) **44** (1994), no. 1, 1–38.
[7] Jean-Marc Couveignes and Granboulan, *Dessins from a geometric point of view*, in *The Grothendieck theory of dessins d'enfants*, London Math. Soc. Lecture Note Ser., vol. 200, Cambridge University Press, 1994, 79–113.
[8] Pierre Dèbes and Jean-Claude Douai, *Algebraic covers: field of moduli versus field of definition*, Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338.
[9] Pierre Dèbes and Michel Emsalem, *On fields of moduli of curves*, J. Algebra **211** (1999), no. 1, 42–56.
[10] P. Deligne, *Le groupe fondamental de la droite projective moins trois points*, in *Galois Groups over* $\mathbb{Q}$, MSRI Publ. 16 (1989), 79-–297.
[11] Noam D. Elkies, *The Klein quartic in number theory*, in *The eightfold way*, 51–101, Math. Sci. Res. Inst. Publ., 35, Cambridge Univ. Press, Cambridge.
[12] Alexandre Grothendieck, *Sketch of a programme (translation into English)*, in *Geometric Galois actions 1*, eds. Leila Schneps and Pierre Lochak, London Math. Soc. Lect. Note Series, vol. 242, Cambridge University Press, Cambridge, 1997, 243–283.
[13] Alexandre Grothendieck, *Techniques de construction et théorèmes d'existence en géométrie algébrique III: préschémas quotients*, Séminaire N. Bourbaki, 1960–1961, exp. no. 212, 99–118.
[14] Alexandre Grothendieck, *Techniques de construction et théorèmes d'existence en géométrie algébrique IV: les schémas de Hilbert*, Séminaire N. Bourbaki, 1960–1961, exp. no. 221, 249–276.
[15] Rubén A. Hidalgo and Sebstian Reyes, *A constructive proof of Weil's Galois descent theorem.* Preprint at `http://arxiv.org/abs/1203.6294`. Preprint, 2012.
[16] Bonnie Huggins, *Fields of Moduli and Fields of Definition of Curves*, Ph.D. thesis, University of California, Berkeley, 2005.
[17] Jun-Ichi Igusa, *Arithmetic Variety of Moduli for Genus Two*, Annals of Mathematics, Vol. 72, No. 3 (1960), 612–649.
[18] Reynald Lercier and Christophe Ritzenthaler, *Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects.* Journal of Algebra, 372(0):595-636, December 2012.
[19] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling, *Fast computation of isomorphisms of hyperelliptic curves and explicit descent.* ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium, 463-486, 2013.
[20] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling, *Explicit Galois obstruction and descent for hyperelliptic curves with tamely cyclic reduced automorphism group*, `arXiv:1301.0695`, 2013.
[21] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, in *Effective methods in algebraic geometry*, volume 94 of *Prog. Math.*, 313–334, Boston, 1991. Birkhäuser.
[22] James S. Milne, *Lectures on Etale Cohomology (v2.10)*, 2008. Available at `http://www.jmilne.org/math/`, 196 pp.
[23] Bjorn Poonen, Edward F. Schaefer, and Michael Stoll, *Twists of* $X(7)$ *and primitive solutions to* $x^2 + y^3 = z^7$, Duke Math. J. **137** (2007), no. 1, 103–158.
[24] Bounab Sadi, *Descente effective du corps de définition des revêtements galoisiens*, J. Number Theory **77**(1), 1999, 71–82.
[25] Jean-Pierre Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics 117, Springer, 1988.
[26] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics 67, Springer, 1979.
[27] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics 1, Jones and Bartlett, 1992.
[28] Jeroen Sijsling and John Voight, *On computing Belyi maps*, Publ. Math. Besançon: Algèbre Théorie Nr. 2014/1, Presses Univ. Franche-Comté, Besançon, 73–131.
[29] Mark van Hoeij and Raimundas Vidunas, *Algorithms and differential relations for Belyi functions*, `arxiv:1305.7218v1`, 2013.
[30] André Weil, *The field of definition of a variety*, Amer. J. Math. 78, 1956, 509–524.

Mathematics Institute, Zeeman Building, University of Warwick, Coventry CV4 7AL, UK; Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: sijsling@gmail.com

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA

E-mail address: jvoight@gmail.com