RATIONAL POINTS ON HURWITZ TOWERS

ANNA CADORET

cadoret@math.jussieu.fr
Univ. Lille 1, Mathématiques, 59655 Villeneuve d'Ascq Cedex, France.

Abstract. Generalizing some work of P. Bailey and M. Fried, we show that, given a number field k and a profinite group G which is an extension of a finite group by a projective pronilpotent group of finite rank, there is no projective system of k-rational points on any tower of Hurwitz spaces associated with G. In particular, there is no regular realization of such a group G over k.

2000 *Mathematic Subject Classification.* Primary 12F12, 14G32, 20E18; Secondary 20E06, 14D22.

Introduction

The problem motivating this paper is the regular inverse Galois problem RIGP for profinite groups over number fields and its translation in terms of projective systems of rational points on towers of Hurwitz spaces. Though strongly related to the RIGP for finite groups, additional obstructions - such as the lack of roots of 1 - are attached to the RIGP for profinite groups. For instance, the branch cycle argument (lemma 1.1) rules out the regular realization of such elementary profinite groups as $\mathbb{Z}_p$ or D_{2p^∞} over any number field [F95b]. On the contrary, groups as $\mathrm{GL}_n(\mathbb{Z}_p)$ have been recently regularly realized over $\mathbb{Q}$ by Katz's algorithm for the rigidity method [?]. So, there is no hope to obtain a global answer to the RIGP for profinite groups over number fields.

In this paper, we generalize some results of [BF02] which states that, given a number field k and a centerless p-perfect finite group G, there is no regular realization of its universal p-Frattini cover ${}_p\tilde{G}$ over k with only inertia groups of finite prime-to-p order. More precisely, we replace the universal p-Frattini cover ${}_p\tilde{G}$ of G by any profinite group G which is an extension of a finite group G_0 by a pronilpotent projective group P of finite rank and we impose no restriction on the ramification. We thus obtain

Theorem (Theorem 2.1): *Let $1 \to P \to G \xrightarrow{s} G_0 \to 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a pronilpotent projective group of finite rank. Then there is no regular realization of G over $k(T)$ for any number field k.*

In terms of towers of Hurwitz spaces, this means that, for any number field k, there is no projective system of k-points lying in the non-obstruction locus (that is, corresponding to G-covers defined over k) of any tower of Hurwitz spaces associated with such a profinite group G. It is rather natural to ask whether there exist projective systems of k-rational points outside the non-obstruction locus on such tower of Hurwitz spaces. We show the answer is no

Theorem (Theorem 4.1): *Let $1 \to P \to G \xrightarrow{s} G_0 \to 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a projective pronilpotent group of finite rank. Then there is no regular Galois extension $K/\overline{k}(T)$ with group G and field of moduli a number field k. In other words, $\varprojlim_{n\geq 0} \mathcal{H}_{r,G_n}(k) = \emptyset$ for any tower of Hurwitz spaces $(\mathcal{H}_{r_{n+1},G_{n+1}} \to \mathcal{H}_{r_n,G_n})_{n\geq 0}$ associated with G and any number field k.*

The proof of theorem 2.1 involves arguments which generalize those of [F95b] (lemma 2.2, 1st variant) and [BF02] (lemma 2.2, 2nd variant) as well as a technical adaptation of the branch cycle argument (lemma 2.3). Theorem 4.1 is a corollary of both theorem 2.1 and the following result

Theorem (Theorem 3.1): *Let $1 \to P \to G \xrightarrow{s} G_0 \to 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a projective pronilpotent group of finite rank. Let k be a field of characteristic 0. Then any regular Galois extension $K/\overline{k}(T)$ with group G and field of moduli k is defined over a finite extension k_0/k.*

For finite G-covers, there is a classical obstruction to the field of moduli being a field of definition. The proof of theorem 3.1 uses a generalization of this obstruction. This essentially reduces the problem to a group theoretic verification.

The paper is organized as follows: section 1 recalls the basic notions and introduces the notations, section 2 is devoted to the proof of theorem 2.1, section 3 to the one of theorem 3.1. Finally, section 4 gives some applications and shows the strong torsion conjecture for abelian varieties implies one of Fried's conjectures for modular towers.

Aknowledgment: This work originates in Fried's papers [F95b], [FK97], [BF02] where some of the key ideas we generalize here already appear.

1. Notations and basic notions

Given a field k, we will always denote by Γ_k its absolute Galois group. For any $r \geq 3$, set $\mathcal{U}^r = \mathrm{spec}(\mathbb{Z}[T_1, ..., T_r]_{\prod_{1\leq i<j\leq r}(T_i - T_j)})$ and let $\mathcal{U}_r = \mathcal{U}^r/\mathcal{S}_r$ be the quotient of $\mathcal{U}^r$ by the natural action of the symmetric group $\mathcal{S}_r$.

1.1. **Arithmetic fundamental group and G-covers.** Let k be a field of characteristic 0 and $\overline{k(T)}$ an algebraic closure of $k(T)$. We fix a compatible system $(\zeta_n)_{n\geq 2}$ of primitive roots of 1 in k that is, $\zeta_{mn}^m = \zeta_n$, $n, m \geq 2$ (when $k = \mathbb{C}$, the canonical choice is $\zeta_n = \mathrm{e}^{2i\pi/n}$, $n \geq 0$). Given a non singular projective algebraic curve X/k and a divisor $\mathbf{t}$ on it, let $M_{k,X,\mathbf{t}}/\overline{k}(T)$ be the maximal algebraic extension of $\overline{k}(X)$ (in a fixed algebraic closure $\overline{k(X)}$) unramified outside $\mathbf{t}$ then $M_{k,X,\mathbf{t}}/\overline{k}(T)$ and $M_{k,X,\mathbf{t}}/k(T)$ are Galois extension with groups we denote by $\pi_{1,k}^{\mathrm{alg}}(X \setminus \mathbf{t})$ and $\pi_{1,k}^{\mathrm{ar}}(X \setminus \mathbf{t})$ respectively.

If $X = \mathbb{P}^1_k$ and $\mathbf{t} \in \mathcal{U}_r(k)$, we write $M_{k,\mathbf{t}}$, $\pi_{k,\mathbf{t}}^{\mathrm{alg}}$, $\pi_{k,\mathbf{t}}^{\mathrm{ar}}$ instead of $M_{k,,\mathbf{t}X}$, $\pi_{1,k}^{\mathrm{alg}}(X \setminus \mathbf{t})$, $\pi_{1,k}^{\mathrm{ar}}(X \setminus \mathbf{t})$. In particular, we have the fundamental short exact sequence from Galois theory

$$\begin{tikzcd} 1 \arrow[r] & \pi_{k,\mathbf{t}}^{\mathrm{alg}} \arrow[r] & \pi_{k,\mathbf{t}}^{\mathrm{ar}} \arrow[r] & \Gamma_k \arrow[r] \arrow[l, bend right, "s"'] & 1 \end{tikzcd} .$$

which splits since $\mathbb{P}^1(k) \neq \emptyset$. By Riemann Existence Theorem, $\pi_{k,\mathbf{t}}^{\mathrm{alg}}$ is the profinite completion of the group defined by the generators $\gamma_1, ..., \gamma_r$ with the single relation $\gamma_1 \cdots \gamma_r = 1$ ($\gamma_1, ..., \gamma_r$ rise from a standard topological bouquet of loops around the branch points for $\mathbb{P}^1_k \setminus \mathbf{t}$ and, in the following, we will always assume such a topological bouquet has been fixed); the action of Γ_k on $\pi_{k,\mathbf{t}}^{\mathrm{alg}}$ has the property

Lemma 1.1. (Branch cycle argument) *For any $\sigma \in \Gamma_k$, ${}^{s(\sigma)}\gamma_i$ is conjugated in $\pi_{k,\mathbf{t}}^{alg}$ to $\gamma_{\pi(\sigma(i))}^{\chi(\sigma)}$ where $\chi : \Gamma_k \to \hat{\mathbb{Z}}$ denotes the cyclotomic character and $\pi(\sigma) \in \mathcal{S}_r$ the permutation induced by σ on $\{t_1, ..., t_r\}$.*

A G-cover is a pair (f, α) where $f : X \to \mathbb{P}^1$ is an algebraic Galois cover and $\alpha : \mathrm{Aut}(f) \to G$ is a group isomorphism. G-extensions $(K/\overline{k}(T), \alpha)$ are defined similarly. One can attach to any G-cover defined over an algebraic closed field $\overline{k}$ of characteristic 0 three invariants: the Galois group G, the branch point divisor $\mathbf{t} = \{t_1, ..., t_r\} \in \mathcal{U}_r(\overline{k})$ and, for each $t \in \mathbf{t}$, the corresponding inertia canonical conjugacy class C_t[1].

Let G be a finite group, $\mathbf{t} = \{t_1, ..., t_r\} \in \mathcal{U}_r(\overline{k})$ and $\mathbf{C} = (C_t)_{t\in\mathbf{t}}$ an r-tuple of non trivial conjugacy classes of G, the following categories are classically equivalent:

- (C1) the category of $\overline{k}$-G-covers $(f : X \to \mathbb{P}^1_{\overline{k}}, \alpha)$ with invariants G, $\mathbf{t}$, $\mathbf{C}$.
- (C2) the category of $\overline{k}(T)$-G-extensions $(K/\overline{k}(T), \alpha)$ with invariants G, $\mathbf{t}$, $\mathbf{C}$.
- (C3) the category of group epimorphisms $\Phi : \pi^{\mathrm{alg}}_{k,\mathbf{t}} \twoheadrightarrow G$ such that $(C^G_{\Phi(\gamma_1)}, ..., C^G_{\Phi(\gamma_r)}) = \mathbf{C}$, where C^G_g is the conjugacy class of g in G.

In the category (C1) (and thus (C2) since the equivalence from (C1) to (C2) is just the function field functor), a morphism from $(f_1 : X_1 \to \mathbb{P}^1_{\overline{k}}, \alpha_1)$ to $(f_2 : X_2 \to \mathbb{P}^1_{\overline{k}}, \alpha_2)$ is the data of a morphism of covers $u : f_1 \to f_2$ such that for any $g \in \mathrm{Aut}(f_1)$ $\alpha_2(u \circ g \circ u^{-1}) = \alpha_1$; in the category (C3), a morphism from Φ_1 to Φ_2 is an inner automorphism $\mathrm{i}_g \in \mathrm{Inn}(G)$ such that $\mathrm{i}_g \circ \Phi_1 = \Phi_2$.

The usual notions of field of moduli and field of definition can be easily described in the category (C3). Indeed, let $(f : X \to \mathbb{P}^1_{\overline{k}}, \alpha)$ be a $\overline{k}$-G-cover corresponding to $\Phi_{(f,\alpha)} : \pi^{\mathrm{alg}}_{k,\mathbf{t}} \twoheadrightarrow G$ then

- (fod) k is a field of definition for (f, α) if the two following equivalent conditions are fulfilled:
(i) There exists a k-G-cover (f_k, α_k) such that $(f, \alpha) \simeq (f_k, \alpha_k) \times_k \overline{k}$.
(ii) $\Phi_{(f,\alpha)} : \pi^{\mathrm{alg}}_{k,\mathbf{t}} \twoheadrightarrow G$ extends to a group epimorphism $\Phi_{(f,\alpha),k} : \pi^{\mathrm{ar}}_{k,\mathbf{t}} \twoheadrightarrow G$.

- (fom) k is the field of moduli for (f, α) (relatively to the extension $\overline{k}/k$) if the two following equivalent conditions are fulfilled:
(i) $k = \overline{k}^{M_{(f,\alpha),k}}$ where $M_{(f,\alpha),k} = \{\sigma \in \Gamma_k \mid (f, \alpha) \simeq (f, \alpha)^\sigma\} <_f \Gamma_k$ is the closed subgroup (of finite index) of Γ_k fixing the isomorphism class of (f, α).
(ii) There exists an application $h^s_{(f,\alpha),k} : \Gamma_k \to G$ such that $\Phi_{(f,\alpha)}({}^{s(\sigma)}\gamma) = h^s_{(f,\alpha),k}(\sigma) \cdot \Phi_{(f,\alpha)}(\gamma) \cdot (h^s_{(f,\alpha),k}(\sigma))^{-1}$, $\gamma \in \pi^{\mathrm{ar}}_{k,\mathbf{t}}$, $\sigma \in \Gamma_k$. (Observe that the notion of field of moduli does not depend on the section $s : \Gamma_k \hookrightarrow \pi^{\mathrm{ar}}_{k,\mathbf{t}}$).

Clearly (fod) implies (fom) but the converse is false in general. One can define a cohomological obstruction $[\omega_{(f,\alpha),k}] \in \mathrm{H}^2(k, Z(G))$ for a G-cover (f, α) with group G and field of moduli k to be defined over k [DDo97]. With the notations above, the map

$$\begin{array}{rccl} \overline{\phi}^s_{(f,\alpha),k}\colon & \Gamma_k & \to & G/Z(G) \\ & \sigma & \to & h^s_{(f,\alpha),k}(\sigma)[\mathrm{mod}\ \mathrm{Z}(G)] \end{array}$$

is a well-defined group morphism, which only depends on s and not on the particular representative $h^s_{(f,\alpha),k}$. Considering $Z(G)$ as a trivial Γ_k-module, the cochain

$$\begin{array}{rccl} \omega^s_{(f,\alpha),k}\colon & \Gamma_k \times \Gamma_k & \to & Z(G) \\ & (\sigma, \tau) & \to & h^s_{(f,\alpha),k}(\sigma\tau)^{-1} h^s_{(f,\alpha),k}(\sigma) h^s_{(f,\alpha),k}(\tau) \end{array}$$

[1]this latest invariant can be defined as follows: the inertia groups of f above $t \in \mathbf{t}$ are conjugated cyclic groups of order the ramification index e_t. Let P_t be a place of $\overline{k}(X)$ dividing t and u_t a uniformizing parameter. The distinguished generator of the inertia group $\mathrm{I}(P_t|t)$ is the preimage of ζ_{e_t} by the well-defined group isomorphism (which does not depend on the choice of the uniformizing parameter u_t of P_t) $\mathrm{I}(P_t|t) \to U_{e_t}(k)$ mapping ω to $\omega(u_t)/u_t[\mathrm{mod}\ P_t]$ (where $U_{e_t}(k)$ is the group of all the e_tth roots of 1 in the residue field $\kappa(P_t) \simeq \overline{k}$); replacing P_t by $\sigma(P_t)$, $\sigma \in \mathrm{Gal}(\overline{k}(X)|\overline{k}(T))$ does not change the conjugacy class C_t of these distinguished generators.

defines a class $[\omega_{(f,\alpha),k}] \in \mathrm{H}^2(k, Z(G))$ which does not depend on s. Classically, $[\omega_{(f,\alpha),k}] \in \mathrm{H}^2(k, Z(G))$ is 0 in $\mathrm{H}^2(k, Z(G))$ iff (f, α) is defined over k which, in turn, is equivalent to the existence of a group morphism $\phi^s_{k,(f,\alpha)} : \Gamma_k \to G$ making the following diagram commute

$$\begin{tikzcd} 1 \arrow[r] & Z(G) \arrow[r] & G \arrow[r] & G/Z(G) \arrow[r] & 1 \\ & & & \Gamma_k \arrow[ul, dotted, "\exists \phi^s_{k,(f,\alpha)}"] \arrow[u, "\overline{\phi}^s_{(f,\alpha),k}"'] & \end{tikzcd}$$

(this occurs in particular if $Z(G) = \{1\}$ or if $Z(G)$ is a direct factor of G). We call $[\omega_{(f,\alpha),k}] \in \mathrm{H}^2(k, Z(G))$ the cohomological obstruction for (f, α) to be defined over k.

1.2. **Hurwitz spaces and modular towers.**

1.2.1. *Notations for Hurwitz spaces.* Given a finite group G and an integer $r \geq 3$, denote by $\psi_{r,G} : \mathcal{H}_{r,G} \to \mathcal{U}_r$ the coarse moduli space (fine assuming $Z(G) = \{1\}$) for the category of G-covers of $\mathbb{P}^1$ with group G and r branch points, where $\psi_{r,G}$ is the application which to a given isomorphism class of G-covers associates its branch point set. For any r-tuple $\mathbf{C} = (C_1, ..., C_r)$ of non trivial conjugacy classes of G let $\mathcal{H}_{r,G}(\mathbf{C})$ be the corresponding *Hurwitz space* [FV91], that is the union of all irreducible components of $\mathcal{H}_{r,G}$ parametrizing the isomorphism classes of G-covers with r branch points, group G and inertia canonical invariant $\mathbf{C}$. We will freely use the general theory of Hurwitz spaces (*cf.* for instance [FV91], [V99], [W98] *etc*). In particular, given a field k of characteristic 0, $\mathcal{H}_{r,G}(k)$ corresponds to G-covers with field of moduli k and we write $\mathcal{H}_{r,G}(k)^{noob}$ for the k-non obstruction locus that is, the (possibly empty) subset of $\mathcal{H}_{r,G}(k)$ corresponding to G-covers defined over k (equivalently, $\mathcal{H}_{r,G}(k)^{noob}$ is the vanishing set of $\mathcal{H}_{r,G}(k) \to \mathrm{H}^2(k, Z(G))$, $(f, \alpha) \to [\omega_{(f,\alpha),k}]$).

1.2.2. *Modular towers.* In the following, given a short exact sequence of profinite groups $1 \to P \to G \to G_0 \to 1$ with G_0 a finite group and P a finitely generated pro-p-group, we will write $P_0 = P$, $P_1 = P_0^p[P_0, P_0]$, ..., $P_{n+1} = P_n^p[P_n, P_n]$ *etc.* for the Frattini series of P, which constitutes a fundamental system of open neighborhoods of 1 in P by [RZ00], proposition 2.8.13. We will also write G_n for the characteristic quotient G/P_n and $s_n : G \twoheadrightarrow G_n$ for the canonical projection, $n \geq 0$.

Now, fix a finite group G and a prime number p dividing $|G|$. Let ${}_p\tilde{\phi} :_p \tilde{G} \twoheadrightarrow G$ be the universal p-Frattini cover of G. Then $P := \ker({}_p\tilde{\phi})$ is a free pro-p group of finite rank. In this special case, we will write ${}^n_p\tilde{G}$ instead of G_n, $n \geq 0$. We thus obtain a complete projective system of finite groups $(s_{n+1,n} :_p^{n+1} \tilde{G} \to_p^n \tilde{G})_{n\geq 0}$ with the property that for any p'-conjugacy class (that is, the element od which are of prime to p order) C_n of ${}^n_p\tilde{G}$ there exists a unique conjugacy class C_{n+1} of ${}^{n+1}_p\tilde{G}$ above C_n the element of which have the same order as those of C_n (this is Schur-Zassenhauss lemma, [D04], lemma 1.1). Assume furthermore that G is p-perfect, that is generated by p'-elements, then any r-tuple $\mathbf{C} = (C_1, ..., C_r)$ of non trivial p'-conjugacy classes of G such that the set of all $g_1, ..., g_r \in G$ verifying (i) $G =< g_1, ..., g_r >$, (ii) $g_1 \cdots g_r = 1$ and (iii) $g_{\sigma(i)} \in C_i$ for some permutation $\sigma \in \mathcal{S}_r$ is non empty defines a unique projective system of tuples $(\mathbf{C}_n)_{n\geq 0}$ and the corresponding system of Hurwitz spaces

$$(s_{n+1,n} : \mathcal{H}_{r,{}^{n+1}_p\tilde{G}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r,{}^n_p\tilde{G}}(\mathbf{C}_n))_{n\geq 0}$$

is called *the modular tower associated with the data* $(G, \mathbf{C}, p)$. These objects were introduced and studied by M. Fried ([F95a], [FK97], [BF02], [D04] *etc.*) and were the starting point of this work.

From now on, we will simply denote a G-cover (f, α) by f.

2. Projective systems of rational points in the non obstruction locus

In this section, we give a somewhat more general version of the following result

Theorem.([BF02], theorem 6.1) *Let G be a centerless p-perfect finite group, $\mathbf{C}$ a r-tuple of p'-conjugacy classes of G and k a number field. Then there is no projective system of k-rational points on any Modular Tower associated with the data $(p,\mathbf{C}\ ,G)$.*

More precisely, we consider the problem of realizing regularly over a number field k a profinite group G presented as an extension of a finite group G_0 by a free pro-p group of finite rank P and we show this is not possible.

Theorem 2.1. *Let $1 \to P \to G \xrightarrow{s} G_0 \to 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a pronilpotent projective group of finite rank and k be either a number field or a finite field of characteristic q not dividing $|G_0|$ and distinct from one prime p dividing $|P|$. Then there is no regular realization of G over $k(T)$ for any number field k.*

2.1. **Proof.** For simplicity, we only give here the proof for the case $k = \mathbb{Q}$, leaving to the reader the details of the generalization to the number field case. As for the finite field case, we make some comments in 2.2.

Since P is a pronilpotent group, it can be written as the direct product of its Sylow subgroups: $P \simeq \prod_{p|\ |P|} P_p$ and, P being projective, each group P_p is a free pro-p group [RZ00] proposition 7.6.7 and corollary 7.7.6, $p|\ |P|$. As a result, considering the characteristic subgroup $P'_p = \prod_{p'|\ |P|, p' \neq p} P_{p'}$ of P, one gets the quotient short exact sequence of profinite groups:

$$\begin{tikzcd} 1 \arrow[r] & P \arrow[r] \arrow[d, two heads] & G \arrow[r] \arrow[d, two heads] & G_0 \arrow[r] \arrow[d, two heads] & 1 \\ 1 \arrow[r] & P_p \arrow[r] & G/P'_p \arrow[r] & G_0 \arrow[r] & 1 \end{tikzcd}$$

So, it is enough to consider the case when P is a free pro-p group. The proof of theorem 2.1 then results from the two lemmas below.

Lemma 2.2. *There is no regular realization of G over $k(T)$ with only inertia groups of finite order.*

Proof. Let $K/\mathbb{Q}(T)$ be a regular Galois extension with group G and only inertia groups of finite order. Since P is torsion free the extension K/K^P is unramified and the places which ramify in $K/\mathbb{Q}(T)$ are those which ramify in $K^P/\mathbb{Q}(T)$, in particular there are only a finite number - say r - of such places. Let $\mathbf{t} \in \mathcal{U}_r(k)$ be the ramification divisor of $K/\mathbb{Q}(T)$ and $\mathbf{C} = (C_1, ..., C_r)$ the corresponding canonical inertia invariant. We give now two variants of the proof; the first one generalizes a reduction argument of [F95b] for the prodihedral groups and the second one relies on the central argument of the proof of [F95a].

First variant: Consider the characteristic subgroup $[P,P] < P$ then, $[P,P]$ being normal in G, the regular extension $K^{[P,P]}/\mathbb{Q}(T)$ is Galois extension with invariants $\overline{G} := G/[P,P]$, $\overline{\mathbf{C}} := (\overline{C}_1, ..., \overline{C}_r)$ (where $\overline{C}_i$ denotes the image of C_i in $G \twoheadrightarrow G/[P,P]$), $\mathbf{t}$. Since P is a free pro-p group of finite rank ρ, $P^{ab} := P/[P,P]$ is a free abelian group of rank ρ that is, [RZ00], theorem 4.3.4, $P^{ab} \simeq \mathbb{Z}_p^\rho$ and, as a result, $(P^{ab})_n = p^n P^{ab}$, $n \geq 0$. The tower of regular G-extensions $\mathbb{Q}(T) < K^{(P^{ab})_0} < K^{(P^{ab})_1} < ... < K^{(P^{ab})_n^{ab}} < K^{(P^{ab})_{n+1}} < ...$ corresponds to a tower of $\mathbb{Q}$-G-covers $... \to X_{n+1} \to X_n \to ... \to X_0 \to \mathbb{P}^1_{\mathbb{Q}}$. Let $k/\mathbb{Q}$ be a finite extension such that $X_0(k) \neq \emptyset$ then, $X_n \times_{\mathbb{Q}} k \to X_0 \times_{\mathbb{Q}} k$ being an unramified G-cover defined over k with group $P^{ab}/(P^{ab})_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^\rho$, it comes from an unramified G-cover $A_n \to \mathrm{Jac}(X_0 \times_{\mathbb{Q}} k)$ defined over

k with group $(\mathbb{Z}/p^n\mathbb{Z})^\rho$. Thus, since $\mathrm{End}(A_n)$ is torsion free, A_n carries a k-torsion point of order p^n. Let Q be a place of k not dividing p where $\mathrm{Jac}(X_0\times_{\mathbb{Q}} k)$ has good reduction then, A_n and $\mathrm{Jac}(X_0\times_{\mathbb{Q}} k)$ being isogenous, their reductions modulo Q $\overline{A_n^Q}$ and $\overline{\mathrm{Jac}(X_0\times_{\mathbb{Q}} k)^Q}$ have the same number of $\mathbb{F}_{q^m}$-points (where $[k:\mathbb{Q}]=m$). Consequently, the reduction modulo Q map being injective on the p^n-torsion subgroup of A_n, $p^n|\ |\overline{\mathrm{Jac}(X_0\times_{\mathbb{Q}} k)^Q}(\mathbb{F}_{q^m})|$ for all $n\geq 1$: a contradiction.

Second variant: Let $f_0: X_0\rightarrow \mathbb{P}^1_{\mathbb{Q}}$ be the normalisation of $\mathbb{P}^1_Q$ in K^P, then the function field functor defines a bijective correspondence between the ($\overline{\mathbb{Q}}$-isomorphism classes of) Galois extension $\mathcal{K}/\overline{\mathbb{Q}}(T)$ with invariants G, $\mathbf{C}$, $\mathbf{t}$ such that $\mathcal{K}^P=K^P.\overline{\mathbb{Q}}$ and the ($\overline{\mathbb{Q}}$-isomorphism classes of) projective systems $(f_n:X_n\rightarrow\mathbb{P}^1_{\overline{\mathbb{Q}}})_{n\geq 0}$ of G-covers f_n with invariants ${}^n_p\tilde{G}$, $\mathbf{C}_n$, $\mathbf{t}$, $n\geq 0$, lying above f_0. We use the notation $\mathcal{P}(f_0,\mathbf{t},\mathbf{C})/\mathrm{Isom}_{\overline{\mathbb{Q}}}$ for these two identified sets. Let $(f_n:X_n\rightarrow\mathbb{P}^1_{\overline{\mathbb{Q}}})_{n\geq 0}\in\mathcal{P}(f_0,\mathbf{t},\mathbf{C})/\mathrm{Isom}_{\overline{\mathbb{Q}}}$, since $X_n\rightarrow X_0$ is etale with group the p-group P/P_n, $n\geq 0$, it defines up to inner conjugation a group epimorphism $j:\pi_1^{\mathrm{alg}}(X_0)^{(p)}\twoheadrightarrow \varprojlim_{n\geq 0} P/P_n=:P$ (where $\pi_1^{\mathrm{alg}}(X_0)^{(p)}$ denotes the pro-p completion of $\pi_1^{\mathrm{alg}}(X_0)$). Each group epimorphism $j:\pi_1^{\mathrm{alg}}(X_0)^{(p)}\twoheadrightarrow P$ in turn defines a unique group epimorphism $\overline{j}:\mathbb{T}_p(X_0)\twoheadrightarrow P^{ab}$ which makes the following diagramm commute

$$\begin{array}{ccc}\pi_1^{\mathrm{alg}}(X_0)^{(p)} & \xrightarrow{j} & P\\ \downarrow & & \downarrow\\ \mathbb{T}_p(X_0) & \xrightarrow{\exists!\overline{j}} & P^{ab}\end{array}$$

where $\mathbb{T}_p(X_0):=\pi_1^{\mathrm{alg}}(X_0)^{(p)}/[\pi_1^{\mathrm{alg}}(X_0)^{(p)},\pi_1^{\mathrm{alg}}(X_0)^{(p)}]$ is the (p-part of) the Tate module of X_0. As a result, we get the well defined $\Gamma_{\mathbb{Q}}$-equivariant maps (here, $\mathrm{Inn}(P)$ denotes the group of inner automorphisms of P)

$$\begin{array}{ccccc}\mathcal{P}(f_0,\mathbf{t},\mathbf{C})/\mathrm{Isom}_{\overline{\mathbb{Q}}} & \hookrightarrow & \mathrm{Epi}(\pi_1^{\mathrm{alg}}(X_0)^{(p)},P)/\mathrm{Inn}(P) & \rightarrow & \mathrm{Epi}(\mathbb{T}_p(X_0),P^{ab})\\ (f_n:X_n\rightarrow\mathbb{P}^1_{\overline{\mathbb{Q}}})_{n\geq 0} & \rightarrow & j & \rightarrow & \overline{j}\end{array}$$

where the action of $\Gamma_{\mathbb{Q}}$ on $\mathrm{Epi}(\pi_1^{\mathrm{alg}}(X_0)^{(p)},P)/\mathrm{Inn}(P)$ is defined by the canonical (non necessarily split) short exact sequence

$$1\rightarrow\pi_1^{\mathrm{alg}}(X_0)^{(p)}\rightarrow\pi_1^{\mathrm{alg}}(X_0)^{(p)}\rightarrow\Gamma_{\mathbb{Q}}\rightarrow 1$$

and on $\mathrm{Epi}(\mathbb{T}_p(X_0),P^{ab})$ by the usual action of $\Gamma_{\mathbb{Q}}$ on $\mathbb{T}_p(X_0)$. Furthermore, recall that, on the one hand $\mathbb{T}_p(X_0)$ is a free $\mathbb{Z}_p$-module of rank $2g(X_0)$ (with $g(X_0)$ the genus of X_0) and, on the other hand, P^{ab} is a free $\mathbb{Z}_p$-module of rank ρ so $\overline{j}$ is automatically a $\mathbb{Z}_p$-module epimorphism. Now, consider the projective system of G-covers corresponding to $K/\mathbb{Q}(T)$, this defines $j\in\mathrm{Epi}(\pi_1^{\mathrm{alg}}(X_0)^{(p)},P)$ such that $\sigma.j\equiv j[\mathrm{mod}\ \mathrm{Inn}(P)]$, $\sigma\in\Gamma_{\mathbb{Q}}$. in other words, any $\sigma\in\Gamma_{\mathbb{Q}}$ acts trivially on the ρ-dimensional $\mathbb{Q}_p$-vector space $\mathbb{T}_p(X_0)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\ker(\overline{j}\otimes_{\mathbb{Z}_p}\mathbb{Q}_p)$ and, in particular, 1 is an eigenvalue of σ. Now, let $\mathcal{X}\rightarrow\mathrm{spec}(\mathbb{Z})$ be the minimal model of $K^P/\mathbb{Q}$ and $q\neq p\in\mathbb{Z}$ where $\mathcal{X}\rightarrow\mathrm{spec}(\mathbb{Z})$ has good reduction. Then for any place Q of $\overline{\mathbb{Q}}/\mathbb{Q}$ dividing q, any element σ of the decomposition group D_Q of Q/q reducing to the Frobenius of $\mathbb{F}_q$ in $D_Q\twoheadrightarrow\Gamma_{\mathbb{F}_q}$ has all its spectral values of module $\sqrt{q}$ when acting on $\mathbb{T}_p(X_0)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ (*cf.* [L96], chapter XI, §6): a contradiction. □

Lemma 2.3. *There is no regular realization of G over $k(T)$ with an inertia group of infinite order.*

Proof. Assume there exists a regular Galois extension $K/\mathbb{Q}(T)$ with group G and an inertia group $< g >$ of infinite order. Denote by α the order of the element $s(g) \in G_0$ (so, in particular, $g^\alpha \in P$) and by $n_0 \geq 0$ the smallest integer such that $g^\alpha \in P_{n_0} \setminus P_{n_0+1}$. Since $[P_{n_0}, P_{n_0}] < P_{n_0+1}$, g^α is non zero modulo $[P_{n_0}, P_{n_0}]$. Consider the quotient short exact sequence of profinite groups:

$$\begin{tikzcd}
1 \arrow[r] & P_{n_0} \arrow[r] \arrow[d] & G \arrow[r, "s_{n_0}"] \arrow[d] & G/P_{n_0} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & P_{n_0}^{ab} \arrow[r] & G/[P_{n_0}, P_{n_0}] \arrow[r, "\overline{s}_{n_0}"] & G/P_{n_0} \arrow[r] & 1
\end{tikzcd}$$

By [RZ00], corollary 3.6.4, P_{n_0} is a free pro-p group of finite rank - say r. Thus $P_{n_0}^{ab}$ is a free abelian pro-p group of rank r that is, [RZ00], theorem 4.3.4, $P_{n_0}^{ab} \simeq \mathbb{Z}_p^r$. Given any set-theoretic section $\sigma_{n_0} : G/P_{n_0} \to G/[P_{n_0}, P_{n_0}]$ of $\overline{s}_{n_0}$, any element $u \in G/[P_{n_0}, P_{n_0}]$ can be written in a unique way $u = \sigma_{n_0}(\overline{s}_{n_0}(u))z_u$ with $z_u \in P_{n_0}^{ab}$, which implies that $uzu^{-1} = \sigma_{n_0}(\overline{s}_{n_0}(u))z\sigma_{n_0}(\overline{s}_{n_0}(u))^{-1}$ for any $z \in P_{n_0}^{ab}$. As a result, the conjugacy class of any $z \in P_{n_0}^{ab}$ in $G/[P_{n_0}, P_{n_0}]$ contains at most $|G/P_{n_0}|$ elements. Observe that this remains true when replacing $P_{n_0}^{ab}$ and $G/[P_{n_0}, P_{n_0}]$ by $P_{n_0}^{ab}/U$, $(G/[P_{n_0}, P_{n_0}])/U$ for any characteristic subgroup $U < P_{n_0}^{ab}$. Now, write $L = K^{[P_{n_0}, P_{n_0}]}$. Since $g^\alpha \in P_{n_0}$ is non zero modulo $[P_{n_0}, P_{n_0}]$, its image in $G \twoheadrightarrow G/[P_{n_0}, P_{n_0}]$ is of infinite order and so is the image of g. But the image of g modulo $[P_{n_0}, P_{n_0}]$ generates an inertia group of $L/\mathbb{Q}(T)$ and, $L^{P_{n_0}^{ab}}/\mathbb{Q}(T)$ being finite, the Galois extension $L/L^{P_{n_0}^{ab}}$ is necessarily ramified. The following diagram of regular Galois extensions sums up the situation,

$$\begin{tikzcd}
\mathbb{Q}(T) \arrow[r, hook] \arrow[r, bend left=50, dash, "G/P_{n_0}"] \arrow[rr, bend right=30, dash, "G/[P_{n_0},P_{n_0}]"'] & L^{P_{n_0}^{ab}} \arrow[r, hook] \arrow[r, bend left=50, dash, "P_{n_0}^{ab}"] & L \arrow[r, hook] \arrow[r, bend right=50, dash, "{[P_{n_0},P_{n_0}]}"'] & K
\end{tikzcd}$$

Recall $P_{n_0}^{ab} = \varprojlim_{n\geq 0}(\mathbb{Z}_p/p^n\mathbb{Z}_p)^r$ and set $L_n = L^{(p^n\mathbb{Z}_p)^r}$, $n \geq 0$. Then at least one of the inertia group of L_n/L_0 is of order p^n. Let $< g_n >$ be one of those inertia groups of order p^n; by lemma 1.1, the groups $< g_n^m >$ with m prime to $p|G/P_{n_0}|$ are also inertia groups of L_n/L_0. Write $\psi(n)$ for the number of integers $1 \leq m \leq p^n - 1$ such that $(m, p|G/P_{n_0}|) = 1$, then at least $\psi(n)/|G/P_{n_0}|$ groups $< g_n^m >$ with m prime to p, $|G/P_{n_0}|$ are non conjugate (we apply the observation above to the characteristic subgroup $U = (p^n\mathbb{Z}_p)^r < P_{n_0}^{ab}$) so there are at least $\psi(n)/|G/P_{n_0}|$ places of L_0 which ramify in L_n/L_0. Furthermore, each of these places also ramifies in L_1/L_0 (indeed, any element g_n of order p^n in $(\mathbb{Z}/p^n\mathbb{Z})^r$ has a non zero image in $(\mathbb{Z}/p\mathbb{Z})^r$). But $\lim_{n\to+\infty} \psi(n)/|G/P_{n_0}| = +\infty$: a contradiction. $\square$

Remark 2.4. We can reformulate theorem 2.1 in terms of Galois groups. Let k be a number field and $K/k(T)$ a regular Galois extension then, for any open normal subgroup $U \lhd_o \mathrm{Gal}(K|k(T))$, none of the characteristic quotient of U is a free pro-p group.

2.2. **Comments about the finite field case.** Both variants of lemma 2.2 rely on a reduction modulo q argument and, actually, they also work for any finite field of characteristic not dividing $p|G_0|$; their adaptation is straightforward and we refer for instance to [D04] for the second variant. Likewise, in lemma 2.3, the obstruction to the regular realization of G over $k(T)$ rises from the lack of roots of 1 in k and, as a result, lemma 2.3 also works for any field k of characteristic 0 such that $[k \cap \mathbb{Q}^{ab} : \mathbb{Q}]$ is finite or any finite field of characteristic q not dividing $p|G_0|$. This yields the finite field assertion of theorem 2.1. One could ask what occurs for the missing characteristics. The following theorem shows - at least for the characteristics p dividing $|P|$ - this situation is quite different.

Theorem 2.5. *Let G be a finite group, p a prime dividing $|G|$ and ${}_p\tilde{G}$ the universal p-Frattini cover of G. Then, given a finite field F of characteristic p, any regular realization of G over F yields a regular realization of ${}_p\tilde{G}$ over F.*

Proof. Starting from a regular realization $N_0/F(T)$ of G, we construct inductively a projective system $(N_n/F(T))_{n\geq 0}$ of regular Galois extension $N_n/F(T)$ with group ${}_p^n\tilde{G}$, $n \geq 0$. So, assume $N_n/F(T)$ exists and observe that the canonical projection $\pi_{n+1,n} :_p \tilde{G}_{n+1} \twoheadrightarrow_p \tilde{G}_n$ is a Frattini cover with elementary p-abelian kernel $\ker(\pi_{n+1,n}) \simeq P_n/P_{n+1} \simeq \mathbb{F}_p^{r_n}$. The corresponding embedding problem

$$\begin{array}{ccccccccc} & & & & & & \Gamma_{F(T)} & & \\ & & & & & & \downarrow{\scriptstyle \phi_n} & & \\ 1 & \longrightarrow & \mathbb{F}_p^{r_n} & \longrightarrow & {}_p\tilde{G}_{n+1} & \xrightarrow{\pi_{n+1,n}} & {}_p\tilde{G}_n & \longrightarrow & 1 \end{array}$$

(where $N_n = (F(T)^s)^{\ker(\phi_n)}$) is thus a geometric Frattini embedding problem with p-group kernel. Consequently, by [MMa99], theorem IV.8.3, it has a solution and, by [MMa99], proposition IV.5.1, any solution is a geometric proper solution. Conclude there exists $\phi_{n+1} : \Gamma_{F(T)} \twoheadrightarrow {}_p\tilde{G}_{n+1}$ such that $\pi_{n+1,n} \circ \phi_{n+1} = \phi_n$ and $N_{n+1} := (F(T)^s)^{\ker(\phi_{n+1})}/F(T)$ is regular. The existence of F results from Harbater's theorem V.2.7 [MMa99]; to get an explicit bound for $|F|$, choose a covering $G_0 \twoheadrightarrow G$ with G_0 a centerless finite group (take for instance the wreath product $A^{|G|} \rtimes_w G$ of G with any centerless finite group A) and apply to G_0 the procedure described in [W98], proposition 4.2.5 [W98]. □

One can formulate theorem 2.1 in terms of Hurwitz spaces

Theorem 2.6. *Let $1 \to P \to G \xrightarrow{s} G_0 \to 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a projective pronilpotent group of finite rank. Then $\varprojlim_{n\geq 0} \mathcal{H}_{r_n,G_n}(k)^{noob} = \emptyset$ for any tower of Hurwitz spaces $(\mathcal{H}_{r_{n+1},G_{n+1}} \to \mathcal{H}_{r_n,G_n})_{n\geq 0}$ associated with G and any field k which is either a number field or a finite field of characteristic q not dividing $p|G_0|$.*

Proof. In the preceeding sections we have worked with the specific complete projective system of finite groups $(G/P_{n+1} \twoheadrightarrow G/P_n)_{n\geq 0}$ but our results remain true for any complete projective system $(G_{n+1} \twoheadrightarrow G_n)_{n\geq 0}$ of finite groups such that $G = \varprojlim_{n\geq 0} G_n$. Indeed, if $(s_{i,n+1,n}G_{i,n+1} \twoheadrightarrow G_{i,n})_{n\geq 0}$, $i = 1, 2$ are two complete projective systems of finite groups such that $G = \varprojlim_{n\geq 0} G_{i,n}$, $i = 1, 2$, write $s_{i,n} : G \twoheadrightarrow G_{i,n}$ for the canonical projection and $P_{i,n} := \ker(s_{i,n})$, $n \geq 0$, $i = 1, 2$. By [RZ00], lemma 2.1.1, $(P_{1,n})_{n\geq 0}$ and $(P_{2,n})_{n\geq 0}$ are two fundamental systems of open neighbourhoods of 1 and, in particular, there exists two injective maps $\phi_1, \phi_2 : \mathbb{N} \hookrightarrow \mathbb{N}$ such that $P_{1,\phi_1(n)} < P_{2,n}$ and $P_{2,\phi_2(n)} < P_{1,n}$, $n \geq 0$. This provides, for any tuple $\mathbf{C}$ of non trivial conjugaccy classes of G, commutative diagrams of towers of Hurwitz spaces

$$\begin{array}{ccc} \mathcal{H}_{r_{i,\phi_i(n+1)},G_{i,\phi_i(n+1)}}(\mathbf{C}_{i,\phi_i(n+1)}) & \longrightarrow & \mathcal{H}_{r_{j,n+1},G_{j,n+1}}(\mathbf{C}_{j,n+1}) \quad 1 \leq i \neq j \leq 2 \\ \downarrow & & \downarrow \\ \mathcal{H}_{r_{i,\phi_i(n)},G_{i,\phi_i(n)}}(\mathbf{C}_{i,\phi_i(n)}) & \longrightarrow & \mathcal{H}_{r_{j,n},G_{j,n}}(\mathbf{C}_{j,n}) \end{array}$$

which shows that both towers $(\mathcal{H}_{r_{1,n+1},G_{1,n+1}}(\mathbf{C}_{1,n+1}) \to \mathcal{H}_{r_{1,n},G_{1,n}}(\mathbf{C}_{1,n}))_{n\geq 0}$ and $(\mathcal{H}_{r_{2,n+1},G_{2,n+1}}(\mathbf{C}_{2,n+1}) \to \mathcal{H}_{r_{2,n},G_{2,n}}(\mathbf{C}_{2,n}))_{n\geq 0}$ have the same properties concerning their (projective systems of) rational points. □

It is now natural to wonder if $\varprojlim_{n\geq 0} \mathcal{H}_{r,G_n}(k)$ is empty as well. We will prove this fact in section 4 (theorem 4.1), as a corollary of the results of section 3.

3. Projective system of rational points

The aim of this section is to prove the following statement

Theorem 3.1. *Let $1 \to P \to G \xrightarrow{s} G_0 \to 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a pronilpotent projective group of finite rank. Let k be a field of characteristic 0. Then any regular Galois extension $K/\overline{k}(T)$ with group G and field of moduli k is defined over a finite extension k_0/k.*

We divide the proof into two steps. We explain first how to generalize the classical cohomological obstruction $[\omega_f] \in \mathrm{H}^2(k, Z(G))$ for a $\overline{k}$-G-cover f with group G and field of moduli k to be defined over k to a projective system $(f_n)_{n\geq 0}$ of $\overline{k}$-G-covers f_n with group G_n and field of moduli k. We then apply these results to reduce theorem 3.1 to a group theoretical statement.

3.1. Generalization of the field of moduli obstruction.

3.1.1. *Notations.* Let $(s_{n+1,n} : G_{n+1} \twoheadrightarrow G_n)_{n\geq 0}$ be a complete projective system of finite groups and $G := \varprojlim_{n\geq 0} G_n$. For each $n \geq 0$, denote by $s_n : G \twoheadrightarrow G_n$ the canonical projection and by $P_n := \ker(s_n)$ its kernel. Given a field k of characteristic 0, any regular Galois extension $K/\overline{k}(T)$ with group G and field of moduli k corresponds to a projective system $(f_n)_{n\geq 0}$ of $\overline{k}$-G-covers f_n with group G_n and field of moduli k. Indeed, if $K/\overline{k}(T)$ has field of moduli k then so do the f_n, $n \geq 0$. Conversely, if for all $n \geq 0$ f_n has field of moduli k, for each $\sigma \in \Gamma_k$ the number of k-isomorphisms $f_n \simeq^{\sigma} f_n$ is finite, which implies that $K/\overline{k}(T)$ also has field of moduli k. We come back to this in the following. For each $n \geq 0$, let $\mathbf{t}_n \in \mathcal{U}_{r_n}(k)$ be the branch point divisor of f_n and $\Phi_n : \pi^{\mathrm{alg}}_{k,\mathbf{t}_n} \twoheadrightarrow G_n$ the corresponding group epimorphism. We get the commutative diagrams

$$\begin{tikzcd} \pi^{\mathrm{alg}}_{k,\mathbf{t}_{n+1}} \arrow[r, two heads, "e_n"] \arrow[d, two heads, "\Phi_{n+1}"'] & \pi^{\mathrm{alg}}_{k,\mathbf{t}_n} \arrow[d, two heads, "\Phi_n"] \\ G_{n+1} \arrow[r, two heads, "s_n"] & G_n \end{tikzcd}$$

where $e_n : \pi^{\mathrm{alg}}_{k,\mathbf{t}_{n+1}} \twoheadrightarrow \pi^{\mathrm{alg}}_{k,\mathbf{t}_n}$ is the canonical restriction epimorphism defined by the Galois extensions $\overline{k}(T) < M_{k,\mathbf{t}_n} < M_{k,\mathbf{t}_{n+1}}$, $n \geq 0$.

3.1.2. *Projective system of splitting morphisms.* Next, considering the projective system of fundamental short exact sequences

$$\begin{tikzcd} 1 \arrow[r] & \pi^{\mathrm{alg}}_{k,\mathbf{t}_{n+1}} \arrow[r] \arrow[d, two heads, "e_n"'] & \pi^{\mathrm{ar}}_{k,\mathbf{t}_{n+1}} \arrow[r] \arrow[d, two heads, "e_n"'] & \Gamma_k \arrow[r] \arrow[d, "\mathrm{Id}"'] & 1 \\ 1 \arrow[r] & \pi^{\mathrm{alg}}_{k,\mathbf{t}_n} \arrow[r] & \pi^{\mathrm{ar}}_{k,\mathbf{t}_n} \arrow[r] & \Gamma_k \arrow[r] & 1 \end{tikzcd}$$

observe that one can take the splitting morphisms $(s_{\mathbf{t}_n} : \Gamma_k \to \pi^{\mathrm{ar}}_{k,\mathbf{t}_n})_{n\geq 0}$ in such a way that $e_n \circ s_{\mathbf{t}_{n+1}} = s_{\mathbf{t}_n}$, $n \geq 0$. Indeed, set $M = \cup_{n\geq 0} M_{k,\mathbf{t}_n}$ and choose $t_0 \in k$; the Galois extension $M/\overline{k}(T)$ can be embedded into the field of Puiseux series $\overline{k}\{\{T - t_0\}\}$, on which Γ_k acts naturally. This defines a splitting morphism $s : \Gamma_k \to \mathrm{Gal}(M|k(T))$ and so, by restriction, a compatible system of splitting morphisms $(s_{\mathbf{t}_n} = \mathrm{res}|_{M_{t_n}} \circ s : \Gamma_k \to \pi^{\mathrm{ar}}_{k,\mathbf{t}_n})_{n\geq 0}$. If $k \setminus (k \cap \cup_{n\geq 0} \mathbf{t}_n) \neq \emptyset$

(which, for instance, always occurs if k is uncountable), one can choose $t_0 \in k \setminus (k \cap \cup_{n\geq 0}\mathbf{t}_n)$, embedding then $M/\overline{k}(T)$ into the field of Laurent series $\overline{k}((T-t_0))$ as usual.

3.1.3. *Action of* Γ_k. Observe that for any $n \geq 0$

$$\begin{array}{rcl} s_{\mathbf{t}_n} & = & \mathrm{res}|_{M_{k,\mathbf{t}_n}} \circ s = \mathrm{res}|_{M_{k,\mathbf{t}_n}} \circ \mathrm{res}|_{M_{k,\mathbf{t}_{n+1}}} \circ s \\ & = & e_n \circ s_{\mathbf{t}_{n+1}} \end{array}$$

and so, for any $\gamma \in \pi^{\mathrm{ar}}_{k,\mathbf{t}_{n+1}}$, $\sigma \in \Gamma_k$

$$\begin{array}{rcl} e_n(s_{\mathbf{t}_{n+1}}(\sigma)\gamma s_{\mathbf{t}_{n+1}}(\sigma)^{-1}) & = & e_n \circ s_{\mathbf{t}_{n+1}}(\sigma)\ e_n(\gamma)\ e_n \circ s_{\mathbf{t}_{n+1}}(\sigma)^{-1} \\ & = & s_{\mathbf{t}_n}(\sigma) e_n(\gamma) s_{\mathbf{t}_n}(\sigma)^{-1} \end{array}$$

3.1.4. *Projective system of cohomological obstructions.* Now, with the notations of 1.1, for any $n \geq 0$, $\sigma \in \Gamma_k$, there exists $h_n(\sigma) := h^{s_{\mathbf{t}_n}}_{k,f_n}(\sigma) \in G_n$ such that

$$\Phi_n(s_{\mathbf{t}_n}(\sigma)\gamma s_{\mathbf{t}_n}(\sigma)^{-1}) = h_n(\sigma)\Phi_n(\gamma)h_n(\sigma)^{-1},\ \gamma \in \pi^{\mathrm{ar}}_{k,\mathbf{t}_n}$$

Denote by $H_n(\sigma) \subset G_n$ the set of all such elements. From the surjectivity of e_n and the fact that for any $\gamma \in \pi^{\mathrm{ar}}_{k,\mathbf{t}_{n+1}}$ one has, on the one hand

$$\begin{array}{rcl} s_{n+1,n} \circ \Phi_{n+1}(s_{\mathbf{t}_{n+1}}(\sigma)\gamma s_{\mathbf{t}_{n+1}}(\sigma)^{-1}) & = & s_{n+1,n}(h_{n+1}(\sigma)\ \Phi_{n+1}(\gamma)\ h_{n+1}(\sigma)^{-1}) \\ & = & s_{n+1,n}(h_{n+1}(\sigma))\ \Phi_n \circ e_n(\gamma)\ s_{n+1,n}(h_{n+1}(\sigma)^{-1}) \end{array}$$

and, on the other hand,

$$\begin{array}{rcl} s_{n+1,n} \circ \Phi_{n+1}(s_{\mathbf{t}_{n+1}}(\sigma)\gamma s_{\mathbf{t}_{n+1}}(\sigma)^{-1}) & = & \Phi_n \circ e_n(s_{\mathbf{t}_{n+1}}(\sigma)\gamma s_{\mathbf{t}_{n+1}}(\sigma)^{-1}) \\ & = & \Phi_n(s_{\mathbf{t}_n}(\sigma)e_n(\gamma)s_{\mathbf{t}_n}(\sigma)^{-1}) \end{array}$$

so, $s_{n+1,n}(h_{n+1}(\sigma)) \in H_n(\sigma)$ that is, $(H_{n+1}(\sigma) \to H_n(\sigma)_{n\geq 0}$ is a projective system of non empty finite sets. Hence, we can define maps $h : \Gamma_k \to G$, $\sigma \to h(\sigma) = (h_n(\sigma))_{n\geq 0} \in \varprojlim_{n\geq 0} H_n(\sigma)$. Write $\overline{\phi}_n : \Gamma_k \to G_n/Z(G_n)$, $\omega_n : \Gamma_k \times \Gamma_k \to Z(G_n)$ and $[\omega_n] \in \mathrm{H}^2(k, Z(G_n))$, $n \geq 0$ for the group morphism, cochains and cohomological classes associated with $h_n : \Gamma_k \to G_n$, $n \geq 0$. Similarly, set

$$\begin{array}{rrcl} \overline{\phi}\colon & \Gamma_k & \to & G/Z(G) \\ & \sigma & \to & h(\sigma)\ [\mathrm{mod}\ Z(G)] \end{array}\ ,\quad \begin{array}{rrcl} \omega\colon & \Gamma_k \times \Gamma_k & \to & Z(G) \\ & (\sigma,\tau) & \to & h(\sigma\tau)^{-1}h(\sigma)h(\tau) \end{array}\ ,\quad [\omega] \in H^2(k, Z(G))$$

Clearly, $i\circ\overline{\phi} = \varprojlim_{n\geq 0} \overline{\phi}_n$ where $i : G/Z(G) \hookrightarrow \varprojlim_{n\geq 0} G_n/Z(G_n)$ is the canonical monomorphism (note that $\varprojlim_{n\geq 0} Z(G_n) = Z(G)$). Likewise, $\omega = \varprojlim_{n\geq 0} \omega_n$ and $j([\omega]) = \varprojlim_{n\geq 0} [\omega_n]$ where $j : H^2(k, Z(G)) \to \varprojlim_{n\geq 0} H^2(k, Z(G_n))$ is the canonical morphism. In particular, if $[\omega]$ is 0 in $H^2(k, Z(G))$ then $[\omega_n]$ is 0 in $H^2(k, Z(G_n))$, $n \geq 0$ so we call $[\omega] \in H^2(k, Z(G))$ the cohomological obstruction for the G-covers $(f_n)_{n\geq 0}$ to be defined over k[2]. Furthermore, $[\omega] \in H^2(k, Z(G))$ being the cohomological obstruction to solve the embedding problem

$$\begin{tikzcd} 1 \arrow[r] & Z(G) \arrow[r] & G \arrow[r] & G/Z(G) \arrow[r] & 1 \\ & & & \Gamma_k \arrow[u, "\overline{\phi}"'] & \end{tikzcd}$$

we get

[2]Since, in general, the canonical morphism j is not injective, one cannot conclude that if $[\omega_n]$ is 0 in $H^2(k, Z(G_n))$, $n \geq 0$ then $[\omega]$ is 0 in $H^2(k, Z(G))$.

Proposition 3.2. *(1) If $Z(G) = \{1\}$ or if the short exact sequence $1 \to Z(G) \to G \to G/Z(G) \to 1$ is split, then any projective system $(f_n)_{n\geq 0}$ of $\overline{k}$-G-covers f_n with group G_n and field of moduli k is a projective system of G-covers defined over k.*
(2) If $[G : Z(G)]$ is finite then any projective system $(f_n)_{n\geq 0}$ of $\overline{k}$-G-covers f_n with group G_n and field of moduli k is defined over a finite extension k_0/k of degree $[k_0 : k] \leq [G : Z(G)]$.
(3) If $Z(G) \cap P_{n_0} = \{1\}$ for some $n_0 \geq 0$ then any projective system $(f_n)_{n\geq 0}$ of $\overline{k}$-G-covers f_n with group G_n and field of moduli k is a projective system of G-covers defined over a finite extension k_0/k with $[k_0 : k] \leq |G_{n_0}|$.

Proof. (1) is straightforward, for (2), take for instance $k_0 = \overline{k}^{\ker(\overline{\phi})}$ and, for (3), if $Z(G) \cap P_{n_0} = \{1\}$, there is canonical commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & s_{n_0}(Z(G)) \arrow[r] & G_{n_0} \arrow[r, "\pi_{n_0}"] & G_{n_0}/Z(G) \arrow[r] & 1 \\
1 \arrow[r] & Z(G) \arrow[r] \arrow[u, "\simeq"] & G \arrow[r] \arrow[u, "s_{n_0}"] & G/Z(G) \arrow[r] \arrow[u, "\overline{s}_{n_0}"'] & 1 \\
 & & & \Gamma_k \arrow[u, "\overline{\phi}"] \arrow[uul, dotted, "\exists \phi"] &
\end{tikzcd}$$

and $[s_{n_0} \circ \omega] \in \mathrm{H}^2(k, s_{n_0}(Z(G)))$ is the cohomological obstruction for the existence of a group morphism $\phi : \Gamma_k \to G_{n_0}$ such that $\pi_{n_0} \circ \phi = \overline{s}_{n_0} \circ \overline{\phi}$. As a result, setting $k_0 := \overline{k}^{\ker(\overline{s}_{n_0} \circ \overline{\phi})}$ (which is a degree $[G_{n_0} : Z(G)]$ extension of k) one has $[s_{n_0} \circ \omega] = 0$ in $\mathrm{H}^2(k_0, s_{n_0}(Z(G)))$, that is, $s_{n_0} \circ \omega$ is a coboundary and, since s_{n_0} is injective on $Z(G)$, so is ω: conclude $[\omega] = 0$ in $\mathrm{H}^2(k_0, Z(G))$. □

To end this section, let us give a geometrical interpretation of these results. Given an integer $r \geq 3$ and a finite group G we denote by $\mathcal{H}_{r,G}(k)^{noob}$ the set of k-non obstruction that is, the set of all k-rational points on $\mathcal{H}_{r,G}$ corresponding to G-covers defined over k. With this notation:

Corollary 3.3. *If $Z(G) = \{1\}$ or if the short exact sequence $1 \to Z(G) \to G \to G/Z(G) \to 1$ is split then any projective system of k-rational points on any tower $(\mathcal{H}_{r_{n+1},G_{n+1}} \to \mathcal{H}_{r_n,G_n})_{n\geq 0}$ of Hurwitz spaces associated with the projective system $(s_n : G_{n+1} \twoheadrightarrow G_n)_{n\geq 0}$ actually lies in $\varprojlim_{n\geq 0} \mathcal{H}_{r_n,G_n}(k)^{noob}$.*

3.2. **Proof of theorem 3.1.** We consider first the case when P is a free pro-p group of finite rank and then deduce the general case.

3.2.1. *Two lemmas.* In this paragraph, assume P is a free pro-p group of finite rank. By proposition 3.2, it is enough to prove that $Z(G) \cap P_{n_0} = \{1\}$ for some $n_0 \geq 0$ or that $[G : Z(G)]$ is finite. We consider separately the case $\mathrm{rank}(P) \geq 2$ and $\mathrm{rank}(P) = 1$.

Lemma 3.4. ($\mathrm{rank}(P) \geq 2$) *If* $\mathrm{rank}(P) \geq 2$ *then* $P \cap Z(G) = \{1\}$*.*

Proof. Assume there exists $\underline{x} = (x_n)_{n\geq 0} \in P \cap Z(G) \setminus \{1\}$ and let $n_0 \geq 0$ be the smallest integer such that $\underline{x} \in P_{n_0} \setminus P_{n_0+1}$. Then, according to [RZ00], corollary 3.6.4, P_{n_0} is a free pro-p group of rank $\mathrm{rank}(P_{n_0}) = 1 + [P_0 : P_{n_0}](\mathrm{rank}(P_0) - 1) \geq 2$. And since $\underline{x} \in P_{n_0}$ is non zero modulo P_{n_0+1}, corollary 7.6.10 of [RZ00] shows there exists $(u_2, ..., u_r) \in P_{n_0}$ such that $(\underline{x}, u_2, ..., u_r) \in P_{n_0}$ freely generate P_{n_0}. The group P_{n_0} can be viewed as the free product $< \underline{x} > \coprod < u_2, ..., u_r >$ so, according to [RZ00], theorem 9.1.12, for any $\underline{y} \in P_{n_0} \setminus < \underline{x} >$ one has $< \underline{x} > \cap < \underline{x}^{\underline{y}} > = \{1\}$, in particular $\underline{x}^{-1}\underline{x}^{\underline{y}} \neq 1$: a contradiction since $\underline{x} \in Z(G)$. □

Lemma 3.5. (rank$(P)=1$) *If* rank$(P)=1$ *then either* $P\cap Z(G)=\{1\}$ *or* $[G:Z(G)]$ *is finite and, furthermore, if one of the two following condition is fulfilled: (i)* $[G,G]$ *is not finite or (ii) for each* $n\geq 0$, $p|\,|G_n|$, G_n *is p-perfect and the short exact sequences* $1\to P_n\to G\overset{s_n}{\to} G_n\to 1$ *is unsplit, then* $P\cap Z(G)=\{1\}$.

Proof. If rank$(P)=1$ and $P\cap Z(G)\neq\{1\}$ then by [RZ00], proposition 2.7.1, $P\cap Z(G)=<\underline{x}>$ for some $\underline{x}=(x_n)_{n\geq 0}\in P\setminus\{1\}$ and $[P:<\underline{x}>]$ is finite. As a result, $[G:Z(G)\cap P]=[G:P][P:<\underline{x}>]=|G_0|[P:<\underline{x}>]$ is finite and so, $[G:Z(G)]$ is too, whence the first assertion of lemma 3.5.

As for the second one, assume once again that $P\cap Z(G)=<\underline{x}>$ for some $\underline{x}=(x_n)_{n\geq 0}\in P\setminus\{1\}$ and observe that $P_n\simeq p^n\mathbb{Z}_p$, $n\geq 0$ thus, if n_0 is the smallest integer such that $\underline{x}\in P_{n_0}\setminus P_{n_0+1}$ we have $P_{n_0}=<\underline{x}>< Z(G)$.
(i) Now, since G is finitely generated, let $\tilde{g}_1,...,\tilde{g}_r\in G$ be a generating system of G and set $s_{n_0}(\tilde{g}_i)=g_i$, $i=1,...,r$. Denote by F_r the pro-free group with r generators $\gamma_1,...,\gamma_r$. The universal property of F_r allows us to define uniquely two epimorphisms $u:F_r\twoheadrightarrow G_{n_0}$ and $\tilde{u}:F_r\twoheadrightarrow G$ mapping γ_i to g_i and $\tilde{g}_i$ respectively; in particular $s\circ\tilde{u}=u$. Set $N=\ker(u)$ then, since P_{n_0} is central, $\tilde{u}([N,F_r])<[P_{n_0},G]=\{1\}$. Thus, we obtain the following commutative diagram of short exact sequences

$$\begin{tikzcd} 1 \arrow[r] & N\cap[F_r,F_r]/[N,F_r] \arrow[r] \arrow[d] & {[F_r,F_r]/[N,F_r]} \arrow[r, "u"] \arrow[d, "\overline{\tilde{u}}^0"] & {[G_{n_0},G_{n_0}]} \arrow[r] \arrow[d, "Id"] & 1 \\ 1 \arrow[r] & P_{n_0} \arrow[r] & {[G,G]} \arrow[r, "s"] & {[G_{n_0},G_{n_0}]} \arrow[r] & 1 \end{tikzcd}$$

But, by Schur's theorem, $N\cap[F_r,F_r]/[N,F_r]\simeq M(G_{n_0})$ is the Schur multiplier of G_{n_0} and, in particular, it is of finite exponent which implies, P_{n_0} being torsion free, that $N\cap[F_r,F_r]/[N,F_r]\subset\ker(\overline{\tilde{u}}^0)$ thus, the above commutative diagramm yields the following one

$$\begin{tikzcd} 1 \arrow[r] & 1 \arrow[r] \arrow[d] & {[F_r,F_r]/N\cap[F_r,F_r]} \arrow[r, "\overline{u}"] \arrow[d, "\overline{\tilde{u}}"] & {[G_{n_0},G_{n_0}]} \arrow[r] \arrow[d, "Id"] & 1 \\ 1 \arrow[r] & P_{n_0} \arrow[r] & {[G,G]} \arrow[r, "s"] & {[G_{n_0},G_{n_0}]} \arrow[r] & 1 \end{tikzcd}$$

where $\overline{\tilde{u}}$ maps a finite group onto a non finite group: a contradiction.
(ii) If G_{n_0} is p-perfect then, denoting by $M(G_{n_0})_p$ the p-part of the Schur multiplier of G_{n_0} there exists a central extension $1\to M(G_{n_0})_p\to\widehat{G^p_{n_0}}\overset{u}{\to}G_{n_0}\to 1$ which is universal for central extensions of G_{n_0} with p-group kernel [BF02], §3.6. Consequently, there exists a canonical commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & M(G_{n_0})_p \arrow[r] \arrow[d] & \widehat{G^p_{n_0}} \arrow[r, "u"] \arrow[d, "\tilde{u}"] & G_{n_0} \arrow[r] \arrow[d, "Id"] & 1 \\ 1 \arrow[r] & P_{n_0} \arrow[r] & G \arrow[r, "s"] & G_{n_0} \arrow[r] & 1 \end{tikzcd}$$

so, using once again the fact that $M(G_{n_0})_p$ is of finite exponent and P_{n_0} is torsion free, we have $M(G_{n_0})_p\subset\ker(\tilde{u})$, which leads to a commutative diagram

$$\begin{tikzcd} 1 \arrow[r] & 1 \arrow[r] \arrow[d] & \widehat{G^p_{n_0}}/M(G_{n_0})_p \arrow[r, "\overline{u}"] \arrow[d, "\overline{\tilde{u}}"] & G_{n_0} \arrow[r] \arrow[d, "Id"] & 1 \\ 1 \arrow[r] & P_{n_0} \arrow[r] & {[G,G]} \arrow[r, "s"] & G_{n_0} \arrow[r] & 1 \end{tikzcd}$$

so $\overline{\tilde{u}} \circ \overline{u}^{-1}$ provides a section of s_{n_0}: a contradiction. □

Remark 3.6. Proposition 3.2 leads to a statement slighty more precise than theorem 3.1: *Let* $1 \to P \to G \xrightarrow{s} G_0 \to 1$ *be a short exact sequence of profinite groups with* G_0 *a finite group and* P *a free pro-p group of finite rank. Let* k *be a field of characteristic* 0 *and* $K/\overline{k}(T)$ *a regular Galois extension with group* G *and field of moduli* k*, then*
- If $P \cap Z(G) = \{1\}$ *(for instance, if* $\mathrm{rank}(P) \geq 2$ *or if one of the two conditions (i), (ii) above is fulfilled) then* $K/\overline{k}(T)$ *is defined over a field extension* k_0/k *of degree* $[k_0 : k] \leq |G_0|$.
- Else, $K/\overline{k}(T)$ *is defined over a finite extension* k_0/k *with* $[k_0 : k] \leq [G : Z(G)]$.

In particular, when considering the universal p-Frattini cover ${}_p\tilde{\phi} :_p \tilde{G} \twoheadrightarrow G$ of a finite p-perfect group G, for each $n \geq 0$ ${}^n_p\tilde{\phi} :_p \tilde{G} \twoheadrightarrow^n_p \tilde{G}$ is the universal p-Frattini cover of ${}^n_p\tilde{G}$ and, as a result, does not split. Consequently, $Z({}_p\tilde{G}) \cap P = \{1\}$ and one obtains

Corollary 3.7. [3] *Let* G *be a finite group and* p *a prime dividing* $|G|$ *such that* G *is* p*-perfect. Then any regular Galois extension* $K/\overline{k}(T)$ *with group the universal* p*-Frattini cover* ${}^n_p\tilde{G}$ *of* G *is defined over a field extension* k_0/k *of degree* $[k_0 : k] \leq |G|$.

3.2.2. *The general case.* Consider now the case when P is a pronilpotent projective group, that is it can be written as the direct product $P \simeq \prod_{p|\,|P|} P_p$ of its Sylow subgroups and, for each $p|\,|P|$, P_p is a free pro-p group of finite rank. From the fact that P_p is a characteristic subgroup of P, $p|\,|P|$, deduce that $Z(G) \cap P \simeq \prod_{p|\,|P|} Z(G) \cap P_p$. Denote by S_1 the set of those prime $p||P|$ such that $Z(G) \cap P_p = \{1\}$, by S_2 the set of those prime $p|\,|P|$ such that $Z(G) \cap P_p \neq \{1\}$ and write $Q_i = \prod_{p \in S_i} P_p$, $i = 1, 2$. Then,
- $P/Q_2 \cap Z(G/Q_2) = \{1\}$ (indeed, for any $g_1 \in Q_1$, if $g_1 g g_1^{-1} g^{-1} \in Q_2$ for all $g \in G$ then, since Q_1 is a characteristic subgroup of P, one also has $g_1 g g_1^{-1} g^{-1} \in Q_1$ for all $g \in G$ and, as a result, $g_1 \in Z(G) \cap Q_1 = \{1\}$). So, according to proposition 3.2 (3), $K^{Q_2}/\overline{k}(T)$ is defined over a finite extension k_2/k.
- $[G/Q_1 : Z(G/Q_1)]$ is finite (indeed, since $Z(G) \cap Q_1 = \{1\}$, $Z(G)$ is a subgroup of $Z(G/Q_1)$ and, $[G/Q_1 : Z(G/Q_1)]$ divides $[G/Q_1 : (Z(G) \cap P)/Q_1]$ with $[G/Q_1 : (Z(G) \cap P)/Q_1] = |G_0|[P/Q_1 : (Z(G) \cap P)/Q_1] = |G_0|[Q_2 : Z(G) \cap Q_2]$, which is finite by lemmas 3.4 and 3.5). So, according to proposition 3.2 (2), $K^{Q_1}/\overline{k}(T)$ is defined over a finite extension k_1/k.
- Set $k_0 = k_1.k_2$, then $K^{Q_i}/\overline{k}(T)$ is defined over k_0 that is, there exists a regular Galois extension $K_i/k_0(T)$ with group G/Q_i such that $K_i.\overline{k} = K^{Q_i}$, $i = 1, 2$. Furthermore, $K_1^{Q_2}.\overline{k} = K^P = K_2^{Q_1}.\overline{k}$, so, up to taking a finite extension of k_0, we may assume that $K_1^{Q_2} = K_2^{Q_1} =: K_0$. Conclude by showing that $K_1.K_2/k_0(T)$ is a model for $K/\overline{k}(T)$. For this, set $Q_{i,n} = \prod_{p \in S_i} P_{p,n}$, $K_{i,n} = K_i^{Q_{i,n}}/k_0(T)$, $i = 1, 2$ and $K_n = K_{1,n}.K_{2,n}/k_0(T)$, $n \geq 0$. Then $K_1.K_2 = \cup_{n \geq 0} K_n$, which implies $K_1.K_2.\overline{k} = K$. So, we are left to show that $K_1.K_2/k_0(T)$ is regular or, equivalently, that $K_n/k_0(T)$ is regular, $n \geq 0$. This, in turn, is equivalent to $[K_n.\overline{k} : \overline{k}(T)] = [K_n : k_0(T)]$. On the one hand,

$$\begin{aligned}
[K_n.\overline{k} : \overline{k}(T)] &= [K_n.\overline{k} : K^P]|G_0| \\
&= [K^{Q_{1,n}}.K^{Q_{2,n}} : K^P]|G_0| \\
&= [K^{Q_{1,n}} : K^P][K^{Q_{2,n}} : K^P]|G_0| \\
&= [K_{1,n} : K_0][K_{2,n} : K_0]|G_0|
\end{aligned}$$

and, on the other hand, $[K_n : k_0(T)] = [K_n : K_0]|G_0|$. But, $[K_{i,n} : K_0]|[K_n : K_0]$, $i = 1, 2$, which entails $[K_{1,n} : K_0][K_{2,n} : K_0]|[K_n : K_0]$ (since $(|Q_1/Q_{1,n}|, |Q_2/Q_{2,n}|) = 1$) and so $[K_{1,n} : K_0][K_{2,n} : K_0] = [K_n : K_0]$.

[3] K.Kimura also obtained corollary 3.7, giving furthermore a precise description of the center $Z({}_p\tilde{G})$ of the universal p-Frattini cover of G.

4. Applications

4.1. **Projective systems of rational points on towers of Hurwitz spaces.** As an immediate consequence of theorems 2.1 and 3.1, one obtains the announced arithmetic property about projective systems of k-rational points on tower of Hurwitz spaces when k is a number field.

Theorem 4.1. *Let G be a profinite group admitting a quotient $\overline{G}$ presented as an extension of a finite group G_0 by a free pro-p group of finite rank. Then there is no Galois extension $K/\overline{k}(T)$ with group G and field of moduli a number field k. In other words, $\varprojlim_{n\geq 0}\mathcal{H}_{r,G_n}(k)=\emptyset$ for any tower of Hurwitz spaces $(\mathcal{H}_{r,G_{n+1}}\rightarrow\mathcal{H}_{r,G_n})_{n\geq 0}$ associated with G and any number field k.*

Proof. Let N be the kernel of the epimorphism $G\twoheadrightarrow\overline{G}$. Then $K^N/\overline{k}(T)$ is a Galois extension with group $\overline{G}$ and field of moduli k. So, according to theorem 3.1, $K^N/\overline{k}(T)$ is defined over a finite extension k_0/k, which contradicts theorem 2.1. □

As a special case of theorem 4.1, we obtain the following generalization of theorem 6.1 [BF02]

Corollary 4.2. *Let $\mathbf{C}$ a r-tuple of non trivial p'-conjugacy classes of G such that $\overline{\mathrm{sni}}(\mathbf{C})\neq\emptyset$. Then there is no projective systems of k points on the modular tower defined by the data $(G,p,\mathbf{C})$ for any number field $k/\mathbb{Q}$.*

In the following, let $1\rightarrow P\rightarrow G\xrightarrow{s}G_0\rightarrow 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a pronilpotent projective group of finite rank. Here is another consequence of theorem 3.1

Corollary 4.3. *G can be regularly realized over an algebraic extension $k/\mathbb{Q}$ where only a finite number of primes ramify.*

Proof. By construction, G is finitely generated so, let $g_1,...,g_r\in G$ be a generating system of G such that $g_1\cdots g_r=1$ and denote by C_i the conjugacy class of g_i, $i=1,...,r$. Set $\mathbf{C}=(C_1,...,C_r)$ and let $\mathbf{C}_n=(C_{1,n},...,C_{r,n})$ be the canonical image of $\mathbf{C}$ in $G_{n,P}:=G/\prod_{p|\,|P|}P_{p,n}$, $n\geq 0$. The projective system of r-tuples $(\mathbf{C}_n)_{n\geq 0}$ defines a tower of Hurwitz spaces

$$\mathcal{H}:=(\mathcal{H}_{r,G_{n+1,P}}(\mathbf{C}_{n+1})\rightarrow\mathcal{H}_{r,G_{n,P}}(\mathbf{C}_n))_{n\geq 0}$$

Consider then any $\mathbf{t}\in\mathcal{U}_r(\mathbb{Q})$ and a projective system of points $(\mathbf{p}_n)_{n\geq 0}$ on $\mathcal{H}$ above $\mathbf{t}$. Each $\mathbf{p}_n$ corresponds to a G-cover f_n with invariants $G_{n,P}$, $\mathbf{C}_n$, $\mathbf{t}$ and field of moduli k_n, $n\geq 0$. Denote by $S_\mathbf{t}$ the finite set of primes where $\mathbf{t}$ has bad reduction and by $S(|G_0|)$ the set of all prime divisors of $|G_0|$. By Beckmann's theorem [Be89], the only primes which may ramify in $k:=\cup_{n\geq 0}k_n$ are those from $S_\mathbf{t}\cup S(|G_0|)\cup\{p|P|\}$ and since all the $(f_n)_{n\geq 0}$ have their field of moduli contained in k, theorem 3.1 implies they all are defined over a finite extension k_0/k. □

Corollary 4.4. *G is the Galois group of an algebraic extension $k/\mathbb{Q}$ where only a finite number of primes ramify.*

Proof. By corollary 4.3, there exists a regular Galois extension $K/k(T)$ with group G, a finite number of branch points and such that $k/\mathbb{Q}$ is an algebraic extension where only a finite number of primes - $p_1,...,p_n$ - ramify. In particular, k is contained in the maximal algebraic extension $\mathbb{Q}_{p_1,...,p_n}/\mathbb{Q}$ unramified outside $p_1,...,p_r$. Let $q\notin\{p_1,...,p_n\}$ a prime then $\mathbb{Q}_{p_1,...,p_n}(\sqrt{q})/\mathbb{Q}_{p_1,...,p_n}$ is a proper quadratic extension (indeed, q ramifies in $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$!) and $\mathbb{Q}_{p_1,...,p_n}/\mathbb{Q}$ being Galois, deduce from Weissauer's theorem that $\tilde{k}:=\mathbb{Q}_{p_1,...,p_n}(\sqrt{q})$ is Hilbertian. Now, observe that G verifies (iv) of [S89], proposition 10.6, which allows us to conclude thanks to [S89], theorem

10.6. □

Finally, as already noticed, theorem 2.1 is also true for any finite field F of characteristic q not dividing $p|G_0|$. Likewise, replacing $\pi^{\mathrm{alg}}_{k,\mathbf{t}}$, $\pi^{\mathrm{ar}}_{k,\mathbf{t}}$ by their tame analogs $\pi_1^{\mathrm{tame}}(\mathbb{P}^1_{\overline{F}}\setminus\mathbf{t})$, $\pi_1^{\mathrm{tame}}(\mathbb{P}^1_F\setminus\mathbf{t})$, the proof of theorem 3.1 remains unchanged and we obtain: *For any finite field F of characteristic prime to $p|G_0|$ any regular extension $K/\overline{F}(T)$ with group G and field of moduli F is defined over a finite extension F_0/F.* Now, define for each prime q the subset $X_r^0(q)\subset\mathcal{U}_r(\overline{\mathbb{Q}})$ of all the divisors $\mathbf{t}\in\mathcal{U}_r(\overline{\mathbb{Q}})$ having good reduction at q and, given a number field k, by $X_r(k,q)$ the $\mathrm{PGL}_2(k)$-orbit of $X_r^0(q)$. Then

Proposition 4.5. *Still with the same notations:*
- For any tuple $\mathbf{C}$ of non trivial conjugacy classes of G, if $\mathbf{C}_n$ denotes the image of $\mathbf{C}$ in G_n, for any prime q not dividing $|G|$, any integer $d\geq 1$ there exists $n(\mathbf{C},q,d)\geq 0$ such that

$$\bigcup_{[k:\mathbb{Q}]\leq d}\Psi^{-1}_{r_n,{}_p^n\tilde{G}}(X_r(k,q))\cap\mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(k)=\emptyset,\ \ n\geq n(\mathbf{C},q,d).$$

- For any prime q not dividing $|G|$ and any finite extension $k/\mathbb{Q}_q$, there exists a regular realization of G over k iff G is generated by a finite number of elements of finite order and, in that case, any regular realization of G over k has a finite branch point divisor with bad reduction at q.

Proof. From [W98], corollary 4.2.3 and the remark following it, for any prime q not dividing $|G|$ the tower of Hurwitz spaces $(\mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1})\to\mathcal{H}_{r_n,G_n}(\mathbf{C}_n))_{n\geq 0}$ has good reduction modulo q. For any $n\geq 0$, let $f_n:X_n\to\mathbb{P}^1_{\overline{\mathbb{Q}}}$ be a G-cover with invariants G_n, $\mathbf{t}_n$, $\mathbf{C}_n$ and field of moduli a number field k_n such that $[k_n:\mathbb{Q}]=d$ (that is a k_n-rational point $\mathbf{p}_n$ on $\mathcal{H}_{r,G_n}(\mathbf{C}_n)$). Assume furthermore that for some prime q not dividing $|G|$, $\mathbf{t}_n\in X_r(k,q)$ for all $n\geq 0$ then, up to translating by elements of $\mathrm{PGL}_2(k)$, one may assume that $\mathbf{t}_n\in X_r^0(q)$ for all $n\geq 0$. As a result, for any place Q_n of k_n dividing q, f_n has good reduction modulo Q_n and reduces to a G-cover $\overline{f}_n$ with invariants G_n, $\overline{\mathbf{t}}_n$, $\mathbf{C}_n$ and field of moduli contained in $\mathbb{F}_{q^d}$ (that is a $\mathbb{F}_{q^d}$-rational point $\overline{\mathbf{p}}_n$ on the reduced Hurwitz space $\overline{\mathcal{H}}^q_{r_n,{}_p^n\tilde{G}}(\mathbf{C}_n)$)[4]. This produces a projective system of non-empty finite sets

$$(\overline{\mathcal{H}}^q_{r_{n+1},{}_p^{n+1}\tilde{G}}(\mathbf{C}_{n+1})(\mathbb{F}_{q^m})\to\overline{\mathcal{H}}^q_{r_n,{}_p^n\tilde{G}}(\mathbf{C}_n)(\mathbb{F}_{q^m}))_{n\geq 0}$$

the projective limit of which should be empty by the finite field version of theorem 4.1: a contradiction.

For the second part of the claim, the only if condition results from the fact lemma 2.3 holds for any field k of characteristic 0 such that $[k\cap\mathbb{Q}^{ab}:\mathbb{Q}]$ is finite so any regular realization $K/k(T)$ of G has only inertia groups of finite orders but then, these are the ones of the finite extension $K^P/k(T)$ so there are only finitely many of them. The if condition can be proved using Pop's Half Riemann existence theorem [P94] as in [DDes04]. The last assertion is obtained by reducing modulo q as above. □

Remark 4.6. The second part of proposition 4.5 leads to the following stronger version of theorem 4.1: *For any algebraic extension $k/\mathbb{Q}$ such that $\varprojlim_{n\geq 0}\mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(k)\neq\emptyset$ there are only finitely many primes q having an extension Q in $k/\mathbb{Q}$ with finite residue field and finite ramification indice.*

[4]Indeed, if Q is any place of $\overline{\mathbb{Q}}$ dividing Q_n, identifying $\Gamma_{\mathbb{F}_q}$ with D_Q/I_Q (where D_Q and I_Q respectively denote the decomposition and inertia groups of Q in $\overline{\mathbb{Q}}/\mathbb{Q}$), the reduction modulo Q yields a canonical Galois-equivariant isomorphism $c:(\pi^{\mathrm{alg}}_{\mathbb{Q},\mathbf{t}})^{(q')}\simeq(\pi^{\mathrm{alg}}_{\mathbb{F}_q,\mathbf{t}})^{(q')}$ and, if f_n corresponds to a group epimorphism $\Phi_{f_n}:(\pi^{\mathrm{alg}}_{\mathbb{Q},\mathbf{t}})^{(q')}\twoheadrightarrow{}_p^n\tilde{G}$ then $\overline{f}_n$ corresponds to $\Phi_{f_n}\circ c^{-1}$.

4.2. **The abelianization procedure.** We re-use in this section the method of lemmas 2.2, 2.3 to give an effective estimation of $n(\mathbf{C},q,d)^{noob}$ (where $n(\mathbf{C},q,d)^{noob}$ is defined as in proposition 4.5 but considering only the non obstruction locus) when $\mathbf{C}$ is a finite tuple of non trivial conjugacy classes of elements of finite order and discuss one of Fried's conjectures for modular towers.

We first described what we call the abelianization procedure. We still consider a short exact sequence of profinite groups $1 \to P \to G \to G_0 \to 1$ with G_0 a finite group and P a free pro-p group of finite rank ρ. As in lemmas 2.2, 2.3, write $\overline{G} = G/P^{ab}$, $\overline{G}_n = \overline{G}/(P^{ab})_n$, $n \geq 0$ and for any tuple $\mathbf{C}$ of conjugacy classes of G, $\overline{\mathbf{C}}$ for the image of $\mathbf{C}$ in $G \twoheadrightarrow \overline{G}$ and $\overline{\mathbf{C}}_n$ for the image of $\mathbf{C}$ in $G \twoheadrightarrow \overline{G} \twoheadrightarrow \overline{G}_n$, $n \geq 0$. From the canonical commutative diagrams of finite groups (*) one deduces the canonical commutative diagrams of Hurwitz spaces (**)

$$(*)\ \begin{array}{ccc} G_{n+1} & \twoheadrightarrow & \overline{G}_{n+1} \\ \downarrow & & \downarrow \\ G_n & \twoheadrightarrow & \overline{G}_n \end{array} \qquad (**)\ \begin{array}{ccc} \mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1}) & \twoheadrightarrow & \mathcal{H}_{r_{n+1},\overline{G}_{n+1}}(\overline{\mathbf{C}}_{n+1}) \\ \downarrow & & \downarrow \\ \mathcal{H}_{r_n,G_n}(\mathbf{C}_n) & \twoheadrightarrow & \mathcal{H}_{r_n,\overline{G}_n}(\overline{\mathbf{C}}_n) \end{array}$$

We call the right-hand sides of diagrams (*), (**) the abelianized situation corresponding to G, $\mathbf{C}$.

From now on, assume furthermore $\mathbf{C} = (C_1, ..., C_r)$ is a r-tuple of non trivial conjugacy classes of elements of finite order and write n_i for the order of any element of $C_{0,i}$, $i = 1, ..., r$. Then, given a number field k, any G-cover $f_n : X_n \to \mathbb{P}^1_k$ defined over k with invariants G_n, $\mathbf{C}_n$ induces a G-cover $\overline{f}_n : \overline{X}_n \to \mathbb{P}^1_k$ defined over k with invariants $\overline{G}_n$, $\overline{\mathbf{C}}_n$. Denote by $f_0 : X_0 \to \mathbb{P}^1_k$ the quotient of $\overline{f}_n$ modulo $P^{ab}/(P^{ab})_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^\rho$ (which is also the quotient of f_n modulo P/P_n); it is defined over k with invariants G_0, $\mathbf{C}_0$. Furthermore, with $n(\mathbf{C}_0) = \max_{1\leq i\leq t}\{n_i\}$, one can always find a field extension k_0/k of degree $[k_0 : k] \leq \frac{|G|}{n(\mathbf{C}_0)}$ such that $X_0(k_0) \neq \emptyset$. Furthermore, since $X_n \times_k k_0 \to X_0 \times_k k_0$ is an etale cover defined over k_0 with group $P^{ab}/(P^{ab})_n$, it rises from a cartesian diagram

$$\begin{array}{ccc} X_n \times_k k_0 & \longrightarrow & A_n \\ \downarrow & \square & \downarrow \\ X_0 \times_k k_0 & \longrightarrow & \mathrm{Jac}(X_0 \times_k k_0) \end{array}$$

where A_n is an abelian variety defined over k_0, isogenous to $\mathrm{Jac}(X_0 \times_k k_0)$ and carrying a k_0-torsion point of order p^n. Conclude

Abelianization procedure conclusion: *Given a number field k and an integer $n \geq 0$, any G-cover $f_n : X_n \to \mathbb{P}^1_k$ defined over k with invariants G_n, $\mathbf{C}_n$ gives rise to an abelian variety A_n defined over an extension k_0 of k of degree $[k_0 : k] \leq \frac{|G|}{n(\mathbf{C}_0)}$, isogenous to $Jac(X_0 \times_k k_0)$ and carrying a k_0-torsion point of order p^n.*

We are going to use this conclusion to give an effective bound for $n(\mathbf{C},q,d)^{noob}$. For this, define

$$g(\mathbf{C}_0) = 1 + |G|(\frac{1}{2}\sum_{i=1}^{r}\frac{n_i - 1}{n_i} - 1)$$

and, given integers $g, n, m \geq 1$,

$$c(g,n,m) = n^{mg} + 2gn^{(m-1)/2} + (2^g - 2g - 1)n^{m-1}$$

With these notations, we can state

Proposition 4.7.
$$n(\mathbf{C}, q, d)^{noob} \leq \frac{\ln(c(g(\mathbf{C}_0), q^{d|G_0|/n(\mathbf{C}_0)}, 1))}{\ln(p)}$$

Proof. Let k be any number field such that $[k:\mathbb{Q}] \leq d$ and $f_n : X_n \to \mathbb{P}^1_k$ be a G-cover defined over k with invariants G_n, $\mathbf{C}_n$, $\mathbf{t}$. Let q be a prime not dividing $p|G_0|$ and such that $\mathbf{t} \in X_r(k, q)$; up to translating f_n by an element of $\mathrm{PGL}_2(k)$, we can assume $\mathbf{t} \in X^0_r(q)$. Let Q be any place of k_0 dividing q then X_0 has good reduction at Q and, consequently, so does $\mathrm{Jac}(X_0 \times_k k_0)$. As a result, if F denotes the residue field of k_0 at Q, $p^n | \ |\overline{\mathrm{Jac}(X_0 \times_k k_0)|^Q}(F)$ so, in particular,
$$n \leq \frac{\ln(|\overline{\mathrm{Jac}(X_0 \times_k k_0)|^Q}(F))}{\ln(p)}$$
Writing F_m for the unique degree m extension of F (in a given algebraic closure of F), we are left to compute $|\overline{\mathrm{Jac}(X_0 \times_k k_0)|^Q}(F_m)$. For this observe that by Riemann-Hurwitz formula, X_0 has genus $g = g(\mathbf{C}_0)$ so $\overline{\mathrm{Jac}(X_0 \times_k k_0)|^Q}$ is a g-dimensional abelian variety defined over F which, by Lang-Weil bounds [Mi86], theorem 9.1, yields
$$||\overline{\mathrm{Jac}(X_0 \times_k k_0)|^Q}(F_m)| - |F|^{mg}| \leq 2g|F|^{(m-1)/2} + (2^g - 2g - 1)|F|^{m-1}$$
and conclude using $|F| \leq q^{d|G_0|/n(\mathbf{C}_0)}$. □

The proof of proposition 4.7 shows that, writing $Y^0_r(k, q)$ for the set of all the divisor $\mathbf{t} \in \mathcal{U}_r(\overline{\mathbb{Q}})$ such that the jacobian $\mathrm{Jac}(X_0)$ of any G-cover $f_0 : X_0 \to \mathbb{P}^1_k$ with invariants G_0, $\mathbf{C}_0$, $\mathbf{t}$ has good reduction at any place Q of k dividing q and $Y_r(k, q)$ for its $\mathrm{PGL}_2(k)$-orbit, we have *For any r-tuple $\mathbf{C}$ of non trivial conjugacy classes of elements of finite order, for any prime q not dividing $p|G_0|$ and for any integer $d \geq 1$ there exists $n(\mathbf{C}, q, d)^{noob} \geq 0$ such that* $\bigcup_{[k:\mathbb{Q}] \leq d} \Psi^{-1}_{r,G_n}(Y_r(k, q)) \cap \mathcal{H}_{r,G_n}(\mathbf{C}_n)(k)^{noob} = \emptyset$, $n \geq n(\mathbf{C}, q, d)^{noob}$. The proof of proposition 4.10 shows that up to enlarge $n(\mathbf{C}, q, d)^{noob}$ this statement remains true without the "noob" labellings provided that $Z(G) \cap P = \{1\}$.

Consider the following variant of Fried's conjectures for modular towers [FK97], [D04]

Conjecture 4.8. (Fried) *Let G be a p-perfect finite group then, for any integer $r \geq 3$, any r-tuple $\mathbf{C}$ of p'-conjugacy classes of G and any integer $d \geq 1$ there exists $n(d, g(\mathbf{C})) \geq 0$ such that*
$$\bigcup_{[k:\mathbb{Q}] \leq d} \mathcal{H}_{r, {}^n_p\tilde{G}}(\mathbf{C}_n)(k) = \emptyset, \text{ for each } n \geq n(d, g(\mathbf{C}))$$

The abelianization procedure statement suggests it is connected to the Strong Torsion Conjecture for abelian varieties [Si92], [Ka98]

Conjecture 4.9. (S.T.C.) *Given two integers g, $d \geq 1$, there exists an integer $n(d, g) \geq 1$ such that the set of all abelian varieties A (i) defined over a number field k of degree $[k:\mathbb{Q}] \leq d$, (ii) of dimension g and (iii) carrying a k-rational torsion point of order n is empty for $n \geq n(d, g)$.*

Indeed, conjecture 4.9 combined with the abelianization procedure conclusion and the arguments of the proof of proposition 4.7 implies that with $n(d, g(\mathbf{C}))^{noob} := n(g(\mathbf{C}), \frac{d|G|}{n(\mathbf{C})}) \geq 0$ such that
$$\bigcup_{[k:\mathbb{Q}] \leq d} \mathcal{H}_{r, {}^n_p\tilde{G}}(\mathbf{C}_n)(k)^{noob} = \emptyset, \text{ for each } n \geq n(d, g(\mathbf{C}))^{noob}$$
and this result yields

Proposition 4.10. *Conjecture 4.9 implies conjecture 4.8.*

Proof. From lemmas 3.4, 3.5 we have $P \cap Z({}_p\tilde{G}) = \{1\}$ so, in particular, for each $n \geq 0$ there exists $N_n \geq n$ such that the image of $P/P_{N_n} \cap Z({}_p^{N_n}\tilde{G})$ in $P/P_n \cap Z({}_p^{n}\tilde{G})$ via the canonical epimorphism $s_{N_n,n}$ is trivial (recall that $P \cap Z({}_p\tilde{G}) = \varprojlim_{n\geq 0} P/P_n \cap Z({}_p^{n}\tilde{G})$). Setting

$$\begin{array}{lll} n_1 & = & n(g(\mathbf{C}), \frac{d|G|}{n(\mathbf{C})}) \\ n_2 & = & N_{n_1} \\ d_0 & = & |G| \end{array}$$

we are going to show that for any integer $d \geq d_0$

$$\bigcup_{[k:\mathbb{Q}]\leq d/d_0} \mathcal{H}_{r,{}_p^n\tilde{G}}(\mathbf{C}_n)(k) = \emptyset, \text{ for each } n \geq n_2$$

Indeed, let k be any number field such that $[k : \mathbb{Q}] \leq d/d_0$ and suppose there exists a G-cover $f_{n_2} : X_{n_2} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ with invariants ${}_p^{n_2}\tilde{G}$, $\mathbf{C}_{n_2}$ and field of moduli k. Denote by f_{n_1} its quotient modulo P_{n_1}/P_{n_2}. Let $[\omega_{n_2}] \in \mathrm{H}^2(k, Z({}_p^{n_2}\tilde{G}))$ be the cohomological obstruction for f_{n_2} to be defined over k then $[s_{n_2,n_1} \circ \omega_{n_2}] \in \mathrm{H}^2(k, Z({}_p^{n_1}\tilde{G}))$ is the cohomological obstruction for f_{n_1} to be defined over k. Consider the following canonical diagram

$$\begin{tikzcd}
1 \arrow[r] & s_{n_2,0}(Z({}_p^{n_2}\tilde{G})) \arrow[r] & G \arrow[r] & G/s_{n_2,0}(Z({}_p^{n_2}\tilde{G})) \arrow[r] & 1 \\
1 \arrow[r] & Z({}_p^{n_2}\tilde{G}) \arrow[r] \arrow[u, "\simeq"] & {}_p^{n_2}\tilde{G} \arrow[r] \arrow[u, two heads, "s_{n_2,0}"] & {}_p^{n_2}\tilde{G}/Z({}_p^{n_2}\tilde{G}) \arrow[r] \arrow[u, "\overline{s}_{n_2,0}"] & 1 \\
 & & & \Gamma_k \arrow[u, "\overline{\phi_{n_2}}"] &
\end{tikzcd}$$

and set $k_0 := \overline{k}^{\ker(\overline{s}_{n_2,0}\circ\overline{\phi}_{n_2})}$. Then $[s_{n_2,0} \circ \omega_{n_2}] = 0$ in $\mathrm{H}^2(k_0, s_{n_2,0}(Z({}_p^{n_2}\tilde{G})))$ that is there exists $\tilde{h} : \Gamma_{k_0} \to s_{n_2,0}(Z({}_p^{n_2}\tilde{G}))$ such that $s_{n_2,0} \circ \omega_{n_2}(\sigma,\tau) = \tilde{h}(\sigma\tau)^{-1}\tilde{h}(\sigma)\tilde{h}(\tau)$, $\sigma, \tau \in \Gamma_{k_0}$. Since $s_{n_2,0} : Z(G_{n_2}) \twoheadrightarrow s_{n_2,0}({}_p^{n_2}\tilde{G}))$ is an epimorphism, one can define a map $\tilde{h}_{n_2} : \Gamma_{k_0} \to Z({}_p^{n_2}\tilde{G})$ such that $s_{n_2} \circ \tilde{h}_{n_2} = \tilde{h}$ and thus a coboundary

$$\begin{array}{rccl} \tilde{\omega}_{n_2}: & \Gamma_{k_0}^2 & \to & Z({}_p^{n_2}\tilde{G}) \\ & \sigma,\tau & \to & \tilde{h}_{n_2}(\sigma\tau)^{-1}\tilde{h}_{n_2}(\sigma)\tilde{h}_{n_2}(\tau) \end{array}$$

Now, up to replacing ω_{n_2} by the equivalent cocycle $\omega_{n_2}\tilde{\omega}_{n_2}^{-1}$, one has $s_{n_2,0} \circ \omega_{n_2} = 0$ that is $\mathrm{Im}(\omega_{n_2}) < P/P_{n_2} \cap Z({}_p^{n_2}\tilde{G})$. But then, by definition of n_2, we have $s_{n_2,n_1} \circ \omega_{n_2} = 0$ and, consequently, f_{n_1} is defined over k_0, which contradicts the definition of n_1. □

Remark 4.11. In conjecture 4.8, replace the bound $n(d, g(\mathbf{C}))$ by a bound $n(d, g(\mathbf{C}), p)$ depending furthermore on p. Likewise, in conjecture 4.9, replace the bound $n(d, g)$ by a bound $n(d, g, p)$ also depending on p and condition (iii) by condition (iii)' *carrying a k-rational torsion point of order p^n.* We thus obtain two weaker conjectures for which proposition 4.10 remains true.

The discussion above provides a conjectural approach of conjecture 4.8. When considering the weaker form of conjecture 4.8 obtained by replacing the bound $n(\mathbf{C}, d)$ by a bound $n(\mathbf{C}, k)$ depending on the number field k, there is an alternative conjectural approach, based on reduced modular towers $(\mathcal{H}^{rd}_{r,{}_p^{n+1}\tilde{G}}(\mathbf{C}_{n+1}) \to \mathcal{H}^{rd}_{r,{}_p^n\tilde{G}}(\mathbf{C}_n))_{n\geq 0}$ (we refer to [FK97] or [DF99] for the existence and properties of reduced Hurwitz spaces. In brief, $\mathcal{H}^{rd}_{r,G}(\mathbf{C})$ is the quotient space $\mathcal{H}_{r,G}(\mathbf{C})/\mathrm{PSL}_2(\mathbb{C})$ where the action of $\mathrm{PSL}_2(\mathbb{C})$ on $\mathcal{H}_{r,G}(\mathbf{C})$ is obtained by extending the one of $\mathrm{PSL}_2(\mathbb{C})$ on $\mathcal{U}_r(\mathbb{C})$ and, in particular, it is a $r-3$-dimensional variety). This approach consists in proving that all the geometrically irreducible component of $\mathcal{H}^{rd}_{r,{}^n_p\tilde{G}}(\mathbf{C}_n)$ are of general type (of genus ≥ 2 when $r=4$) and then, relying on Bombieri-Lang conjecture (Faltings' theorem when $r=4$), obtaining that if $\mathcal{H}^{rd}_{r,{}^n_p\tilde{G}}(\mathbf{C}_n)(k) \neq \emptyset$ for all $n \geq 0$ then $\varprojlim_{n\geq 0} \mathcal{H}^{rd}_{r,{}^n_p\tilde{G}}(\mathbf{C}_n)(k) \neq \emptyset$. Up to taking a finite extension k_0/k, this entails that $\varprojlim_{n\geq 0} \mathcal{H}_{r,{}^n_p\tilde{G}}(\mathbf{C}_n)(k_0) \neq \emptyset$, [DF99] §6.5, contradicting theorem 4.1. When $r=4$, M. Fried gives in [F04] an outline of the proof of the fact all the geometrically irreducible components of $\mathcal{H}^{rd}_{4,{}^n_p\tilde{G}}(\mathbf{C}_n)$ have genus ≥ 2 for n large enough.

References

[BF02] P. Bayley et M. Fried, *Hurwitz monodromy, spin separation and higher levels of Modular Towers*, Proceedings of the Von Neumann Symposium on Arithmetic Fundamental Groups and Noncommutative Algebra (MSRI 1999), Proceedings of Symposia in Pure Mathematics, AMS, ed. par M. Fried et Y. Ihara, 2002.

[Be89] S. Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*, J. Algebra, **125**, p.236-255, 1989.

[D04] P. Dèbes *Modular Towers, construction and diophantine questions*, Preprint, 2004.

[DDes04] P.Dèbes and B. Deschamps, *Corps ψ-libres et théorie inverse de Galois infinie*, J. fur die reine und angew. Math., to appear.

[DDo97] 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.

[DF99] P.Dèbes and M. Fried, *integral spacialization of families of rational functions*, Pacific J. Math. **190** No1, p. 45-85, 1999.

[F95a] M. Fried, *Introduction to Modular Towers:Generalizing the relation between dihedral groups and modular curves*, Proceedings AMS-NSF Summer Conference, **186**, Cont. Math. series, Recent Developments in the Inverse Galois Problem, p.111-171, 1995.

[F95b] M. Fried, *Topics in Galois theory*, expanded version of review of Serre's book with same title, Proceedings AMS-NSF Summer Conference, **186**, Contemporary Math., Recent Developments in the Inverse Galois Problem, p.111-171, 1995.

[F04] M. Fried, *Higher rank modular towers*, preprint, 2004.

[FK97] M.Fried and Y.Kopeliovich, *Applying modular towers to the inverse Galois problem*, in *Geometric Galois Action*, London Math. Soc. Lecture Note Series **243**, L.Schneps and P.Lochak ed., Cambridge University Press, p. 151-175, 1997.

[FV91] M. Fried and H. Volklein, *The Inverse Galois Problem and Rational Points on Moduli Spaces*, Math. Ann. **290**, p. 771-800, 1991.

[Ka98] S. Kamienny *On torsion in abelian varieties*, Communication in Algebra **26**, p. 1675-1678, 1998.

[L96] D. Lorenzini, *An invitation to arithmetic geometry*, G.S.M. vol. **9**, A.M.S., 1996.

[MMa99] G. Malle and H.B. **Matzat**, *Inverse Galois theory*, S.M.M., Springer-Verlag, 1999.

[Mi86] J.S. Milne , *Abelian varieties*, in *Arithmetic Geometry*, G. Cornell and J.H. Silverman ed., Springer-Verlag, 1986.

[P94] F. Pop *Half Riemann's existence theorem with Galois action*, Algebra and number theory, De Gruyter Proceedings in Mathematics, p.1-26, 1994.

[RZ00] L.Ribes and P.Zalesskii, *Profinite Groups*, E.M.G. **40**, Springer-Verlag, 2000.

[S89] J.-P.Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, Friedr. Wieweg & Sohn, 1989.

[Si92] A. Silverberg, *Points of finite order on Abelian varieties*, in *p-adic Methods in Number Theory and Algebraic Geometry*, Adolphson, Sperber, Tretkoff eds; Contmporary Math. **133**, A.M.S., p. 175-193, 1992.

[V99] H.Volklein, *Groups as Galois groups - an introduction*, Cambridge Studies in Advanced Mathematics **53**, Cambridge University Press, 1999.

[W98] S.Wewers *Construction of Hurwitz spaces*, thesis, Preprint **21** of the I.E.M., Essen, 1998.