ON THE PROFINITE REGULAR INVERSE GALOIS PROBLEM

ANNA CADORET

anna.cadoret@math.u-bordeaux1.fr
Univ. Bordeaux 1, Laboratoire A2X, I.M.B., 351 Cours de la libération, F-33405 Talence cedex, FRANCE.[1]

Abstract. Given a field k, a k-curve X and a k-rational divisor $\mathbf{t} \subset X$, we analyze the constraints imposed on X and $\mathbf{t}$ by the existence of abelian G-covers $f : Y \to X$ defined over k and unramified outside $\mathbf{t}$. We show that these constraints produce an obstruction to the weak regular inverse Galois problem for a whole class of profinite groups - we call p-obstructed - when k is a finitely generated field of characteristic $\neq p$.

2000 *Mathematics Subject Classification.* Primary: 12F12; Secondary:12G05, 14K15.

Introduction

Given a field k, we will always assume that a separable closure $\overline{k}/k$ is fixed and denote by Γ_k the absolute Galois group of k. A k-curve means a smooth, projective, geometrically connected k-scheme of dimension 1.

Given a field k and a k-curve X, recall that *a k-G-extension of $k(X)$* is a Galois extension $E/k(X)$ regular over k (*i.e.* such that k is algebraically closed in E). Then, given a (pro)finite group G, the regular inverse Galois problem for G over X can be stated as follows:

(RIGP$/G/X$) *There exists a k-G-extension $E/k(X)$ with group G.*

One can state weaker versions of the regular inverse Galois problem by allowing, for instance, the k-curve X to vary.

(W-fod RIGP$/G/k$) *There exists a k-curve X_G and a k-G-extension $E/k(X_G)$ with group G.*

Or, even, by only requiring the G-extension to have field of moduli k.

(W-fom RIGP$/G/k$) *There exists a k-curve X_G and a $\overline{k}$-G-extension $E/\overline{k}(X_G)$ with group G and field of moduli k.*

(In our notation, the prefixes "W-fod" and "W-fom" stand for "weak version for fields of definition" and "weak version for fields of moduli" respectively).

A standard descent argument based on Bertini-Noether theorem shows that for a finite group G and a field k the (W-fod RIGP$/G/k$) can be deduced from the (RIGP$/G/\mathbb{P}^1_{k((T))}$) (which is proved in [13])[2]. In [7], partial results are obtained for the (RIGP$/G/\mathbb{P}^1_{k((T))}$) when G is profinite (not finite) but the descent argument for profinite G no longer works. There are also very few profinite groups G for which direct constructive proofs of the (W-fod RIGP$/G/k$) have been given when k is "arithmetically interesting" (*cf.* for instance [10] for non trivial examples). In this note we show that, actually, such profinite groups are rather exceptional.

[1]Partially supported by JSPS fellowship P06033

[2]Alternatively, this result can be deduced from the (RIGP$/\mathcal{S}_n/\mathbb{P}^1_k$), where $\mathcal{S}_n$ denotes the symmetric group of order $n!$ and the fact that any finite group G can be embedded into $\mathcal{S}_n$ for some $n \geq 1$.

More precisely, our main result (theorem 3.5) is the following.

Theorem: *Let p be a prime. Then the* (W-fom RIGP$/G/k$) *fails for any finitely generated field k of characteristic $\neq p$ and any profinite group G containing an open subgroup $U \subset G$ with $U \twoheadrightarrow \mathbb{Z}_p$.*

In the sequel, we will refer to profinite groups G satisfying the hypotheses of the theorem as being *p-obstructed*. Typical examples of p-obstructed profinite groups are universal p-Frattini covers of finite groups of order divisible by p or pronilpotent projective groups of order divisible by p.

In particular, as $\mathbb{Z}_p$ is p-obstructed, one obtains the following statement (which is, actually, equivalent to our main result).

Corollary: *Let p be a prime and let k be a finitely generated field of characteristic $\neq p$. Then, for any k-curve X, its function field $\overline{k}(X)$ over $\overline{k}$ has no $\mathbb{Z}_p$-extension with field of moduli k.*

The paper is organized as follows. In section 1, we recall a few basics about G-curves and G-covers. In section 2, we analyze the constraints imposed by the existence of an abelian G-cover $f : Y \to X$ defined over k on X and the ramification divisor $\mathbf{t}$ of f; these are what we refer to as the *abelian constraints for $X \setminus \mathbf{t}$*. These constraints are too rigid to allow the existence of projective systems $(f_n : Y_n \to X)_{n\geq 0}$ of degree p^n cyclic G-covers defined over k, $n \geq 0$, which is enough to prove our statement for the (W-fod RIGP$/G/k$) (corollary 2.7).

In section 3.2, we deduce the statement for the (W-fom RIGP$/G/k$) (theorem 3.5) from the statement for the (W-fod RIGP$/G/k$) using a profinite generalization of the classical cohomological obstruction for a G-cover to be defined over its field of moduli. We carry out the construction of this obstruction in section 3.1.2. We conclude by giving a moduli formulation of our main result (corollary 3.6) using variants of the techniques of [3].

Acknowledgments

I would like to thank A. Tamagawa for his constructive suggestions and comments.

1. Basic definitions and notation

1.1. **G-curves and G-covers.** Let S be a connected scheme. An *S-curve* of genus g is a smooth, projective, geometrically connected S-scheme of dimension 1 whose geometric fibers have genus g.

Given a finite group G of order prime to the characteristics of S, an *S-G-curve with group G* is a pair (Y, α), where Y is an S-curve and $\alpha : G \hookrightarrow \mathrm{Aut}_S(Y)$ is a group monomorphism. Two S-G-curves (Y_i, α_i), $i = 1, 2$ with the same group G are *S-G-isomorphic* if there exists an S-scheme isomorphism $u : Y_1 \to Y_2$ such that $u\alpha_1(g)u^{-1} = \alpha_2(g)$, $g \in G$. An *S-G-cover with group G* is a pair $(f : Y \to X, \alpha)$, where $f : Y \to X$ is a Galois cover of S-curves and $\alpha : G \tilde{\to} \mathrm{Aut}_X(Y)$ is a group isomorphism. Two S-G-covers $(Y_i \to X, \alpha_i)$, $i = 1, 2$ of a given S-curve X with the same group G are *S-G-isomorphic* if there exists an X-scheme isomorphism $u : Y_1 \to Y_2$ such that $u\alpha_1(g)u^{-1} = \alpha_2(g)$, $g \in G$. Two S-G-covers $(Y_i \to X_i, \alpha_i)$, $i = 1, 2$ with the same group G are *weakly S-G-isomorphic* if there exists an S-scheme isomorphism $v : X_1 \to X_2$ such that the S-G-covers $(v \circ f_1 : Y_1 \to X_2, \alpha_1)$ and $(f_2 : Y_2 \to X_2, \alpha_2)$ are S-G-isomorphic. The groupoid of S-G-curves with group G and S-G-isomorphisms is then equivalent to the groupoid of S-G-covers with group G and weak S-G-isomorphisms. In the following, we will drop the α in our notation though it remains part of the data.

Assume now that $S = \mathrm{spec}(k)$ is the spectrum of a field and fix a geometric generic point $\overline{\xi}$: $\mathrm{spec}(\overline{k(X)}) \to X$. Then, for any k-rational divisor $\mathbf{t} \subset X$ one has the fundamental short exact sequence from Galois theory:

$$1 \longrightarrow \pi_1(X_{\overline{k}} \setminus \mathbf{t}, \overline{\xi}) \longrightarrow \pi_1(X \setminus \mathbf{t}, \overline{\xi}) \longrightarrow \Gamma_k \longrightarrow 1. \tag{1}$$

In our situation, writing $M_{k,X,\mathbf{t}}/\overline{k}(X)$ for the maximal separable extension of $\overline{k}(X)$ in $\overline{k(X)}$ unramified outside $\mathbf{t}$, $\pi_1(X_{\overline{k}} \setminus \mathbf{t}, \overline{\xi})$ and $\pi_1(X \setminus \mathbf{t}, \overline{\xi})$ are simply the Galois groups of $M_{k,X,\mathbf{t}}/\overline{k}(X)$ and $M_{k,X,\mathbf{t}}/k(X)$

respectively. In the following, we will drop the $\overline{\xi}$ in our notation.

The function field functor defines an equivalence between the groupoids:

- (C1) of G-covers of $X \to k$ defined over k with group G and unramified outside $\mathbf{t}$.
- (C2) of continuous group epimorphisms $\Phi : \pi_1(X \setminus \mathbf{t}) \twoheadrightarrow G$ such that $\Phi(\pi_1(X_{\overline{k}} \setminus \mathbf{t})) = G$; in the following, we will call such epimorphisms*regular epimorphisms*.

In the category (C1) morphisms are k-G-isomorphisms and in the category (C2) a morphism from Φ_1 to Φ_2 is an element $g \in G$ such that $g\Phi_1(\cdot)g^{-1} = \Phi_2$. Those two groupoids are also equivalent to the groupoid (C3) of k-G-extensions $E/k(X)$ with group G, unramified outside $\mathbf{t}$ together with isomorhisms of $k(X)$-extensions. Depending on the context, we will adopt one point of view or another.

1.2. **Inertia canonical invariant.** Fix a compatible system $(\zeta_n)_{n\geq 1}$ of primitive roots of unity in $\overline{k}$ (that is $\zeta_{nm}^n = \zeta_m$, $n, m \geq 1$).

Assume first that k is of characteristic 0. By Riemann's existence theorem, $\pi_1(X_{\overline{k}} \setminus \mathbf{t})$ is the profinite completion of the group defined by the generators $u_1, ..., u_g, v_1, ..., v_g, \gamma_{t_1}, ..., \gamma_{t_r}$ with the single relation $[u_1, v_1] \cdots [u_g, v_g]\gamma_{t_1} \cdots \gamma_{t_r} = 1$, where g is the genus of X and $\mathbf{t}_{\overline{k}} = \{t_1, \ldots, t_r\}$. For each $t \in \mathbf{t}_{\overline{k}}$, the element γ_t is a *distinguished generator* of the inertia group $I(\tilde{t}|t)$ at some place $\tilde{t}$ of $M_{k,X,\mathbf{t}}$ above t. Write $M_{k,X,\mathbf{t}}$ as a countable union of finite Galois extensions $M_{k,X,\mathbf{t}} = \bigcup_{n\geq 0} M_{k,X,\mathbf{t},n}$ and let $\tilde{t}_n$ denote the restriction of $\tilde{t}$ to $M_{k,X,\mathbf{t},n}$, $n \geq 0$. Fix a compatible sytem $(u_{t,n})_{n\geq 0}$ of uniformizing parameters of the $\tilde{t}_n$, $n \geq 0$ (that is $u_{t,n+1}^{e_{t,n+1}/e_{t,n}} = u_{t,n}$, where $e_{t,n}$ denote the order of the inertia group $I(\tilde{t}_n|t)$ of $\tilde{t}_n$ over t, $n \geq 0$). Then, by distinguished we mean that γ_t is the preimage of $(\zeta_{e_{t,n}})_{n\geq 0}$ *via* the group isomorphism $I(\tilde{t}|t)\tilde{\to}\varprojlim \mu_{e_{t,n}}$, $\omega \to (\frac{\omega(u_{t,n})}{u_{t,n}} \bmod \tilde{t}_n)_{n\geq 0}$. Let $f : Y \to X$ be a G-cover over k unramified outside $\mathbf{t}$ inducing a continuous group epimorphism $\Phi : \pi_1(X_{\overline{k}} \setminus \mathbf{t}) \twoheadrightarrow G$ then the conjugacy class C_t of $\Phi(\gamma_t)$ in G is called the *inertia canonical class* of f at $t \in \mathbf{t}$ and the r-tuple $\mathbf{C} = (C_t)_{t\in\mathbf{t}}$ is called the *inertia canonical invariant* of f.

If k is of characteristic $l > 0$, write $M_{k,X,\mathbf{t}}^{tame}/\overline{k}(X)$ for the maximal algebraic subextension of $M_{k,X,\mathbf{t}}/\overline{k}(X)$ at most tamely ramified at $\mathbf{t}$ (and unramified outside $\mathbf{t}$) and $\pi_1^{tame}(X_{\overline{k}} \setminus \mathbf{t})$ for the corresponding tame quotient of $\pi_1(X_{\overline{k}} \setminus \mathbf{t})$. Then there exists a discrete valuation ring R with residue field $\overline{k}$ and fraction field K of characteristic 0 such that the $\overline{k}$-curve $X_{\overline{k}}$ can be lifted to a R-curve $\tilde{X}$ and $\mathbf{t}_{\overline{k}}$ can be lifted to r K-rational distinct points $\tilde{\mathbf{t}} = \{\tilde{t}_1, \ldots, \tilde{t}_r\}$ on $\tilde{X}$. This yields a specialization epimorphism $\pi_1(\tilde{X}_{\overline{K}} \setminus \tilde{\mathbf{t}}_{\overline{K}}) \twoheadrightarrow \pi_1^{tame}(X_{\overline{k}} \setminus \mathbf{t})$ inducing an isomorphism on the prime-to-l parts $\pi_1(\tilde{X}_{\overline{K}} \setminus \tilde{\mathbf{t}}_{\overline{K}})^{(l')} \tilde{\to} \pi_1^{tame}(X_{\overline{k}} \setminus \mathbf{t})^{(l')}$. In particular, the inertia canonical invariant of a G-cover with group of prime-to-l order is still well-defined.

1.3. **Projective systems of G-covers.** The considerations of paragraphs 1.1 and 1.2 extend naturally to the profinite situation. More precisely, given a complete (that is, such that each transition morphism is an epimorphism) projective system of finite groups $(G_{n+1} \twoheadrightarrow G_n)_{n\geq 0}$, set $G := \varprojlim G_n$. Then any k-G-extension $E/k(X)$ can be written as a union $E = \bigcup_{n\geq 0} E_n/k(X)$, where E_n denotes the subfield of E fixed by the kernel of $G \twoheadrightarrow G_n$, $n \geq 0$. This, in turn, corresponds to a projective system $E = (f_n : Y_n \to X)_{n\geq 0}$ of G-covers defined over k with group G_n and ramification divisor say $\mathbf{t}_n$ or, alternatively, to a projective system of regular epimorphisms $(\Phi_n : \pi_1(X \setminus \mathbf{t}_n) \twoheadrightarrow G_n)_{n\geq 0}$. Here, projective means that one gets commutative diagrams:

$$\begin{array}{ccc} \pi_1(X \setminus \mathbf{t}_{n+1}) & \xrightarrow{e_n} & \pi_1(X \setminus \mathbf{t}_n) \\ \downarrow{\scriptstyle \Phi_{n+1}} & & \downarrow{\scriptstyle \Phi_n} \\ G_{n+1} & \twoheadrightarrow & G_n \end{array},$$

where $e_n : \pi_1(X \setminus \mathbf{t}_{n+1}) \twoheadrightarrow \pi_1(X \setminus \mathbf{t}_n)$ is the canonical restriction epimorphism defined by the inclusions $M_{k,X,\mathbf{t}_n} \subset M_{k,X,\mathbf{t}_{n+1}}$, $n \geq 0$ (with the notation of paragraph 1.1).

Thus, introducing

$$M = \bigcup_{n\geq 0} M_{k,X,\mathbf{t}_n}$$

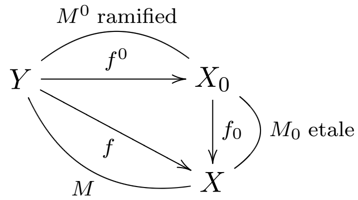
and $\pi_1(X\setminus \underline{\mathbf{t}}) := \varprojlim \pi_1(X\setminus \mathbf{t}_n) = \mathrm{Gal}(M|k(X))$, $\pi_1(X_{\overline{k}}\setminus \underline{\mathbf{t}}) := \varprojlim \pi_1(X_{\overline{k}}\setminus \mathbf{t}_n) = \mathrm{Gal}(M|\overline{k}(X))$,

projective systems of regular epimorphisms $(\Phi_n : \pi_1(X\setminus \mathbf{t}_n) \twoheadrightarrow G_n)_{n\geq 0}$ correspond to continuous group epimorphisms $\Phi : \pi_1(X\setminus \underline{\mathbf{t}}) \twoheadrightarrow G$ such that $\Phi(\pi_1(X_{\overline{k}}\setminus \underline{\mathbf{t}})) = G$ (which we still refer to as "regular epimorphisms") *etc.*. In particular, note that we still have the short exact sequence from Galois theory:

$$1 \longrightarrow \pi_1(X_{\overline{k}}\setminus \underline{\mathbf{t}}) \longrightarrow \pi_1(X\setminus \underline{\mathbf{t}}) \longrightarrow \Gamma_k \longrightarrow 1. \quad (2)$$

2. Abelian constraints

From now on fix a field k, a finite abelian group M of order prime to the characteristic of k, a k-curve X and a G-cover $f : Y \to X$ with group M, ramification divisor $\mathbf{t}$ and inertia canonical invariant $\mathbf{C} = (\{\omega_t\})_{t\in\mathbf{t}}$. Let $M^0 \subset M$ be the subgroup generated by the inertia groups $I_t =< \omega_t >$, $t \in \mathbf{t}$ and set $M_0 := M/M^0$. Then $f : Y \to X$ factors uniquely through a ramified G-cover $f^0 : Y \to X_0$ with group M^0 and an etale G-cover $f_0 : X_0 \to X$ with group M_0.



We will say that $f = (f^0, f_0)$ is the *canonical decomposition* of f and that f^0 (resp. f_0) is the ramified (resp. the etale) part of f.

The ramified part f^0 can, again, be decomposed as follows. For each prime $p|\,|M^0|$ and $t \in \mathbf{t}$ write $|I_t| = p^{n_p(t)}m_p(t)$ with $p \not| \, m_p(t)$. Then the p-Sylow M^0_p of M^0 is the subgroup $M^0_p =< I_t^{m_p(t)}, t \in \mathbf{t} >$ and its exponent is $p^{n_p(t_0)}$ for some $t_0 \in \mathbf{t}$. Write $f^0_p : X_{0,p} \to X_0$ for the quotient of f^0 modulo $\oplus_{q\neq p} M^0_q$. Then $f^0_p : X_{0,p} \to X_0$ is a G-cover with group M^0_p and a totally ramified place $P_p(t_0) \in X_0$ of index $p^{n_p(t_0)}$. In particular, if Q is the place lying above $P_p(t_0)$ in $f^0_p : X_{0,p} \to X_0$, then the residue fields at $P_p(t_0)$ and at Q are equal.

Given an abelian variety A over k, write $A[\chi]$ for the set of al $T \in A(\overline{k})$ such that ${}^{\sigma}T = \chi(\sigma)T$, $\sigma \in \Gamma_k$, where $\chi : \Gamma_k \to \widehat{\mathbb{Z}}^{\times}$ is the cyclotomic character of k. Then, on the one hand, the degree of f_0 is bounded by $|\mathrm{J}_{X|k}[\chi]|$, where $\mathrm{J}_{X|k}$ denotes the Jacobian variety of X over k (this is what we refer to as the *etale constraint* for f - lemma 2.4). So, when $|\mathrm{J}_{X|k}[\chi]|$ is finite, the residue fields of the places lying above those of $\mathbf{t}$ in $f_0 : X_0 \to X$ are finite extensions of k of degree bounded (in terms of the degree of $\mathbf{t}$ and the degree of f_0). But, on the other hand, for each prime $p||M^0|$, the residue field at $P_p(t_0)$ contains the $p^{n_p(t_0)}$th roots of unity (this is what we refer to as the *ramification constraint* for f - lemma 2.1). This, in turn, under some arithmetic assumptions on k, will impose that the degree of $f^0_p : X_{0,p} \to X_0$ be bounded. When both the etale and the ramification constraints occur, it appears that there is no G-cover $f : Y \to X$ defined over k with group $\mathbb{Z}/p^n$ for n large enough. This is the general philosophy of our proofs.

2.1. **Ramification constraint.**

Lemma 2.1. *Let k be any field and let X be a k-curve. Consider a G-cover $f : Y \to X$ defined over k and tamely ramified at a point P of X with ramification index e. Let Q be a point of Y lying above P. Then the residue field at Q contains the eth roots of unity.*

Proof. Write $\widehat{K}_{X,P}$ (resp. $\widehat{K}_{Y,Q}$) for the quotient field of the completion $\widehat{\mathcal{O}}_{X,P}$ of the local ring $\mathcal{O}_{X,P}$ of X at P (resp. the completion $\widehat{\mathcal{O}}_{Y,Q}$ of the local ring $\mathcal{O}_{Y,Q}$ of Y at Q). Then $\widehat{K}_{Y,Q}/\widehat{K}_{X,P}$ is a Galois extension with group the decomposition group at Q in $f : Y \to X$. Denote by I the inertia group at Q in $f : Y \to X$ and by $\widehat{K}^{ur}_{X,P}$ the subfield of $\widehat{K}_{Y,Q}$ fixed by I. Then $\widehat{K}_{Y,Q}/\widehat{K}^{ur}_{X,P}$ is totally ramified with group I. In particular, if $\kappa_{Y,Q}$ (resp. $\kappa^{ur}_{X,P}$) denotes the residue field of $\widehat{\mathcal{O}}_{Y,Q}$ (resp. $\widehat{\mathcal{O}}^{ur}_{X,P}$) then $\kappa_{Y,Q} = \kappa^{ur}_{X,P} =: \kappa$.

Now, we claim that there exists $y \in \widehat{K}_{Y,Q}$ such that $y^e \in \widehat{K}^{ur}_{X,P}$ and $\widehat{K}_{Y,Q} = \widehat{K}^{ur}_{X,P}(y)$. Indeed, fix uniformizing parameters $b \in \widehat{\mathcal{O}}_{Y,Q}$ and $a \in \widehat{\mathcal{O}}^{ur}_{X,P}$. Then $b^e = va$ for some $v \in \widehat{\mathcal{O}}^{\times}_{Y,Q}$. But, as $\kappa_{Y,Q} = \kappa^{ur}_{X,P}$, there exists $u \in \widehat{\mathcal{O}}^{ur}_{X,P}$ which has the same image as v in κ. So, up to replacing v with $u^{-1}v$ and a with ua, one can furthermore assume that v maps to 1 in κ. Then, applying Hensel's lemma to $X^e - v$ produces an element $v_0 \in \widehat{K}_{Y,Q}$ such that $v_0^e = v$ and $y := v_0^{-1}b$ has the expected property.

As a result $\widehat{K}_{Y,Q}$ contains the eth roots of unity, hence so does $\kappa_{Y,Q}$. □

Corollary 2.2. *Fix a prime p distinct from the characteristic of k. Let X be a k-curve and let $E/k(X)$ be an abelian extension regular over k with group $\mathbb{Z}_p$. If any finite extension of k contains only finitely many p^nth roots of unity, $n \geq 1$ then $E/k(X)$ is unramified.*

Proof. If not, any inertia group I of $E/k(X)$ being a non trivial closed subgroup of $\mathbb{Z}_p$ is open. So, let I be an inertia group with $[\mathbb{Z}_p : I] = p^n$ minimal and let $\tilde{X}$ be the normalization of X in $E^I/k(X)$. Then there is a place $P \in \tilde{X}$ which ramifies totally in $E/k(\tilde{X})$ with group $I \simeq \mathbb{Z}_p$. For each $n \geq 1$, write $\tilde{X}_n$ for the normalization of $\tilde{X}$ in $E^{(p^n I)}/k(\tilde{X})$ and let P_n be a point lying above P in $\tilde{X}_n \to \tilde{X}$. Then it follows from lemma 2.1 that the residue field $\kappa_{\tilde{X}_n,P_n}$ of $\tilde{X}_n$ at P_n contains the p^nth roots of unity. But as $E^{(p^n I)}/k(\tilde{X})$ is totally ramified, $\kappa_{\tilde{X}_n,P_n}$ is also the residue field $\kappa_{\tilde{X},P}$ of $\tilde{X}$ at P. So $\kappa_{\tilde{X},P}$ contains the p^nth roots of unity for all $n \geq 1$, which contradicts our assumption on k. □

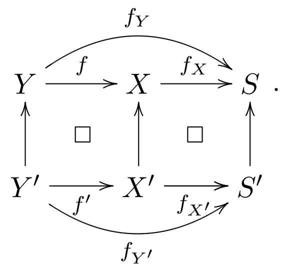
Remark 2.3. Since we apply lemma 2.1 to the residue field $\kappa_{\tilde{X},P}$ of $\tilde{X}$ at P it is essential to assume that not only k but also any finite extension of k contains only finitely many roots of unity. Any finitely generated field satisfies this hypothesis but there are also classical examples of fields containing no p^nth roots of unity with a finite extension containing all the p^nth roots of unity (*e.g.* $\mathbb{R}$ or the subfield of $\mathbb{Q}(\zeta_{p^\infty})$ fixed by μ_{p-1}, where $\mathbb{Z}_p^\times \simeq \mathbb{Z}_p \times \mu_{p-1}$.)

2.2. **Etale constraint.** Given a scheme S, we will classically write $\mathbb{G}_{m\,S}$ and $\mu_{n\,S}$ for the group schemes (etale sheaves) $\mathbb{G}_{m\,S}(T \to S) = \mathrm{H}^0(T, \mathcal{O}_T^\times)$ and $\mu_{n\,S}(T \to S) = \mathrm{H}^0(T, \mathcal{O}_T^\times)[n]$ respectively. Also, given a finite abelian group M, we will write M_S for the corresponding constant group scheme over S and $M_S^\vee$ for its Cartier dual over S (that is, if $M = (\mathbb{Z}/d_1)_S \oplus \cdots \oplus (\mathbb{Z}/d_r)_S$, $d_1|\cdots|d_r$ then $M_S^\vee = \mu_{d_1\,S} \oplus \cdots \oplus \mu_{d_r\,S}$).

Lemma 2.4. *Let X be a k-curve. Then any abelian etale G-cover $f : Y \to X$ defined over k with group M induces a group scheme monomorphism $M^\vee_{\mathrm{spec}(k)} \hookrightarrow \mathrm{J}_{X/k}$.*

Proof. This can be regarded as a consequence of Hochschild-Serre spectral sequence [18, Chap. III, Th. 2.20] for the etale sheaf $\mathbb{G}_m$ and the G-cover $f : Y \to X$.

Set $S := \mathrm{Spec}(k)$ (actually, the argument below works for any connected scheme S). For any connected S-scheme $S' \to S$, we will use the notation in the diagram below for the base change from S to S':



Then one has a spectral sequence:

$$\mathrm{H}^p(M,\mathrm{H}^q_{et}(Y',\mathbb{G}_{m\,Y'}))\Rightarrow \mathrm{H}^{p+q}_{et}(X',\mathbb{G}_m),$$

which yields in low degrees the exact sequence of cohomology groups:

$$(3)\qquad 0\rightarrow \mathrm{H}^1(M,\mathrm{H}^0_{et}(Y',\mathbb{G}_{m\,Y'}))\rightarrow \mathrm{H}^1_{et}(X',\mathbb{G}_{m\,X'})\rightarrow \mathrm{H}^0(M,\mathrm{H}^1_{et}(Y',\mathbb{G}_{m\,Y'}))\rightarrow\dots$$

But from $f_{Y'\star}\mathcal{O}_{Y'}=\mathcal{O}_{S'}$, one gets:

$$\mathrm{H}^0_{et}(Y',\mathbb{G}_{m\,Y'})=\mathrm{H}^0(Y',\mathcal{O}^\times_{Y'})=\mathrm{H}^0(S',f_{Y'\star}\mathcal{O}^\times_{Y'})=\mathrm{H}^0_{et}(S',\mathcal{O}^\times_{S'})=\mathrm{H}^0_{et}(S',\mathbb{G}_{m\,S'}).$$

Similarly, $\mathrm{H}^0_{et}(S',\mathbb{G}_{m\,S'})=\mathrm{H}^0_{et}(X',\mathbb{G}_{m\,X'})$ so from [18, Chap. II, Prop. 1.4]

$$\mathrm{H}^0_{et}(S',\mathbb{G}_{m\,S'})=\mathrm{H}^0_{et}(X',\mathbb{G}_{m\,X'})=\mathrm{H}^0_{et}(X',\mathbb{G}_{m\,X'})^M$$

is a trivial M-module and the left hand term of (3) is just:

$$\begin{aligned}\mathrm{H}^1(M,\mathrm{H}^0_{et}(Y',\mathbb{G}_{m\,Y'}))&=\mathrm{Hom}_{\mathbb{Z}}(M,\mathrm{H}^0_{et}(S',\mathbb{G}_{m\,S'}))\\&=\mathrm{Hom}_{\mathbb{Z}}(M,\mathrm{H}^0(S',\mathcal{O}^\times_{S'}))\\&=\oplus_{1\leq i\leq r}\mathrm{H}^0_{et}(S',\mathcal{O}^\times_{S'})[d_i]\\&=\mathrm{H}^0_{et}(S',M^\vee_{S'}).\end{aligned}$$

So (3) becomes:

$$(4)\qquad 0\rightarrow \mathrm{H}^0_{et}(S',M^\vee_{S'})\rightarrow \mathrm{Pic}(X')\rightarrow \mathrm{Pic}(Y').$$

Now, as taking the sheaf associated with a presheaf is an exact functor, one obtains the sheafification of (3):

$$(5)\qquad 0\rightarrow M^\vee_S\rightarrow \mathcal{P}ic_{X/S}\rightarrow \mathcal{P}ic_{Y/S}.$$

And from representability results for the Picard scheme of a curve [2, Th. VIII.4.3 and Th. IX.3.1], (5) produces an exact sequence of S-group schemes:

$$(6)\qquad 0\rightarrow M^\vee_S\rightarrow \mathrm{Pic}_{X/S}\rightarrow \mathrm{Pic}_{Y/S}.$$

But, as $M^\vee_S$ is torsion, (6) factors through:

$$(7)\qquad 0\rightarrow M^\vee_S\rightarrow \mathrm{J}_{X/S}\rightarrow \mathrm{J}_{Y/S}.\square$$

Remark 2.5. Under our assumption on the characteristic of k, the group scheme monomorphism $i_f: M^\vee_{\mathrm{spec}(k)}\hookrightarrow \mathrm{J}_{X/k}$ induces an isogeny $\phi:\mathrm{J}_{X/k}\rightarrow A$ with kernel isomorphic to $M^\vee_{\mathrm{spec}(k)}$ over k hence, by duality, an isogeny $\phi^\vee: A^\vee\rightarrow \mathrm{J}^\vee_{X/k}$ with kernel isomorphic to $M_{\mathrm{spec}(k)}$ over k.

For any abelian variety A over k and any integer $n\geq 1$ prime to the characteristic of k, consider the following condition:

(A,n) *There is no group scheme monomorphism* $\mu_{n\,\mathrm{spec}(k)}\hookrightarrow A$

It then follows from lemma 2.4 that for any k-curve X such that $(\mathrm{J}_{X/k},p^n)$ holds for some $n\geq 0$ any G-cover $f:Y\rightarrow X$ with group $\mathbb{Z}/p^N$, $N\geq n$ is ramified and, *a fortiori*, any k-G-extension $E/k(X)$ with group $\mathbb{Z}_p$ is ramified as well.

Lemma 2.6 below gives sufficient conditions for (A,n) to hold for all $n\geq n_A$ and prime to the characteristic of k, where $n_A\geq 1$ is an integer depending *a priori* on A (and k).

Lemma 2.6. *Let A be an abelian variety over k. Then there exists an integer $n_A\geq 1$ such that (A,n) holds for all $n\geq n_A$ and prime to the characteristic of k in the following two cases:*

(1) *k is a subfield of the cyclotomic closure*[3] *of a finitely generated field.*

[3] Recall that, given a field k, the cyclotomic closure of k in $\overline{k}$ is the subextension of $\overline{k}$ obtained from k by adjoining all the nth roots of unity in $\overline{k}$; we will denote it by k^{cyc}.

(2) *k is an l-adic field and A has anisotropic reduction*[4]. *Furthermore, in that case, the constant n_A can be taken depending only on the dimension* $\dim(A)$ *of A, l, the ramification index e and the residual degree f of k; we will denote it by $n(\dim(A), l, e, f)$.*

Proof. In case (1), this results from the following generalization of [21]. For any abelian variety $A \to k$ over a field k of characteristic $l \geq 0$, one has $A[\chi] \subset A(k^{cyc})_{tor}$ and the prime-to-l part $A[\chi]^{(l')}$ of $A[\chi]$ is finite. Indeed, any field k finitely generated over its prime field Q is a function field with constant field $k_0 := \overline{Q} \cap k$. So, let $A^{k|k_0}$ be the k/k_0-trace of A. As k_0 is algebraically closed in k, the extension k/k_0 and k_0^{cyc}/k_0 are linearly disjoint over k_0 hence, the k^{cyc}/k_0^{cyc}-trace of $A \times_k k^{cyc}$ is just $A^{k^{cyc}|k_0^{cyc}} = A^{k|k_0} \times_{k_0} k_0^{cyc}$; in particular $A^{k^{cyc}|k_0^{cyc}}(k_0^{cyc}) = A^{k|k_0}(k_0^{cyc})$. From the short exact sequence of $\mathbb{Z}$-modules (the injectivity on the left is Chow's theorem [15, Th. 3.3.3]):

$$0 \to A^{k|k_0}(k_0^{cyc}) \to A(k^{cyc}) \to A(k^{cyc})/A^{k|k_0}(k_0^{cyc}) \to 0,$$

one deduces the exact sequence of torsion submodules:

$$0 \to A^{k|k_0}(k_0^{cyc})_{tor} \to A(k^{cyc})_{tor} \to (A(k^{cyc})/A^{k|k_0}(k_0^{cyc}))_{tor}. \tag{8}$$

From Lang-Neron's theorem [15, Th. 6.2], the $\mathbb{Z}$-module $A(k^{cyc})/A^{k|k_0}(k_0^{cyc})$ is of finite type so the right-hand term of (8) is finite. If $l = 0$ then k_0 is a number field and from [21] the left-hand term of (8) is finite as well. If $l > 0$ then k_0 is finite and (8) induces by restriction a monomorphism $A^{k|k_0}[\chi]^{(l')} \hookrightarrow A[\chi]^{(l')}$ such that $A[\chi]^{(l')}/A^{k|k_0}[\chi]^{(l')} \hookrightarrow (A(k^{cyc})/A^{k|k_0}(k_0^{cyc}))_{tors}$. So it is enough to prove that $A^{k|k_0}[\chi]^{(l')}$ is finite. But, if $\mu_{n\,\mathrm{spec}(k_0)} \hookrightarrow A^{k|k_0}$ is a group scheme monomorphism with n prime to l then, by duality, this induces an isogeny $(A^{k|k_0}/\mu_n)^\vee \to (A^{k|k_0})^\vee$ with kernel isomorphic to $(\mathbb{Z}/n)_{\mathrm{spec}(k_0)}$ over k_0. In particular $n \leq LW(|k_0|, \dim(A))$, where $LW(q, g)$ denotes the Lang-Weil estimate for the number of rational points on a g-dimensional abelian variety defined over a finite field of order q [19, Th. 19.1].

In case (2), the statement follows from [6, Main Th.], which states that if k is an l-adic field and A is an abelian variety with anisotropic reduction over k then there exist a constant $n_A := n(\dim(A), l, e, f)$ such that $|A(k)_{tors}| \leq n_A$. So, once again assume that $\mu_{n\,\mathrm{spec}(k)} \hookrightarrow A$, which, by duality, corresponds to an isogeny $\alpha : B := (A/\mu_n)^\vee \to A$ with kernel isomorphic to $(\mathbb{Z}/n)_{\mathrm{spec}(k)}$ over k. We claim that B has anisotropic reduction if and only if A has and, hence, if A has anisotropic reduction then $n \leq n_A$. If n is prime to l, then the isogeny $\alpha : B \to A$ reduces to an isogeny $\mathfrak{B} \to \mathfrak{A}$ between the identity components of the special fibers of the Neron model of B and A [2, prop. VII.6.6]. More generally, the reduction of $\alpha : B \to A$ induces isogenies $T_B \to T_A$ and $V_B \to V_A$ between the toric and abelian parts of the identity components of the special fibers of the Neron model of B and A respectively[5]. Whence the annouced result. □

2.3. Counter-examples to the profinite (W-fod RIGP/k).

Corollary 2.7. *Assume that k is a finitely generated field of characteristic $\neq p$. Then the* (W-fod RIGP/G/k) *fails for any p-obstructed profinite group G.*

Proof. Assume first that $G = \mathbb{Z}_p$ and that the (W-fod RIGP/$\mathbb{Z}_p$/k) holds. Then there exists a k-curve X and a k-G-extension $E/k(X)$ with group $\mathbb{Z}_p$. From corollary 2.2, $E/k(X)$ is unramified, which contradicts lemma 2.4 and lemma 2.6.

[4]Recall that the identity component of the special fiber $\mathfrak{A}$ of the Neron model of A is an extension (over the residue field κ of k) $1 \to T_A \oplus U_A \to \mathfrak{A} \to V_A \to 1$, where T_A, U_A and V_A are respectively a torus, a commutative unipotent group and an abelian variety over κ. Following [6], we will say that A has *anisotropic* reduction if T_A contains no $\mathbb{G}_{m\,\mathrm{spec}(\kappa)}$, that A has *good reduction* if $\mathfrak{A}$ is an abelian variety and that A has *potentially good reduction* if $A \times_k k'$ has good reduction over some finite extension k' of k. Note that if A has potentially good reduction over k then it has anisotropic reduction over k.

[5]Just observe that if $\beta : A \to B$ is the isogeny such that $\beta \circ \alpha$ is multiplication by n on A then $\mathfrak{A} \to \mathfrak{B} \to \mathfrak{A}$ is again multiplication by n on $\mathfrak{A}$; in particular, it is an isogeny on the abelian and the toric parts (the kernel of multiplication by n is finite).

Now, assume that G is any p-obstructed profinite group. Let $U \subset G$ be an open subgroup such that $U \twoheadrightarrow \mathbb{Z}_p$ and denote by N the kernel of $U \twoheadrightarrow \mathbb{Z}_p$. If the (W-fod RIGP/$G/k$) holds then there exists a k-curve X and a k-G-extension $E/k(X)$ with group G. Let $\tilde{X}$ denote the normalization of X in $E^U/k(X)$ then $E/k(\tilde{X})$ is a k-G-extension with group U. But, then, taking the subextension E^N fixed by N, one gets a k-G-extension $E^N/k(\tilde{X})$ with group $\mathbb{Z}_p$, which contradicts the above. □

2.4. **Remarks.** In this last paragraph, we give counter-examples to corollary 2.7 when one of the hypotheses on k fails. For instance, rigidity straightforwardly implies that the (RIGP/$\mathbb{Z}_p/\mathbb{P}^1_{\mathbb{Q}^{ab}}$) holds. In that case, the ramification constraint vanishes. We consider below the case of finite fields of characteristic $p > 0$ and of l-adic fields ($l \neq p$), for which it is the etale constrainst that may vanish.

2.4.1. *Fields of characteristic $p > 0$.*

Proposition 2.8. *Consider a finite group G_0 of order divisible by p and write $G \twoheadrightarrow G_0$ for its universal p-Frattini cover. Let k be a field of characteristic p and let X be a k-curve such that the* (RIGP/G_0/X) *holds. Then the* (RIGP/G/X) *holds as well and, in particular, the* (W-fod RIGP/$G/\mathbb{F}_p$) *holds.*

Proof. One can write G as a projective limit $G = \varprojlim G_n$, where, for each $n \geq 0$ the group epimorphism $G_{n+1} \twoheadrightarrow G_n$ is Frattini with kernel an elementary p-abelian group $K_n \simeq (\mathbb{Z}/p)^{r_n}$.[6]

From the (RIGP/G_0/X), there exists a G-cover $f_0 : Y_0 \rightarrow X$ defined over k with group G_0; this will allow us to construct inductively a projective system $E = (f_n : Y_n \rightarrow X)_{n \geq 0}$ of G-covers defined over k with group G_n. Indeed, assume that $f_n : Y_n \rightarrow X$ exists, corresponding to a group epimorphism $\Phi_n : \Gamma_{k(X)} \twoheadrightarrow G_n$ then the corresponding embedding problem

$$\begin{array}{ccccccccc} & & & & & & \Gamma_{k(X)} & & \\ & & & & & & \downarrow{\scriptstyle \phi_n} & & \\ 1 & \longrightarrow & K_n & \longrightarrow & G_{n+1} & \longrightarrow & G_n & \longrightarrow & 1 \end{array}$$

is a geometric Frattini embedding problem with p-group kernel. Consequently, by [17, Th. IV.8.3], it has a solution $\Phi_{n+1} : \Gamma_{k(X)} \twoheadrightarrow G_{n+1}$. And by [17, Prop. IV.5.1], any solution is a geometric proper solution. So take for $f_{n+1} : Y_{n+1} \rightarrow X$ the G-cover corresponding to $\Phi_{n+1} : \Gamma_{k(X)} \twoheadrightarrow G_{n+1}$. The last assertion results from the fact the (W-fod RIGP/$G_0/\mathbb{F}_p$) holds.□

Remark 2.9. As $\overline{\mathbb{F}}_p$ is ample[7], the (RIGP/$G_0/\mathbb{P}^1_{\overline{\mathbb{F}}_p}$) holds hence so does the (RIGP/$G_0/\mathbb{P}^1_{\mathbb{F}_{p^r}}$) for some integer $r \geq 1$ and, by proposition 2.8, the (RIGP/$G/\mathbb{P}^1_{\mathbb{F}_{p^r}}$).

Example 2.10. Let G_0 be a finite group of order divisible by p and let $G \twoheadrightarrow G_0$ denote its universal p-Frattini cover. Then, by the universal property of $G \twoheadrightarrow G_0$, any Frattini cover $\tilde{G} \twoheadrightarrow G_0$ with kernel a pro-p group is a quotient of G. So, applying this to $\mathrm{SL}_2(\mathbb{Z}_p) \twoheadrightarrow \mathrm{PSL}_2(\mathbb{F}_p)$ one obtains that the (W-fod RIGP/$\mathrm{SL}_2(\mathbb{Z}_p)/\mathbb{F}_p$) and the (RIGP/$\mathrm{SL}_2(\mathbb{Z}_p)/\mathbb{P}^1_{\mathbb{F}_{p^{r_p}}}$) holds (for some integer $r_p \geq 1$ such that the (RIGP/$\mathrm{PSL}_2(\mathbb{F}_p)/\mathbb{P}^1_{\mathbb{F}_{p^{r_p}}}$) holds).

2.4.2. *l-adic fields ($l \neq p$).* Let l be a prime $\neq 2$, p and let k be an l-adic field. It follows from paragraphs 2.1 and 2.2 that if, for a k-curve X there exists a k-G-extension $E/k(X)$ with group a p-obstructed profinite group G then $\mathrm{J}_{X|k}$ has isotropic reduction. However, one can wonder whether k-G-extensions $E/k(X)$ with group a p-obstructed profinite group G do exist at all even if $\mathrm{J}_{X|k}$ has isotropic reduction.

The simplest examples of such G-extensions can be constructed using Tate elliptic curves $E \rightarrow k$, whose field of functions always admit k-G-extensions with group $\mathbb{Z}_p$. Using Pop's half Riemann existence theorem [20, Main Th.], more general examples can be constructed. Consider for instance the

[6]To see this, just use that the kernel P of $G \rightarrow G_0$ is a free pro-p group of finite positive rank $\rho \geq 1$ and apply the construction of the end of paragraph 3.3.

[7]Recall that a field k is said to be *ample* (or *large*) if for each smooth geometrically irreducible k-variety $V \rightarrow k$, $V(k)$ is infinite provided it is non-empty. It was proved in the nineties that for any ample field k and finite group G the (RIGP/$G/\mathbb{P}^1_k$) holds.

case of hyperelliptic curves.

Recall first the statement of [20, Main Th.].

By chosing a function $T \in k(\mathbb{P}^1_k)$ such that $k(\mathbb{P}^1_k) = k(T)$, we identify $\mathbb{P}^1_k(\overline{k})$ with $\overline{k} \cup \infty$. In the following, $|\cdot|$ stands for the normalized absolute value induced by the l-adic valuation of k on $\overline{k}$. A k-rational divisor $\mathbf{t} \subset \mathbb{P}^1_k$ such that $\mathbf{t}_{\overline{k}} \subset \overline{k}$ is said to be *pairwise adjusted* if $\mathbf{t}_{\overline{k}}$ can be written as a disjoint union $\mathbf{t}_{\overline{k}} = \mathbf{t}_1 \cup \mathbf{t}_2$ with $\mathbf{t}_i = \{t_{i,1}, \dots, t_{i,s}\}$, $i = 1, 2$ and (i) $|t_{1,m} - t_{2,m}| < |t_{1,m} - t_{1,n}|$, $1 \leq n \neq m \leq s$ and (ii) ${}^{\sigma}\mathbf{t}_i = \mathbf{t}_i$, $\sigma \in \Gamma_k$. It follows from the defining condition that $\sigma(t_{1,m}) = t_{1,\sigma(m)}$ if and only if $\sigma(t_{2,m}) = t_{2,\sigma(m)}$, $m = 1, ..., s$, $\sigma \in \Gamma_k$. Say that $\mathbf{t}$ is λ-*pairwise adjusted* if, furthermore, $\mathbf{t}_1$ (hence $\mathbf{t}_2$) has λ orbits under Γ_k.

Let Π denote the free product $< \gamma_{t_{1,1}} > * \cdots * < \gamma_{t_{1,s}} >$ of s copies of $\hat{\mathbb{Z}}/\mathbb{Z}_l \simeq < \gamma_{t_{1,m}} >$, $m = 1, \dots, s$ in the category of profinite groups and let Γ_k act on Π *via* $\sigma \cdot \gamma_{t_{1,m}} = \gamma_{t_{1,\sigma(m)}}^{\chi(\sigma^{-1})}$, $m = 1, \dots, s$ (where, as usual, $\chi : \Gamma_k \to \hat{\mathbb{Z}}^{\times}$ is the cyclotomic character of k). Then [20, Main Th.] states that if $X = \mathbb{P}^1_k$ and $\mathbf{t}$ is λ-pairwise adjusted then (1) has quotient:

$$1 \to \Pi \to \Pi \rtimes \Gamma_k \to \Gamma_k \to 1. \tag{9}$$

Using this result, it is easy to construct k-G-extensions of the field of functions of certain hyperelliptic curves with group $\mathbb{Z}_p$. For this, observe that the prodihedral group $D_{2p^\infty} = \mathbb{Z}_p \rtimes \mathbb{Z}/2$ is a quotient of $\Pi \rtimes \Gamma_k$. Assume that $\lambda \geq 2$. Write $O_1, \dots, O_\lambda$ for the orbits of $\mathbf{t}_1$ under Γ_k and let $\phi : \Pi \twoheadrightarrow D_{2p^\infty}$ sending γ_t to an order two element u in D_{2p^∞}, $t \in O_1$ and γ_t to another order two element u' in D_{2p^∞} such that u and u' generate D_{2p^∞} (for instance, take $u' = uv$, where v is a generator of the unique p-Sylow of D_{2p^∞}), $t \in O_2, \dots, O_\lambda$. Then, by construction, $\phi : \Pi \twoheadrightarrow D_{2p^\infty}$ extends to $\phi \rtimes \tilde{1} : \Pi \rtimes \Gamma_k \twoheadrightarrow D_{2p^\infty}$. (Indeed, observe that for any $1 \leq m \leq s$ and $\sigma \in \Gamma_k$ one has $\phi(\sigma \cdot \gamma_{t_{1,m}}) = \phi(\gamma_{t_{1,\sigma(m)}})^{\chi(\sigma^{-1})} = \phi(\gamma_{t_{1,m}})^{\chi(\sigma^{-1})} = \phi(\gamma_{t_{1,m}})$, where the second equality follows from the fact that $t_{1,m}$, $t_{1,\sigma(m)}$ lie in the same orbit under Γ_k and the third one follows from the fact that $\phi(\gamma_{t_{1,m}})$ has order 2). Composing $\phi \rtimes \tilde{1} : \Pi \rtimes \Gamma_k \twoheadrightarrow D_{2p^\infty}$ with the epimorphism $\pi_1(X \setminus \mathbf{t}) \twoheadrightarrow \Pi \rtimes \Gamma_k$ yields an epimorphism $\Phi : \pi_1(X \setminus \mathbf{t}) \twoheadrightarrow D_{2p^\infty}$ such that $\Phi(\pi_1(X_{\overline{k}} \setminus \mathbf{t})) = \phi(\Pi) = D_{2p^\infty}$ that is a regular epimorphism. In other words, one has constructed a k-G-extension $E/k(\mathbb{P}^1_k)$ unramified outside $\mathbf{t}$ and with group D_{2p^∞}. By construction $E/E^{\mathbb{Z}_p}$ is etale (this also follows from corollary 2.2).

This observation gives a suffficient condition for a hyperelliptic jacobian to have isotropic reduction.

Corollary 2.11. *Let X be a hyperelliptic curve. If its Weierstrass divisor $\mathbf{w}_X \subset \mathbb{P}^1_k$ is λ-pairwise adjusted with $\lambda \geq 2$ then $\mathrm{J}_{X|k}$ has isotropic reduction.*

Whether the condition of corollary 2.11 is necessary is unclear to us. At least, using the above result and coarse moduli schemes for G-covers of the projective line, one can show the following.

Corollary 2.12. *The set $Iso_g(k)$ of k-rational points on the coarse moduli scheme $\mathrm{Hyp}_g \times_{\mathbb{Q}} k$ of genus g hyperelliptic curves corresponding to curves with jacobian having isotropic reduction is Zariski-dense in $\mathrm{Hyp}_g \times_{\mathbb{Q}} k$.*

Proof. Assume that $p \neq 2$. Let $\mathrm{H}_n \to \mathbb{Z}[\frac{1}{2p^n}]$ denote the coarse moduli scheme for G-covers of the projective line with group the order $2p^n$ dihedral group D_{2p^n} and inertia canonical invariant $2g + 2$ copies of the conjugacy class of non-trivial involutions; it is an integral scheme, smooth over $\mathbb{Z}[\frac{1}{2p^n}]$ [23].

(1) From the above discussion $\mathrm{H}_n(k) \neq \emptyset$, hence $\mathrm{H}_n(k)$ is Zariski dense in $\mathrm{H}_n \times_{\mathbb{Q}} k$, $n \geq 1$ (by the l-adic implicit function theorem, k is ample).

(2) The stack morphism sending a G-cover $X \to \mathbb{P}^1$ with group D_{2p^n} and inertia canonical invariant $2g + 2$ copies of the conjugacy class of non-trivial involutions to the isomorphism class of X modded by the unique p-Sylow $\mathbb{Z}/p^n \subset D_{2p^n}$ induces at the level of coarse moduli schemes a morphism $\phi : \mathrm{H}_n \to \mathrm{Hyp}_g$, which is dominant.

Indeed, let X be an hyperelliptic curve over any algebraically closed field Ω. Write $c : X \to \mathbb{P}^1_\Omega$

for the canonical associated degree 2 cover and $i : X\tilde{\to}X$ for the hyperelliptic involution. Choose a Weierstrass point $w \in X(\Omega)$ and write $j_w : X \to \mathrm{J}_{X|\Omega}$ for the induced closed immersion of X into its jacobian. Then $[-1] \circ j_w = j_w \circ i$. Now, take any torsion point $T \in \mathrm{J}_{X|\Omega}(\Omega)$ of order exactly p^n and consider the isogeny dual of $\mathrm{J}_{X|\Omega} \to (\mathrm{J}_{X|\Omega}/ < T >)$ followed by the composition with the canonical polarization $\mathrm{J}^\vee_{X|\Omega}\tilde{\to}\mathrm{J}_{X|\Omega}$. This yields an isogeny $\alpha : A \to \mathrm{J}_{X|\Omega}$ with kernel isomorphic to the constant group scheme $(\mathbb{Z}/p^n)_{\mathrm{spec}(\Omega)}$. Let $f : Y \to X$ denote the pull back of α *via* j_w. As $i(w) = w$, one has the commutative diagram:

$$\begin{array}{ccccccc} \mathbb{P}^1_\Omega & \xleftarrow{c} & X & \xrightarrow{j_w} & \mathrm{J}_{X|\Omega} & \xleftarrow{\alpha} & A \\ & \nwarrow^{c} & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle [-1]} & & \downarrow{\scriptstyle [-1]} \\ & & X & \xrightarrow{j_w} & \mathrm{J}_{X|\Omega} & \xleftarrow{\alpha} & A. \end{array}$$

Now, compose $f : Y \to X$ with $c : X \to \mathbb{P}^1_k$ to obtain a degree $2p^n$ cover $\tilde{f} : Y \to \mathbb{P}^1_\Omega$. Let $t : Y\tilde{\to}Y$ be the automorphism obtained by pulling back the translation t_Θ by a generator Θ of the kernel of α *via* j_w. As $i(w) = w$, the pull-back of $[-1] : A\tilde{\to}A$ *via* j_w yields an involution $\tilde{i} : Y\tilde{\to}Y$ lifting the hyperellitic involution i. Finally, from $[-1] \circ t_\Theta = t_\Theta^{-1} \circ [-1]$ we get $\tilde{i} \circ t = t^{-1} \circ \tilde{i}$ that is the automorphism group of $\tilde{f}$ contains $< t > \rtimes \tilde{i} \simeq D_{2p^n}$. But as $\tilde{f}$ has degree $2p^n$, $\tilde{f}$ is a Galois cover with group D_{2p^n} and inertia canonical invariant a $2g + 2$-tuple of conjugacy classes of involutions.

(3) From lemma 2.6 (2), for $p^n \geq n(g, l, e, f)$, $\phi(\mathrm{H}_n(k)) \subset Iso_g(k)$. □

3. Profinite descent

3.1. Field of moduli and fields of definition. This section is devoted to the definition and construction of the cohomological tools which are required to extend the statement of corollary 2.7 to fields of moduli. This theory is classical for G-covers [8]; we extend it to projective systems of G-covers.

3.1.1. *Definitions.* Let X be a k-curve and let $E = (f_n : Y_n \to X_{\overline{k}})_{n\geq 0}$ be a projective system of G-covers defined over $\overline{k}$ with group G_n and ramification divisor $\mathbf{t}_n \subset X$ assumed to be k-rational. Writing as usual $G := \varprojlim G_n$, E corresponds to a continuous group epimorphism $\Phi : \pi_1(X_{\overline{k}} \setminus \underline{\mathbf{t}}) \twoheadrightarrow G$.

Given an algebraic extension k_0/k, one says that:

- **(fod)** k_0 is *a field of definition of E* if there exists a projective system of G-covers $E_{k_0} = (f_{n,k_0} : Y_{n,k_0} \to X_{k_0})_{n\geq 0}$ defined over k_0 such that f_n and $(f_{n,k_0})_{\overline{k}}$ are $\overline{k}$-G-isomorphic, $n \geq 0$.

Since the set of $\overline{k}$-isomorphisms of G-covers $f_n \simeq (f_{n,k_0})_{\overline{k}}$ is both non-empty (by assumption) and finite, the condition f_n and $(f_{n,k_0})_{\overline{k}}$ are $\overline{k}$-G-isomorphic, $n \geq 0$ in **(fod)** is equivalent to the existence of a projective system $(\chi_n : f_n \simeq (f_{n,k_0})_{\overline{k}})_{n\geq 0}$ of $\overline{k}$-G-isomorphisms. Thus, in terms of $\Phi : \pi_1(X \setminus \underline{\mathbf{t}}) \twoheadrightarrow G$, k_0 is a field of definition of E if and only if $\Phi : \pi_1(X \setminus \underline{\mathbf{t}}) \twoheadrightarrow G$ extends to a continuous group epimorphism $\Phi_{k_0} : \pi_1(X_{k_0} \setminus \underline{\mathbf{t}}) \twoheadrightarrow G$.

- **(fom)** k_0 is *the field of moduli of E (relatively to the extension $\overline{k}/k$)* if it is the subfield of $\overline{k}$ fixed by the closed subgroup $M_E = \bigcap_{n\geq 0} M_{f_n} \subset \Gamma_k$, where M_{f_n} denotes the closed subgroup (of finite index) of all $\sigma \in \Gamma_k$ fixing the $\overline{k}$-G-isomorphism class of f_n, $n \geq 0$.

Again, since the set of $\overline{k}$-G-isomorphism $f_n \simeq {}^\sigma f_n$ is both non-empty (by assumption) and finite, for any $\sigma \in \Gamma_k$, $\sigma \in M_E$ if and only if there exists a projective system $(\chi_{n,\sigma} : f_n \simeq {}^\sigma f_n)_{n\geq 0}$ of $\overline{k}$-G-isomorphisms. Thus, in terms of $\Phi : \pi_1(X \setminus \underline{\mathbf{t}}) \twoheadrightarrow G$, if k_0 is a field of definition of E and if $s : \Gamma_{k_0} \hookrightarrow \pi_1(X_{k_0} \setminus \underline{\mathbf{t}})$ is a continuous (set-theoretic) section of (2) then there exists a continuous map $h : \Gamma_{k_0} \to G$ such that $\Phi(s(\sigma)\gamma s(\sigma)^{-1}) = h(\sigma)\Phi(\gamma)h(\sigma)^{-1}$, for all $\gamma \in \pi_1(X_{\overline{k}} \setminus \underline{\mathbf{t}})$, $\sigma \in \Gamma_{k_0}$. (Observe that the map h depends on the section s but the notion of field of moduli does not).

Note also that it follows from the definition that the field of moduli of E is the compositum (actually the union) of the fields of moduli of the $f_n : Y_n \to X_{\overline{k}}$, $n \geq 0$.

3.1.2. *Cohomological obstruction.* We retain the notation of section 3.1. Clearly, **(fod)** implies **(fom)** but the converse is false in general. Assume that (2) admits a group-theoretic continuous section $s : \Gamma_{k_0} \hookrightarrow \pi_1(X_{k_0} \setminus \mathbf{t})$ (*cf.* paragraph 3.1.3). Then, using s and h, one can construct a *cohomological obstruction* $[\omega] \in \mathrm{H}^2(k_0, Z(G))$ *for f to be defined over k_0* (where $\mathrm{H}^2(k_0, Z(G))$ denotes the second cohomology group of Γ_{k_0} with values in the center $Z(G)$ of G regarded as a trivial Γ_{k_0}-module) as follows.

The map

$$\begin{array}{rccl} \overline{h}\colon & \Gamma_{k_0} & \to & G/Z(G) \\ & \sigma & \to & h(\sigma) \text{ [mod Z}(G)] \end{array}$$

is a well-defined group morphism, which only depends on s and not on the particular representative h. Considering $Z(G)$ as a trivial Γ_{k_0}-module, the continuous cochain

$$\begin{array}{rccl} \omega\colon & \Gamma_{k_0} \times \Gamma_{k_0} & \to & Z(G) \\ & (\sigma, \tau) & \to & h(\sigma\tau)^{-1}h(\sigma)h(\tau) \end{array}$$

defines a class $[\omega]$ which does not depend on s. Classically, $[\omega]$ is trivial in $\mathrm{H}^2(k_0, Z(E))$ if and only if $\overline{h} : \Gamma_{k_0} \to G/Z(G)$ can be lifted to a continuous group morphism $h_{k_0} : \Gamma_{k_0} \to G$ which, in turn, is equivalent to the existence of a continuous group epimorphism $\Phi_{k_0} : \pi_1(X_{k_0} \setminus \underline{\mathbf{t}}) \twoheadrightarrow G$ extending $\Phi : \pi_1(X_{\overline{k}} \setminus \underline{\mathbf{t}}) \twoheadrightarrow G$ (for the if condition take $h_{k_0} := \Phi_{k_0} \circ s$ and for the only if condition take $\Phi_{k_0} = \Phi(\cdot) \rtimes_s h_{k_0}(\cdot)$). So we call $[\omega] \in H^2(k_0, Z(G))$ the *cohomological obstruction for the projective system of G-covers $E = (f_n : Y_n \to X_{\overline{k}})_{n \geq 0}$ to be defined over k_0*. In particular, one has:

Proposition 3.1. *Let X be a k-curve and let $E/\overline{k}(X)$ be a $\overline{k}$-G-extension with group G and field of moduli k. Assume that (2) admits a continuous group-theoretic section.*

(i) If k has p-cohomological dimension ≤ 1 for all primes p dividing $|Z(G)|$ then $E/\overline{k}(X)$ is defined over k.

(ii) If $Z(G)$ is a direct summand of G then $E/\overline{k}(X)$ is defined over k.

(iii) If there exists a closed normal subgroup $N \lhd G$ such that $N \cap Z(G)$ is trivial and $[G : NZ(G)]$ is finite then $E/\overline{k}(X)$ is defined over a finite extension k_0/k with $[k_0 : k] \leq [G : NZ(G)]$.

(iv) The subextension of E fixed by $Z(G)$ is defined over k.

Proof. The assumption that (2) admits a continuous group-theoretic section allows us to use the profinite cohomological obstruction constructed above. Regard the G-extension $E/\overline{k}(X)$ with field of moduli k and group G as a continuous group epimorphism $\Phi : \pi_1(X_{\overline{k}} \setminus \underline{\mathbf{t}}) \twoheadrightarrow G$. We re-use the notation $\overline{h} : \Gamma_k \to G/Z(G)$ and $[\omega] \in \mathrm{H}^2(k, Z(G))$ from the above.

(i) is straightforward.

(ii) If $Z(G)$ is a direct summand of G then $G \twoheadrightarrow G/Z(G)$ admits a continuous section $s : G/Z(G) \hookrightarrow G$ which, composed with $\overline{h}$ yields a lift $s \circ \overline{h}$ of $\overline{h}$ to G.

(iii) Denote by $\psi : G \twoheadrightarrow G/N$ the natural quotient map and consider the commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \psi(Z(G)) & \longrightarrow & G/N & \longrightarrow & (G/N)/\psi(Z(G)) & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle \psi|_{Z(G)}} & & \uparrow{\scriptstyle \psi} & & \uparrow{\scriptstyle \overline{\psi}} & & \\
1 & \longrightarrow & Z(G) & \longrightarrow & G & \longrightarrow & G/Z(G) & \longrightarrow & 1 \\
 & & & & & & \uparrow{\scriptstyle \overline{h}} & & \\
 & & & & & & \Gamma_k & &
\end{array}$$

As $N \cap Z(G)$ is trivial, the restriction $\psi|_{Z(G)} : Z(G) \to \psi(Z(G))$ is an isomorphism, so $\psi : \mathrm{H}^2(k, Z(G)) \to \mathrm{H}^2(k, \psi(Z(G)))$ is an isomorphism too and, consequently, it is enough to prove that $\psi([\omega])$ becomes trivial in $\mathrm{H}^2(k, \psi(Z(G)))$. But $\psi([\omega])$ is the cohomological obstruction for lifting $\overline{\psi} \circ \overline{h} : \Gamma_k \to (G/N)/\psi(Z(G))$ to a morphism $\Gamma_k \to G/N$, hence $[\omega]$ becomes trivial over the fixed field k_0 of

$\ker(\overline{\psi}\circ\overline{h})$ in $\overline{k}$ and $[k_0 : k] \leq [G/N : Z(G)N/N] = [G : NZ(G)]$.

(iv) More generally, if $[\omega] \in \mathrm{H}^2(k, Z(G))$ is the cohomological obstruction for $E/\overline{k}(X)$ to be defined over k then for any closed normal subgroup $N \lhd G$ one has the canonical induced morphisms in cohomology $\mathrm{H}^2(k, Z(G)) \stackrel{p_N}{\to} \mathrm{H}^2(k, Z(G)/N) \stackrel{i_N}{\to} \mathrm{H}^2(k, Z(G/N))$ and $i_N \circ p_N([\omega]) \in \mathrm{H}^2(k, Z(G/N))$ is the cohomological obstruction for $E^N/\overline{k}(X)$ to be defined over k. In particular, with $N = Z(G)$ the class $p_N([\omega])$ is trivial so $E^{Z(G)}/\overline{k}(X)$ is defined over k.□

Remark 3.2. Write $\overline{h}_n : \Gamma_k \to G_n/Z(G_n)$, $\omega_n : \Gamma_k \times \Gamma_k \to Z(G_n)$ and $[\omega_n] \in \mathrm{H}^2(k, Z(G_n))$, $n \geq 0$ for the continuous group morphism, cochain and cohomological class associated with $h_n : \Gamma_k \stackrel{h}{\to} G \twoheadrightarrow G_n$, $n \geq 0$. One can wonder how the "global" cohomological obstruction $[\omega] \in \mathrm{H}^2(k, Z(G))$ for $E = (f_n : Y_n \to X_{\overline{k}})_{n\geq 0}$ to be defined over k_0 and the projective system of "local" cohomological obstructions $([\omega_n])_{n\geq 0} \in \varprojlim \mathrm{H}^2(k, Z(G_n))$ are related. Clearly, $i \circ \overline{h} = \varprojlim \overline{h}_n$ where $i : G/Z(G) \hookrightarrow \varprojlim G_n/Z(G_n)$ is the canonical monomorphism (note that $\varprojlim Z(G_n) = Z(G)$). Likewise, $\omega = \varprojlim \omega_n$ and $j([\omega]) = ([\omega_n])_{n\geq 0}$ where $j : \mathrm{H}^2(k, Z(G)) \to \varprojlim \mathrm{H}^2(k, Z(G_n))$ is the canonical morphism. In general j is not injective and non trivial global cohomological obstructions $[\omega]$ lying in the kernel of j correspond to projective systems of G-covers $(f_n : Y_n \to X)_{n\geq 0}$ defined over $\overline{k}$ such that the set $\mathcal{G}_{f_n}(k)$ of all the k-models of f_n is not empty, $n \geq 0$ but the projective limit $\varprojlim \mathcal{G}_{f_n}(k)$ is.

A sufficient condition for j to be injective is classically given by the Mittag-Leffler property [16, III.10] for the projective system of 1-cocycles $(\mathrm{C}^1(k, Z(G_{n+1})) \to \mathrm{C}^1(k, Z(G_n)))_{n\geq 0}$. It holds, for instance, when one of the following two conditions is fulfilled.

- The center $Z(G)$ of G is trivial.
- The morphism $Z(G_{n+1}) \to Z(G_n)$ is an epimorphim and any morphism $\Gamma_k \to Z(G_n)$ can be lifted to a morphism $\Gamma_k \to Z(G_{n+1})$ (for instance if k is of p-cohomological dimension ≤ 1 for all prime $p|\ |Z(G)|$), $n \geq 0$.

3.1.3. *Splitting of (2).* The following proposition gives criteria for the splitting of (2).

Proposition 3.3. *Assume that either $X(k) \neq \emptyset$ or that Γ_k is projective. Then (2) admits a group-theoretic continuous section.*

Proof. We retain the notation of paragraph 1.3.
- If k has characteristic 0 then choose a uniformizing parameter π for $P \in X(k)$. The Galois extension $M/\overline{k}(X)$ can be embedded into the field of Puiseux series $\overline{k}\{\{\pi\}\}$, on which Γ_k acts naturally. This defines a splitting morphism $s : \Gamma_k \hookrightarrow \mathrm{Gal}(M|k(X)) = \pi_1(X \setminus \underline{\mathbf{t}})$. If $X(k) \setminus \bigcup_{n\geq 0} \mathbf{t}_n \neq \emptyset$ (which, for instance, always occurs if $X = \mathbb{P}^1_k$ and k is uncountable), one can choose $P \in X(k) \setminus \bigcup_{n\geq 0} \mathbf{t}_n$, embedding then $M/\overline{k}(X)$ into the field of Laurent series $\overline{k}((\pi))$ as usual.
- More generally, write $\widehat{k(X)}$ for the completion of $k(X)$ at P. One gets the following commutative diagram of short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma_{\widehat{\overline{k}(X)}} & \longrightarrow & \Gamma_{\widehat{k(X)}} & \longrightarrow & \Gamma_k & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \pi_1(X_{\overline{k}} \setminus \underline{\mathbf{t}}) & \longrightarrow & \pi_1(X \setminus \underline{\mathbf{t}}) & \longrightarrow & \Gamma_k & \longrightarrow & 1 \end{array}$$

and the conclusion follows from the fact that the upper short exact sequence always splits [22, Lemma 2.9].
- If Γ_k is projective (*e.g.* k is a finite field) then by definition the natural epimorphism $\pi_1(X \setminus \underline{\mathbf{t}}) \twoheadrightarrow \Gamma_k$ always admits a section $s : \Gamma_k \hookrightarrow \pi_1(X \setminus \underline{\mathbf{t}})$ without any assumption on $X(k)$.

3.2. **Counter-examples to the (W-fom RIGP/G/k).**

Lemma 3.4. *If G is a p-obstructed profinite group G then the quotient $G/Z(G)$ is either p-obstructed or finite.*

Proof. As G is p-obstructed, there exists an open subgroup $U \subset G$ such that $U \twoheadrightarrow \mathbb{Z}_p$. Set $N_U := \bigcap_{g\in G} gUg^{-1}$. Then N_U is a closed normal subgroup of G of finite index $[G:N_U] \leq [G:U]!$ (use the exactness of $1 \to N_U \to G \to \mathrm{Aut}(G/U)$) hence it is also open in G. Furthermore, let N denote the kernel of any epimorphism $U \twoheadrightarrow \mathbb{Z}_p$. Then $N_U/(N\cap N_U)$ is a closed subgroup of $U/N \simeq \mathbb{Z}_p$, that is either $N_U/(N\cap N_U)$ is trivial (but, then, $N_U \subset N$, which contradicts the finiteness of $[G:N_U]$) or $N_U/(N\cap N_U) = p^n\mathbb{Z}_p \simeq \mathbb{Z}_p$. So, one can assume that U is normal in G. But $U\cap Z(G)$ is then a closed normal subgroup of U and $U/(U\cap Z(G)) \hookrightarrow G/Z(G)$. As the image Z_U of $U\cap Z(G)$ *via* $U \twoheadrightarrow \mathbb{Z}_p$ is a closed subgroup of $\mathbb{Z}_p$, there are two cases to consider:
- Z_U is trivial and, hence, $U \twoheadrightarrow \mathbb{Z}_p$ factors through $U/(U\cap Z(G)) \twoheadrightarrow \mathbb{Z}_p$ and $G/Z(G)$ is again p-obstructed.
- $Z_U = p^n\mathbb{Z}_p \subset \mathbb{Z}_p$, hence $[U:Z_U] = p^n$ and $[G:Z(G)] \leq [G:Z_U] = [G:U]p^n$ is finite. □

Lemma 3.4 together with proposition 3.1 and corollary 2.7 now imply:

Theorem 3.5. *Let k be either a finitely generated field of characteristic 0 or a finite field of characteristic distinct from p. Then the* (W-fom RIGP$/G/k$) *fails for any p-obstructed profinite group G.*

Proof. If not, there would exist a p-obstructed profinite group G, a k-curve X and a $\overline{k}$-G-extension $E/\overline{k}(X)$ with group G and field of moduli k. First, fix a finite extension k_X/k such that $X(k_X) \neq \emptyset$. By lemma 3.4, the quotient $G/Z(G)$ is either p-obstructed or finite. If $G/Z(G)$ is p-obstructed, consider the $\overline{k}$-G-subextension $E^{Z(G)}/\overline{k}(X)$ fixed by $Z(G)$. Then $E^{Z(G)}/\overline{k}(X)$ has group $G/Z(G)$ and, by proposition 3.1 (iv), is defined over k_X, which contradicts corollary 2.7. If $G/Z(G)$ is finite then, by proposition 3.1 (iii), there exists a finite extension k_0/k_X (with $[k_0:k_X] \leq [G:Z(G)]$) such that $E/\overline{k}(X)$ is defined over k_0, which, again, contradicts corollary 2.7. □

The main reason to focus on the field of moduli formulation of the weak (RIGP$/G/k$) is that it can be translated in terms of projective systems of rational points on projective systems of coarse moduli schemes for G-curves.

3.3. **Projective systems of rational points on projective systems of coarse moduli schemes for G-curves.** Given any integer $g \geq 0$ and r-tuple $\mathbf{C} = (C_1,\dots,C_r)$ of non trivial conjugacy classes in G such that $2-2g-r<0$, one can consider the category fibered in groupoids $\mathcal{H}_{g,G,\mathbf{C}} \to \mathbb{Z}[\frac{1}{|G|}]$ of G-curves Y with group G such that the resulting G-cover $Y \to Y/G$ has inertia canonical invariant $\mathbf{C}$ and base curve Y/G of genus g. Equivalently, $\mathcal{H}_{g,G,\mathbf{C}} \to \mathbb{Z}[\frac{1}{|G|}]$ is the category fibered in groupoids of G-covers of genus g curves with group G and inertia canonical invariant $\mathbf{C}$ (with weak G-isomorphism). (More precisely, the genus g curve is assumed to be equipped with an etale divisor of degree r and the inertia canonical invariant $\mathbf{C}$ is assumed to be one for the points on this etale divisor.) Then $\mathcal{H}_{g,G,\mathbf{C}} \to \mathbb{Z}[\frac{1}{|G|}]_{et}$ is a Deligne-Mumford stack (with finite diagonal), smooth and of finite type over $\mathbb{Z}[\frac{1}{|G|}]_{et}$. Its coarse moduli space $\mathrm{H}_{g,G,\mathbf{C}}$ is a scheme of finite type over $\mathbb{Z}[\frac{1}{|G|}]$, normal and of dimension $3g+r-3$. We refer to [1, §1-6] for further details on these stacks.

For any complete projective system $((G_{n+1},\mathbf{C}_{n+1}) \twoheadrightarrow (G_n,\mathbf{C}_n))_{n\geq 0}$ of finite groups G_n and r_n-tuples $\mathbf{C}_n$ of conjugacy classes in G_n, write $G := \varprojlim G_n$, $\mathbf{C} := \varprojlim \mathbf{C}_n$. Functoriality yields a projective system of coarse moduli schemes

$$(\mathrm{H}_{g,G_{n+1},\mathbf{C}_{n+1}} \to \mathrm{H}_{g,G_n,\mathbf{C}_n})_{n\geq 0}.$$

And theorem 3.5 yields the following result on projective systems of rational points on the above tower.

Corollary 3.6. *Assume that G is p-obstructed and that k is a finitely generated field of characteristic prime-to-$|G|$. Then $\varprojlim \mathrm{H}_{g,G_n,\mathbf{C}_n}(k) = \emptyset$.*

Proof. From theorem 3.5, it is enough to show that a projective system of k-rational points

$$\mathbf{p} = (p_n)_{n\geq 0} \in \varprojlim \mathrm{H}_{g,G_n,\mathbf{C}_n}(k)$$

induces a projective system of G-covers

$$E = (f_n : X_n \to X_0, \alpha_n : G_n \tilde{\to} \mathrm{Aut}_{X_0}(X_n))_{n\geq 0}$$

defined over $\overline{k}$ with field of moduli a finite extension k_0/k. The key point is that given such a projective system $E = (f_n : X_n \to X_0)_{n\geq 0}$, the field of moduli of E with respect to G-isomorphisms is a finite extension of the field of moduli of E with respect to weak G-isomorphisms.

To prove this, one can adapt the techniques of [3] as follows. By hypothesis, for each $\sigma \in \Gamma_k$ there exists a weak $\overline{k}$-G-isomorphism from $f_n : X_n \to X_0$ to ${}^\sigma f_n : {}^\sigma X_n \to {}^\sigma X_0$, that is a pair $(u_{n,\sigma}, v_{n,\sigma})$, where $v_{n,\sigma} : X_0 \to {}^\sigma X_0$ is a $\overline{k}$-isomorphism and $u_{n,\sigma}$ is a $\overline{k}$-G-isomorphism from $v_{n,\sigma} \circ f_n$ to ${}^\sigma f_n$.

From the assumption $2 - 2g - 2r_1 < 0$[8] one gets that only one of the following three possibilities occurs:

(i) $g \geq 2$;
(ii) $g = 1$ and $r_1 \geq 1$;
(iii) $g = 0$ and $r_1 \geq 3$.

Write $\mathbf{t}_1 \subset X_0$ for the ramification divisor of $f_1 : X_1 \to X_0$. Then the stabilizer $S_{\mathbf{t}_1}$ of $\mathbf{t}_1$ in $\mathrm{Aut}_{\overline{k}}(X_0)$ is always finite (more precisely, $|S_{\mathbf{t}_1}| \leq |\mathrm{Aut}_{\overline{k}}(X_0)|$ in case (i), $|S_{\mathbf{t}_1}| \leq 12$ in case (ii) [14, Cor IV.4.7] and $|S_{\mathbf{t}_1}| \leq \frac{r_1!}{(r_1-3)!}$ in case (iii)). So, up to replacing k by a finite extension k_0/k, one can assume that X_0, $\mathbf{t}_1$ and all the elements in $S_{\mathbf{t}_1}$ are defined over k.

For each $n \geq 1$, write $\mathcal{H}_{n,\sigma}$ for the set of all weak $\overline{k}$-G-isomorphism $(u_{n,\sigma}, v_{n,\sigma})$ from $f_n : X_n \to X_0$ to ${}^\sigma f_n : {}^\sigma X_n \to X_0$. This defines a projective system of non-empty finite sets $(\mathcal{H}_{n+1,\sigma} \to \mathcal{H}_{n,\sigma})_{n\geq 1}$. Indeed, for $n \geq 1$ let $G_{n+1,n}$ be the automorphism group of $X_{n+1} \to X_n$. Fix $\sigma \in \Gamma_k$ and $(u_{n+1,\sigma}, v_{n+1,\sigma}) \in \mathcal{H}_{n+1,\sigma}$. By definition of a G-cover, for all $g \in G_{n+1}$ one has ${}^\sigma\alpha_{n+1}(u_{n+1,\sigma} g u_{n+1,\sigma}^{-1}) = \alpha_{n+1}(g)$ and ${}^\sigma\alpha_{n+1}({}^\sigma g) = \alpha_{n+1}(g)$ hence $u_{n+1,\sigma} g u_{n+1,\sigma}^{-1} = {}^\sigma g$. In particular $u_{n+1,\sigma} G_{n+1,n} u_{n+1,\sigma}^{-1} = {}^\sigma G_{n+1,n}$. So $(u_{n+1,\sigma}, v_{n+1,\sigma}) \in \mathcal{H}_{n+1,\sigma}$ factors through $(\overline{u}_{n+1,\sigma}, v_{n+1,\sigma}) \in \mathcal{H}_{n,\sigma}$, whence the projectivity (note in particular that $v_{n,\sigma} \in S_{\mathbf{t}_1}$, $n \geq 0$). The finiteness of the $\mathcal{H}_{n,\sigma}$ is straightforward and the fact they are non-empty results from the assumption that the p_n are k-rational points, $n \geq 0$.

Now, choose $(u_{n,\sigma}, v_\sigma)_{n\geq 1} \in \varprojlim \mathcal{H}_{n,\sigma}$. This defines the profinite commutative diagram below.

(10)
$$\begin{array}{ccccccc}
X_{n+1} & \longrightarrow & X_n & \cdots\cdots & X_1 & \longrightarrow & X_{0\,\overline{k}} \\
\downarrow{\scriptstyle u_{n+1,\sigma}} & & \downarrow{\scriptstyle u_{n,\sigma}} & & \downarrow{\scriptstyle u_{1,\sigma}} & & \downarrow{\scriptstyle v_\sigma} \\
{}^\sigma X_{n+1} & \longrightarrow & {}^\sigma X_n & \cdots\cdots & {}^\sigma X_1 & \longrightarrow & X_{0\,\overline{k}}.
\end{array}$$

For each $n \geq 1$, let E_n denote the stabilizer of the G-isomorphism class of f_n under the action of $S_{\mathbf{t}_1}$ by left translation and let N_n denotes the normalizer of E_n in $S_{\mathbf{t}_1}$; note that E_n, N_n and $Q_n := N_n/E_n$ come equipped with a natural structure of trivial Γ_k-module. One has the decreasing sequence of finite groups

$$\ldots \subset E_{n+1} \subset E_n \subset \ldots \subset E_1 \subset S_{\mathbf{t}_1},$$

which is stationary for $n \geq n_0$. Without loss of generality, one can assume that $n_0 = 1$. The map $c : \Gamma_k \to Q_1$ sending σ to v_σ mod E_1 is a well-defined group morphism. So c becomes trivial when restricted to the finite extension $k_0 := \overline{k}^{\ker(c)}/k$. For each $n \geq 1$, denote by $\mathcal{W}_{n,\sigma}$ the set of all $\overline{k}$-G-isomorphism $w_{n,\sigma}$ from $v_\sigma^{-1} \circ f_n$ to ${}^\sigma f_n$. This, once again, yields a projective system of non-empty (because $E_n = E_1$ and $v_\sigma \in E_1$) finite sets $(\mathcal{W}_{n+1,\sigma} \to \mathcal{W}_{n,\sigma})_{n\geq 1}$. Then any $(w_{n,\sigma})_{n\geq 1} \in \varprojlim \mathcal{W}_{n,\sigma}$

[8]Here, r_1 denotes the length of $\mathbf{C}_1$; observe that $r_{n+1} \leq r_n$, $n \geq 0$.

yields a profinite commutative diagram commutative diagram below.

$$\begin{array}{ccccccc}
X_{n+1} & \longrightarrow & X_n & \cdots & X_1 & \longrightarrow & X_{0\,\overline{k}} \\
\downarrow{\scriptstyle w_{n+1,\sigma}} & & \downarrow{\scriptstyle w_{n,\sigma}} & & \downarrow{\scriptstyle w_{1,\sigma}} & & \downarrow{\scriptstyle v_\sigma^{-1}} \\
X_{n+1} & \longrightarrow & X_n & \cdots & X_1 & \longrightarrow & X_{0\,\overline{k}} \\
\downarrow{\scriptstyle u_{n+1,\sigma}} & & \downarrow{\scriptstyle u_{n,\sigma}} & & \downarrow{\scriptstyle u_{1,\sigma}} & & \downarrow{\scriptstyle v_\sigma} \\
{}^\sigma X_{n+1} & \longrightarrow & {}^\sigma X_n & \cdots & {}^\sigma X_1 & \longrightarrow & X_{0\,\overline{k}}
\end{array}$$

showing that $(f_n : X_n \to X_0)_{n\geq 0}$ is a projective system of G-covers with field of moduli k_0.□

Corollary 3.6 implies that for $n \gg 0$ either $\mathrm{H}_{g,G_n,\mathbf{C}_n}(k) = \emptyset$ or $\mathrm{H}_{g,G_n,\mathbf{C}_n}(k)$ is infinite. In particular, if $(\mathcal{C}_{n+1} \to \mathcal{C}_n)_{n\geq 1}$ is any projective system of k-curves on $(\mathrm{H}_{g,G_{n+1},\mathbf{C}_{n+1}} \to \mathrm{H}_{g,G_n,\mathbf{C}_n})_{n\geq 0}$ and if g_n denotes the genus of $\mathcal{C}_n$, $n \geq 0$ then it follows from [9] (Faltings' proof of Mordell conjecture) that only one of the following three situations occurs:

(i) $g_n = 0$, $n \geq 1$;
(ii) $g_n = 1$ with $\mathcal{C}_n(k) = \emptyset$ or $\mathcal{C}_n(k) \neq \emptyset$ and $\mathcal{C}_n(k)$ has rank ≥ 1, $n \gg 1$;
(iii) $g_n \geq 2$ (with $\mathcal{C}_n(k) = \emptyset$), $n \gg 1$.

These considerations are the starting point to tackle conjectures "à la Fried" [11], which deal with special cases of the situation considered in corollary 3.6.

A synthetic formulation of these conjectures is the following. Assume that G contains a normal open subgroup $P \subset G$ which is a free pro-p group of finite positive rank $\rho \geq 1$ and let $\mathbf{C} = (C_1, \dots, C_r)$ be an r-tuple of conjugacy classes of finite order elements in G. Introduce the Frattini series of P defined inductively by $P_0 = P$ and $P_{n+1} = P_n^p[P_n, P_n]$. Then the P_n, $n \geq 0$ are a fundamental system of characteristic neighborhoods of 1 in P hence a fundamental system of normal neighborhoods of 1 in G. As a result one can recover G as the projective limit $G = \varprojlim G_n$, where $G_n := G/P_n$, $n \geq 0$. Eventually, write $\mathbf{C}_n = (C_{n,1}, \dots, C_{n,r})$ for the image of $\mathbf{C}$ in G_n, $n \geq 0$. Then, for any $g \geq 0$ such that $2 - 2g - r < 0$, the projective system of coarse moduli schemes $(\mathrm{H}_{g,G_{n+1},\mathbf{C}_{n+1}} \to \mathrm{H}_{g,G_n,\mathbf{C}_n})_{n\geq 0}$ is called the *modular tower associated with g, G, P and* $\mathbf{C}$. For $g = 0$, G the prodihedral group $D_{2p^\infty} = \mathbb{Z}_p \rtimes \mathbb{Z}/2$, $P = \mathbb{Z}_p$ the unique p-Sylow of G and $\mathbf{C}$ four copies of the conjugacy class of non-trivial involutions in G, one gets $\mathrm{H}_{g,G_n,\mathbf{C}_n} \simeq Y_1(p^n)$, $n \geq 0$. This is the underlying motivation for stating:

Conjecture 3.7. *For any finitely generated field k of characteristic* 0 *one has* $\mathrm{H}_{g,G_n,\mathbf{C}_n}(k) = \emptyset$, $n \gg 0$.

Conjecture 3.7 was recently proved in the 1-dimensional case (that is, $(g, r) = (0, 4)$ or $(1, 1)$) in [5] using lemma 2.4 and corollary 3.6 as key ingredients. Note, however, that the result of [5] does not exclude the possibility that for all $n \geq 0$ some of the connected components of $\mathrm{H}_{g,G_n,\mathbf{C}_n}$ have genus 0 or 1; proving that only case (iii) above can occur for general modular towers (as it does for the tower of modular curves $(Y_1(p^{n+1}) \to Y_1(p^n))_{n\geq 0}$) remains an open problem.

Let us also mention that lemma 2.4 was used in [4] to prove, for instance, that conjecture 3.7 would follow from the strong torsion conjecture for abelian varieties. In [5] it is sketched by different techniques that conjecture 3.7 would even follow from the weaker torsion conjecture for abelian varieties.

References

[1] J. Bertin and M. Romagny, *Champs de Hurwitz*, preprint, 2006.
[2] S. Bosch, W. Lutkebohmert and M. Raynaud, *Néron models*, E.M.G. vol. **21**, Springer-Verlag, 1990.
[3] A. Cadoret, *Lifting results for rational points on Hurwitz moduli spaces*, to appear in Israel Journal of Mathematics, 2006.
[4] A. Cadoret, *A boundedness result for G-covers of curves*, preprint, 2007.
[5] A. Cadoret and A. Tamagawa, *Uniform boundedness for p-primary torsion on abelian schemes*, preprint, 2007.
[6] P.L. Clark and X. Xarles, *Local bounds for torsion points on abelian varieties*, to appear, Canadian J. Math.

[7] P. Dèbes and B. Deschamps, *Corps ψ-libres et théorie inverse de Galois infinie*, J. fur die Reine und Angew. Math. **574**, p. 197-218, 2004.
[8] P. Dèbes and J.-C. Douai, *Algebraic covers: Field of moduli versus field of definition*, Annales Sci. E.N.S. **30**, p. 303-338, 1997.
[9] G. Faltings, G. Wustholz and als, *Rational Points*, Seminar Bonn/Wuppertal 1983/1984, 3rd enlarged ed., Publ. of the Max Planck Institut fur Mathematik, Bonn, Vieweg, 1992.
[10] G. Frey and E. Kani, *Projective p-adic representations of the k-rational geometric fundamental group*, Arch. Math. **77**, p. 32-46, 2001.
[11] M. Fried, *Introduction to modular towers : generalizing the relation between dihedral groups and modular curves*, in *Proceedings of Summer Conference on recent developments in the inverse Galois problem*, A.M.S.-N.S.F. Cont. Math. series, vol. **186**, p. 111-171, 1995.
[12] A. Grothendieck, *Revêtements étales et groupe fondamental - S.G.A.I*, L.N.M. **224**, Springer-Verlag, 1971.
[13] D. Harbater, *Galois coverings of the arithmetic line*, in "Number Theory:New-York, 1984-1985" Lecture Notes in Math. **1240**, p. 165-195, 1987.
[14] R. Hartshorne, *Algebraic geometry*, G.T.M. **52**, Springer-Verlag, 1977.
[15] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, 1983.
[16] S. Lang, *Algebra*, revised third edition, GTM **211**, Springer-Verlag, 2002.
[17] G. Malle and B.H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, 1999.
[18] J. Milne, *Etale cohomology*, Princeton University Press, 1980.
[19] J. Milne, *Abelian varieties*, in *Arithmetic Geometry*, G.Cornell and J.H. Silverman ed., Springer Verlag, 1986.
[20] F. Pop, *Half Riemann Existence Theorem with Galois action*, In "Algebra and Number Theory", G. Frey and J. Ritters eds., de Gruyter Proceedings in Math., p. 1-26, 1994.
[21] K.A. Ribet, *Torsion points on abelian varieties in cyclotomic extensions*, Appendix to an article of N. Katz and S. Lang, Enseignement Math. **27** No2, 1981.
[22] A. Tamagawa, *The Grothendieck conjecture for affine curves*, Compositio Math. **109**, p. 135-194, 1997.
[23] S. Wewers, *Construction of Hurwitz spaces*, Ph.D. thesis, I.E.M. - Essen, 1998.