ABELIAN CONSTRAINTS IN INVERSE GALOIS THEORY

ANNA CADORET AND PIERRE DÈBES

Abstract. We show that if a finite group G is the Galois group of a Galois cover of $\mathbb{P}^1$ over $\mathbb{Q}$, then the orders p^n of the abelianization of its p-Sylow subgroups are bounded in terms of their index m, of the branch point number r and the smallest prime $\ell \nmid |G|$ of good reduction of the branch divisor. This is a new constraint for the regular inverse Galois problem: if p^n is suitably large compared to r and m, the branch points must coalesce modulo small primes. We further conjecture that p^n should be bounded only in terms of r and m. We use a connection with some rationality question on the torsion of abelian varieties. For example, our conjecture follows from the so-called torsion conjectures. Our approach also yields a new viewpoint on Fried's Modular Tower program.

1. Introduction

The central idea behind this work is this. Suppose we are given a finite Galois cover $Y \to \mathbb{P}^1$ over some field k with Galois group G and with ramification indices prime to some prime divisor p of the order of G. Then if P is a p-Sylow subgroup of G, the containment $[P,P] \subset P$ corresponds, *via* Galois theory, to a non-trivial unramified abelian curve cover $Z \to X$ (with group the abelianization P^{ab}). This imposes some non-trivial condition on the Jacobian $\mathrm{Jac}(X)$.

We deduce some bounds on the order of P^{ab}. The first ones, theorem 2.1 and theorem 2.6, use known estimates for the number of rational torsion points on a Jacobian variety, over a finite field for theorem 2.1 and over an ℓ-adic field for theorem 2.6. If $k = \mathbb{Q}$ for example, we obtain a bound involving the number r of branch points, the index m of the p-Sylow subgroups of G and the smallest prime $\ell \nmid |G|$ of good reduction of the branch divisor of $Y \to \mathbb{P}^1$. We also have a conjectural bound, which only depends on r and m: conjecture 2.2

Date: November 15, 2007.

2000 *Mathematics Subject Classification.* Primary 12F12 14H30 11Gxx; Secondary 14G32 14Kxx 14H10.

Key words and phrases. inverse Galois theory, Hurwitz spaces, abelian varieties, torsion, modular towers.

relies on standard conjectures on the torsion of abelian varieties over a number field.

These bounds for the order p^n of P^{ab} can be regarded as new constraints in inverse Galois theory: from our theorems, the branch points of a Galois cover $Y \to \mathbb{P}^1_{\mathbb{Q}}$ of group G must coalesce modulo small primes not dividing $|G|$ if p^n is suitably large compared to r and m; from our conjecture, p^n should actually be bounded in terms of r and m. Dihedral groups D_{p^n} are typical examples: if r is bounded, possible realizations as above have bad reduction modulo any given prime $\ell \neq 2, p$ provided n is suitably large and conjecturally only finitely many of them can be realized with r bounded. More generally we show this holds with the dihedral groups D_{p^n} replaced by characteristic quotients G_n of the universal p-Frattini cover of any finite group.

These results have some modular interpretation in terms of existence of rational points on certain towers of moduli spaces — Fried's Modular Towers — which the tower of modular curves $(Y_1(p^n))_{n\geqslant 1}$ is the starting example of. We show the main conjecture of the Modular Tower program is a special case of our conjecture, and so also a consequence of the standard torsion conjectures. And as a consequence of our results, we prove a weak form of the Modular Tower conjecture.

The paper is organized as follows. Theorem 2.1 and conjecture 2.2, our central statements, are given in §2.1. Theorem 2.1 is proved in §2.3 and some generalization of it, theorem 2.6, in §2.5. Some first consequences to inverse Galois theory, including a proof of conjecture 2.2 for 3 branch points covers, are given in §2.2 and §2.6. In §2.4 we discuss the connection with the torsion of abelian varieties. Section 3 is devoted to the Modular Tower program. The Modular Tower conjecture and corollary 3.1, our weak form of it, are first given in §3.1 in terms of realization of the characteristic quotients G_n alluded to above. The connection with conjecture 2.2 and the torsion conjectures is also established in this subsection. §3.2 reinterprets corollary 3.1 and the Modular Tower conjecture in terms of moduli spaces. §3.3 is concerned with the PGL_2-reduced variants for which covers and their moduli spaces are regarded modulo the natural action of PGL_2. The paper ends with an appendix about the equivalence of the versions of the Modular Tower conjecture over stacks and over moduli spaces.

2. Central Results

Given a field k, we denote its algebraic closure by $\overline{k}$, its separable closure by k^{s} and its absolute Galois group by $\mathrm{Gal}(k^{\mathrm{s}}/k)$.

Given a k-curve[1] B and a finite group G, a k-G-cover of B with group G is a Galois cover $f : X \to B$ of k-curves given with an isomorphism between its automorphism group and G [2]. An isomorphism between two k-G-covers $f : X \to B$ and $g : Y \to B$ is an isomorphism $\chi : X \to Y$ of k-curves such that $g \circ \chi = f$ and which is compatible with the actions of G.

A k^{s}-G-cover $f : X \to B_{k^{\mathrm{s}}}$[3] is said to be defined over k if there exists a k-model of f, that is a k-G-cover $f_k : X_k \to B$ such that the G-cover obtained from f_k by extension of scalars to k^{s} is isomorphic to f. In this case, k is the field of moduli (relative to the extension k^{s}/k): that is, f is isomorphic to each of its conjugate covers f^τ where $\tau \in \mathrm{Gal}(k^{\mathrm{s}}/k)$. The converse is not true in general; see [DD97] for more on fields of definition versus field of moduli. We note that if $f : X \to B_{k^{\mathrm{s}}}$ has field of moduli k, then its branch divisor is defined over k.

Suppose given a field F with a discrete valuation v with valuation ring R and such that the curve B has a model B_R over $\mathrm{Spec}(R)$ with good reduction. We say that a proper closed subset $D \subset B_{\overline{F}}$ is *smooth at v (or modulo its valuation ideal $\mathfrak{p}$)* if each geometric point of D is defined over F^{s} and if no two F^{s}-points of D *coalesce* at any prime over $\mathfrak{p}$, *i.e.* for any two F^{s}-points of D, their closures in $B_{R^{\mathrm{s}}}$ do not meet on the fiber over any prime of R^{s} lying over $\mathfrak{p}$, where R^{s} is the integral closure in F^{s}. For $B = \mathbb{P}^1$, this last condition can be rephrased more explicitly: View $\mathbb{P}^1_{F^{\mathrm{s}}}$ as the t-line and consider two geometric points $\alpha = (t = a)$ and $\alpha' = (t = a')$, where $a, a' \in F^{\mathrm{s}} \cup \{\infty\}$. Then α, α' coalesce at a prime $\mathfrak{p}^{\mathrm{s}}$ of R^{s} over $\mathfrak{p}$ if $|a|_{\mathfrak{p}^{\mathrm{s}}} \leqslant 1$, $|a'|_{\mathfrak{p}^{\mathrm{s}}} \leqslant 1$, and $|a - a'|_{\mathfrak{p}^{\mathrm{s}}} < 1$, or else if $|a|_{\mathfrak{p}^{\mathrm{s}}} \geqslant 1$, $|a'|_{\mathfrak{p}^{\mathrm{s}}} \geqslant 1$, and $|a^{-1} - a'^{-1}|_{\mathfrak{p}^{\mathrm{s}}} < 1$. We sometimes say D has *good reduction* at v instead of "smooth at v". In the opposite case, we say D is *singular* or has *bad reduction* at v.

2.1. **Central statements.** In the statements below, we consider the general situation where P is any subgroup of G (and not only a p-Sylow subgroup as in the introduction).

Theorem 2.1. *Let G be a finite group, k be a henselian field (for a discrete valuation v) with finite residue field $\mathbb{F}_q$ of characteristic prime to $|G|$. Let $f : Y \to \mathbb{P}^1$ be a k^{s}-G-cover of group G, field of moduli k and branch divisor smooth at v. If P is any non trivial subgroup of G of order prime to each of the ramification indices $e_1, \ldots, e_r$ of f and P^{ab} is its abelianization, then we have*

[1] By k-curve, we mean a smooth projective and geometrically connected k-scheme of dimension 1.

[2] We always omit this isomorphism in the notation though it is part of the data.

[3] As usual $B_{k^{\mathrm{s}}}$ is the curve obtained from B by scalar extension from k to k^{s}.

$$|P^{\mathrm{ab}}| \leqslant \mathrm{e}\,(2\sqrt{\mathrm{e}}\,g)^{[G:P]-1}\,q^g$$

where $g = 1 + \frac{1}{2}[G:P](r-2-\sum_{i=1}^{r} 1/e_i)$ *and* $\mathrm{e} = 2,718\ldots$.

A more general and improved form of theorem 2.1 is given in §2.5. For example we need not restrict to covers of $\mathbb{P}^1$ and some of the assumptions (*e.g.* ramification indices are prime to $|P|$) can be weakened. Theorem 2.1 is the ready-to-use version for our main application in section 3. Theorem 2.1 and its generalization are proved in §2.3 and §2.5.

Assume G has a regular realization over some number field K, *i.e.* there exists a G-cover $f : Y \to \mathbb{P}^1$ of group G defined over K. If P is a subgroup of G as above, it follows from theorem 2.1 that $|P^{\mathrm{ab}}|$ can be bounded in terms of K, $[G:P]$, r and the places of bad reduction of the branch divisor. We conjecture the last dependence is unnecessary.

Conjecture 2.2. *Let $m_0 \geqslant 1$ and $r \geqslant 0$ be two integers. Let G be the Galois group of some G-cover $f : Y \to \mathbb{P}^1$ defined over the number field K with at most r branch points. If P is any subgroup of G of order prime to each of the ramification indices $e_1, \ldots, e_r$ of f and of index $[G:P] \leqslant m_0$, then the order of its abelianization P^{ab} can be bounded by a constant depending only on r, m_0 and K.*

There are several variants of the conjecture: its conclusion may be required to hold only for p-subgroups $P \subset G$ (with a constant also depending on p); or the exponent of P^{ab}, instead of its order, may be claimed to be bounded; the dependence of the constant in K may only involve the degree $[K:\mathbb{Q}]$, etc. We will specify when necessary which variant may or should be used.

2.2. **A new constraint in inverse Galois theory.** The case P is a non trivial p-Sylow subgroup of G is of special interest as the order p^n of P^{ab} is $\geqslant p$ (and even $\geqslant p^2$ if $|P| \geqslant p^2$). Assume as above a regular realization $f : Y \to \mathbb{P}^1_K$ of G defined over the number field K is given with at most r branch points and prime-to-p ramification. Conjecture 2.2 predicts that p^n should be bounded in terms of r, $m = [G:P]$ and K. Theorem 2.1 yields the following.

Corollary 2.3. *The branch divisor of f is singular modulo every prime $\ell \not| |G|$ such that $\mathrm{e}\,(2\sqrt{\mathrm{e}}\,\gamma)^{m-1}\,\ell^{\gamma[K:\mathbb{Q}]} < p^n$* [4]*, where $\gamma = 1 + m(r-2)/2$. This includes at least one prime ℓ if p^n is bigger than some constant depending only on r, m and $[K:\mathbb{Q}]$.*

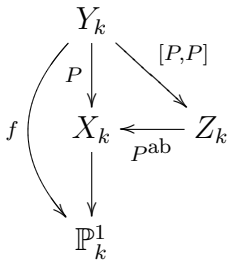
[4]Bounding the cardinality q of the residue field $\mathbb{F}_q$ of places of K by $\ell^{[K:\mathbb{Q}]}$ with ℓ the characteristic of $\mathbb{F}_q$ makes the inequality of theorem 2.1 independent of the place v above ℓ. That is why we may use primes of $\mathbb{Q}$ here.

For instance, if $|G| = 3\,.\,97^N$ with $N \geqslant 2$, then every 4-branch-point regular realization of G over $\mathbb{Q}$ with prime-to-97 ramification necessarily has branch points that coalesce modulo 2. Other more structured examples are given in example 2.5 and in §3.1.

It was already known that the branch points of potential regular realizations of some finite group G over some number field K should satisfy certain conditions: their number should be bigger than the rank of G (a topological condition); actions of $\mathrm{Gal}(\overline{K}/K)$ on them and on the ramification type should be compatible (an arithmetical condition known as the "branch cycle argument" [Völ96, p.34]). Corollary 2.3 is a new constraint.

2.3. **Proof of theorem 2.1.** Let $f : Y \to \mathbb{P}^1$ be a k^{s}-G-cover of group G, field of moduli k and branch divisor smooth at v, with G, k and v as in the statement. From [DH98, theorem 3.1], $f : Y \to \mathbb{P}^1$ is defined over its field of moduli as G-cover. Let $f_k : Y_k \to \mathbb{P}^1_k$ be a k-model of f.

Let $P \subset G$ be a subgroup as in the statement. The k-G-cover $f_k : Y_k \to \mathbb{P}^1_k$ factors as shown on the diagram below



where $Y_k \to X_k$ is a k-G-cover with group P and which is unramified due to the assumption on $|P|$ (in particular X_k is of genus $g \neq 0$) and $X_k \to \mathbb{P}^1_k$ is a k-cover of degree $[G : P]$. In turn the k-G-cover $Y_k \to X_k$ factors through some unramified k-G-cover $Y_k \to Z_k$ with group the commutator subgroup $[P, P]$ of P. The corresponding quotient $Z_k \to X_k$ is an unramified k-G-cover with group P^{ab}.

The abelian etale cover $Z_k \to X_k$ induces a k-isogeny $\alpha : A \to \mathrm{Jac}(X_k)$ with the property that its geometric kernel $\ker(\alpha)(k^{\mathrm{s}})$ is isomorphic to the trivial $\mathrm{Gal}(k^{\mathrm{s}}/k)$-module P^{ab} [Cad07c, lemma 1.4] [5]; in particular, $\ker(\alpha)(k^{\mathrm{s}})$ is contained both in the $|P^{\mathrm{ab}}|$-torsion part of A and in $A(k)$.

From [Ful69, theorem 3.3], the cover $X_k \to \mathbb{P}^1_k$ has good reduction at v and so do the curve X_k and its Jacobian $\mathrm{Jac}(X_k)$ [Mil86, corollary

[5] This is classical when k is algebraically closed [Ser59, Chap.6, §2.12] [Mil86, Prop.9.1]. The paper [Cad07c] extends this result to arbitrary fields.

12.3]. As we assume $(q, |G|) = 1$, the isogeny α reduces modulo v to an isogeny $\overline{\alpha} : \overline{A} \to \overline{\mathrm{Jac}(X_k)}$ [BLR90, proposition 7.3.6]; in particular, $|\overline{A}(\mathbb{F}_q)| = |\overline{\mathrm{Jac}(X_k)}(\mathbb{F}_q)|$ [Tat66]. Furthermore reduction modulo v is injective on the $|P^{\mathrm{ab}}|$-torsion part of A [BLR90, lemma 7.3.2] and so also on $\ker(\alpha)(k^{\mathrm{s}}) \subset A(k)$. Whence

$$|\ker(\alpha)(k^{\mathrm{s}})| = |P^{\mathrm{ab}}| \text{ divides } |\overline{A}(\mathbb{F}_q)| = |\overline{\mathrm{Jac}(X_k)}(\mathbb{F}_q)|$$

The right-hand side term in the desired inequality corresponds to the upper bound, due to Lachaud and Martin-Deschamps [LMD90], for the number of rational points over $\mathbb{F}_q$ on the Jacobian of a curve C of genus g given as a cover $C \to \mathbb{P}^1$ of degree $[G : P]$ [6]. The value of g given in the statement comes from the Riemann-Hurwitz formula. □

2.4. **Torsion of abelian varieties.** A central point of the proof of theorem 2.1 is that

(*) *given a G-cover $Y \to \mathbb{P}^1$ defined over a field K with group G and r branch points, if $P \subset G$ is a non-trivial subgroup of order prime to each of the ramification indices $e_1, \dots, e_r$ of f, then a K-curve X_K of genus $g = 1 + \frac{1}{2}[G : P](r - 2 - \sum_{i=1}^{r} 1/e_i) \geqslant 1$ and a K-isogeny $\alpha : A \to \mathrm{Jac}(X_K)$ can be constructed with the property that its geometric kernel $\ker(\alpha)(K^{\mathrm{s}})$ is isomorphic to the trivial $\mathrm{Gal}(K^{\mathrm{s}}/K)$-module P^{ab}.*

This had been used in this context in special situations (see example 2.5 below) but has been developed in this generality in the first author's thesis [Cad04]. It is further investigated in [Cad07c].

If K is a number field, standard conjectures on torsion of abelian varieties, which we recall below, impose sharp bounds on $|P^{\mathrm{ab}}|$.

Torsion Conjecture. *Let A be an abelian variety of dimension $g \geqslant 1$ and defined over some number field K. Then the order of the torsion subgroup of $A(K)$ can be bounded in terms of g and K.*

There is also a p-Torsion Conjecture in which a prime p is fixed and it is the p-part of the torsion subgroup of $A(K)$ that is bounded, by a constant also depending on p. Strong variants have the dependence in K of the constant only involve the degree $[K : \mathbb{Q}]$.

The discussion above, conjoined with the fact that g can be bounded in terms of the index $[G : P]$ and r, shows the following.

[6] More specifically the bound is obtained from [LMD90] by conjoining their lemma 3 with the inequalities given in the proof of their theorem 3. In some cases, the more standard Weil's inequality $|\overline{\mathrm{Jac}(X_k)}(\mathbb{F}_q)| \leqslant (q + 1 + 2\sqrt{q})^g$ is better than this one; it can be used alternatively.

Proposition 2.4. *The Torsion Conjecture implies conjecture 2.2. The p-Torsion Conjecture implies the weaker form of conjecture 2.2 in which $P \subset G$ is a p-subgroup. Furthermore the possible dependence of the constants in K through $[K : \mathbb{Q}]$ is preserved via these implications.*

Example 2.5 (dihedral group example). Consider the group $G = D_{p^n}$ (dihedral group of order $2p^n$) with p an odd prime and $n \geqslant 1$. Theorem 2.1 immediately yields that any regular realization of D_{p^n} over a henselian field k (as in theorem 2.1) with a bounded number of branch points and with ramification indices equal to 2 necessarily has a singular branch divisor if p^n is suitably large. As for conjecture 2.2, it implies the following statement, which is still open for $r > 5$.

Dihedral Group Conjecture [DF94] [Dèb06]. *Given a number field K and an integer $r \geqslant 3$, only finitely many groups $G = D_{p^n}$ with p an odd prime and $n \geqslant 1$ can be regularly realized over K with at most r branch points (and ramification indices equal to 2)*[7].

For $r \leqslant 5$ it was proved in [DF94, §5.1]. The main case is $r = 4$. The genus g of the curve X_K from (*) above is then $g = 1$ and so the result follows from the Mazur-Merel theorem (that is, the case $g = 1$ of the Torsion Conjecture).

The dihedral group example was the starting point of the Modular Tower program. Section 3 will be devoted to the implications of our central results in this more general situation.

2.5. **Generalization of theorem 2.1.** We give here a generalization of theorem 2.1 where we let the base space of the cover f be a more general curve than $\mathbb{P}^1$, we relax the assumption that the ramification indices are prime to $|G|$ and we use recent results of Clark and Xarles [CXar] on the number of torsion points of abelian varieties over ℓ-adic fields to weaken the good reduction condition, to sometimes drop the condition $(\ell, |G|) = 1$ and to refine our bounds.

Let k be a henselian field (for a discrete valuation v) with finite residue field of characteristic $\ell > 0$ and of cardinality $q = \ell^f$. Let $e = v(\ell)$ [8] denote the ramification index of k.

[CXar] provides a bound for the number of k-rational torsion points on a g-dimensional abelian variety A with anisotropic reduction, under the additional assumption that k is of characteristic 0. We denote it

[7] The ramification condition is actually unnecessary (see proof of corollary 3.2 for a general argument or [Dèb06, 2nd case of conjecture 2.1] for a more specific one).

[8] not to be confused with e=2,718... used previously (but not here).

by $CX(\ell, e, f, g, \alpha, \mu, \beta)$: in addition to ℓ, e, f, g, it involves the respective dimensions α, μ, β of the unipotent, toric and abelian parts of the special fiber of the Neron model of A. Specifically, we have

$$CX(\ell, e, f, g, \alpha, \mu, \beta) = 2^{2\alpha}\, \ell^{f\alpha + 2g[\ln_\ell(\ell e/\ell - 1)]}\, (q+1)^\mu\, [q + 1 + 2\sqrt{q}]^\beta\, \eta(\alpha)$$

where $[x]$ denotes the largest integer $\leqslant x$ and $\eta(\alpha) = \prod_{\ell prime} \ell^{m_\ell(\alpha)}$ with $m_\ell(\alpha) = \sum_{i \geqslant 0} [2\alpha/(\ell^i(\ell-1))]$ if $\ell \neq 2$ and $m_2(\alpha) = [\alpha] + \sum_{i \geqslant 0} [\alpha/2^{i-1}]$.

Theorem 2.6. *With k as above, let G be a finite group, $f : Y \to B$ be a k-G-cover of k-curves with group G and ramification indices $e_1, \ldots, e_r$ and P be any subgroup of G.*

(a) *If the quotient curve $X := Y \bmod P$ has potentially good reduction and $\ell \not| \, |P^{\mathrm{ab}}|$, then*

$$|P^{\mathrm{ab}}| \leqslant (e_1' \cdots e_r')^{[G:P]}\, [q + 1 + 2\sqrt{q}]^g$$

where $e_i' = \gcd(e_i, |P^{\mathrm{ab}}|)$ $(i = 1, \ldots, r)$ and g is the genus of X, i.e. $g = 1 + \frac{1}{2}[G:P](r + 2g_B - 2 - \sum_{1 \leqslant i \leqslant r} 1/e_i)$ with g_B the genus of B.

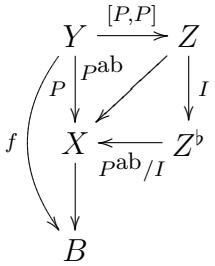
(b) *If $\mathrm{Jac}(X)$ has anisotropic reduction, k is of characteristic 0 and $\ell \not| \, |P^{\mathrm{ab}}|$, then*

$$|P^{\mathrm{ab}}| \leqslant (e_1' \cdots e_r')^{[G:P]}\, CX(\ell, e, f, g, \alpha, \mu, \beta)$$

(c) *If X has good reduction and k is of characteristic 0, then*

$$|P^{\mathrm{ab}}| \leqslant (e_1' \cdots e_r')^{[G:P]}\, \ell^{2g[\ln_\ell(\ell e/\ell - 1)]}\, [q + 1 + 2\sqrt{q}]^g$$

Proof. As in the proof of theorem 2.1, factor $f : Y \to B$ as follows:



where $I \subset P^{\mathrm{ab}}$ is the subgroup generated by all the inertia subgroups of $Z \to X$. Again the abelian etale k-G-cover $Z^\flat \to X$ induces an isogeny $\alpha : A \to \mathrm{Jac}(X)$ with kernel isomorphic to the trivial $\mathrm{Gal}(k^{\mathrm{s}}/k)$-module P^{ab}/I. In particular we have $|P^{\mathrm{ab}}| \leqslant |A(k)_{\mathrm{tors}}|\, |I|$. Here we use the uniform bounds for $|A(k)_{\mathrm{tors}}|$ given in the main theorem of [CXar] (more specifically we use their bound (1) for our statement (a) and their bound (2) for (b) and (c)). One thing to notice is that from

[BLR90, chap.VII, prop.6.6] if $\mathrm{Jac}(X)$ has (potential) good reduction then so does A and if $\mathrm{Jac}(X)$ has anisotropic reduction then so does A provided α is of prime-to-ℓ degree. It remains to bound $|I|$. For each point $P \in X(k^{\mathrm{sep}})$ above some branch point t_i of f $(i = 1, \ldots, r)$, pick a generator ω_P of some inertia group of $Z \to X$ above P, and denote its order by ν_P. Then I is generated by all these ω_P and so $|I| \leqslant \prod_P \nu_P$. Now clearly ν_P divides both e_i and $|P^{\mathrm{ab}}|$, whence the announced bound, which also holds in the case $P^{\mathrm{ab}}/I = \{1\}$. □

Remark 2.7 (on the good reduction assumption). Each of the following conditions guarantees (potentially) good reduction of the curve X in theorem 2.6; for the first two see [KM85] (corollary A7.1.2 and proposition A7.1.3 respectively).

(GR1) the curve Y has good reduction and $Y \to X$ is etale.

(GR2) the curve Y has good reduction and $\ell \nmid |P|$.

(GR3) the cover $f : X \to B$ has good reduction.

Condition (GR3) in turn can be ensured by condition (GR3)$^\sharp$ below given by Fulton's criterion [Ful69, theorem 3.3]; note that the order of the Galois group of the Galois closure of $f : X \to B$ divides both $|G|$ and $m!$ (with $m = [G : P]$)[9].

(GR3)$^\sharp$ The branch divisor of $f : Y \to B$ is smooth and $\ell \nmid (|G|, m!)$.

The following condition is even stronger and also implies (GR2) as well as the first part of (GR1); it is the assumption made in theorem 2.1.

(GR0) The branch divisor of $f : Y \to B$ is smooth and $\ell \nmid |G|$.

Also, under (GR0), the field of moduli of a G-cover with general base B is a field of definition (see [Ems99], which generalizes [DH98]). Hence theorem 2.1 is the special case of theorem 2.6 with $B = \mathbb{P}^1$ and the good reduction assumption ensured by (GR0).

2.6. **Further applications.**

2.6.1. *Removing the dependence on* $e_1, \ldots, e_r$. As in [Cad07a] the following method can be used alternatively to bound $|I|$ in the final part of the proof of theorem 2.6:
- write $|I| \leqslant \exp(I)^{2g_{Z^\flat} + r[G:P](|P^{\mathrm{ab}}|/|I|)}$ with $\exp(I)$ the exponent of I and $g_{Z^\flat}$ the genus of $Z^\flat$,
- use the Riemann-Hurwitz formula to bound $g_{Z^\flat}$ in terms of r, g_B, $[G : P]$ and $|P^{\mathrm{ab}}|/|I|$,

[9]The same remark shows that condition $\ell \nmid |G|$ can be replaced by $\ell \nmid (|G|, m!)$ in corollary 2.3.

- for each prime p, use [Cad07c, Lemma 1.1] to bound the p-part, say p^{n_p}, of $\exp(I)$: the residue field of $Z^\flat$ at each associated branch point in the cover $Z \to Z^\flat$ contains the p^{n_p}-th roots of unity. Therefore $p^{n_p} \mid \ell^{fD} - 1$ where D is the degree of that residue field over k.
- bound D by $[G : P]\,|P^{\mathrm{ab}}|/|I|$ and use the bound for $|P^{\mathrm{ab}}|/|I|$ from the first part of the proof.
This provides the following result where the bound is more complicated but no longer depends on the ramification indices $e_1, \ldots, e_r$.

Corollary 2.8. *With k, G as in theorem 2.6, k of characteristic 0, let $f : Y \to B$ be a k-G-cover of curves with group G and $P \subset G$ be any subgroup. If the quotient curve $X = Y \bmod P$ has good reduction at v, then $|P^{\mathrm{ab}}|$ can be bounded only in terms of $[G : P]$, r, q, e, and g_B.*

2.6.2. *The conjecture for $r = 3$.* The case $r \leqslant 2$ is trivial both in theorem 2.1 and in conjecture 2.2. From now on we will always assume $r \geqslant 3$. We consider here the case $r = 3$.

Corollary 2.9. *Conjecture 2.2 holds for 3 branch point covers.*

Proof. Let $f : Y \to \mathbb{P}^1$ be a G-cover as in the statement of conjecture 2.2 with at most 3 branch points. These branch points are defined over an extension K_0/K of degree $\leqslant 6$. Up to composing f with a linear fractional transformation defined over K_0, one may assume they are 0, 1 or ∞. Let $P \subset G$ be a subgroup of order prime to each of the ramification indices $e_1, \ldots, e_r$ and of index $\leqslant m_0$. Pick a prime $\ell > m_0$. Condition $(\mathrm{GR3})^\sharp$ from remark 2.7 is satisfied with $k = \mathbb{Q}_\ell K_0$. Use then theorem 2.6 to bound $|P^{\mathrm{ab}}|$ by a constant depending only on m_0 and K. □

2.6.3. *Abelian etale covers.* The special case of theorem 2.6 with $G = P$ abelian and $e_1 = \cdots = e_r = 1$ yields the following.

Corollary 2.10. *Let B be a k-curve with good reduction and k of characteristic 0. Then only finitely many abelian groups occur as the Galois group of some unramified k-G-cover of B; and the number of those groups is bounded in terms of q, e and the genus g of B. The same holds for abelian groups with prime-to-ℓ order if either $\mathrm{Jac}(X)$ has anisotropic reduction and k is of characteristic 0 or X has good reduction with k of arbitrary characteristic.*

3. Application to the Modular Tower Program

3.1. **Realization of the characteristic quotients.** Fix a prime p and assume we are given an extension

$$1 \to \widetilde{P} \to \widetilde{G} \to G_0 \to 1$$

of some finite group G_0 by a free pro-p group $\widetilde{P}$ of finite rank $\rho \geqslant 1$. For example, $\widetilde{G} \to G_0$ can be taken to be as in Fried's papers the universal p-Frattini cover of G [FJ04, §22.11]. Consider next the Frattini series $(\widetilde{P}_n)_{n\geqslant 0}$ of $\widetilde{P}$ defined by: $\widetilde{P}_0 = \widetilde{P}$ and $\widetilde{P}_n = \widetilde{P}_{n-1}^p[\widetilde{P}_{n-1}, \widetilde{P}_{n-1}]$ $(n \geqslant 1)$. The groups $\widetilde{P}_n$ are characteristic free pro-p subgroups of $\widetilde{P}$ and form a fundamental system of open neighborhoods of 1 [RZ00, Ex. 2.8.14]; in particular the quotients $G_n = \widetilde{G}/\widetilde{P}_n$ are finite and $\widetilde{G}$ is the inverse limit of the groups G_n. As a consequence of theorem 2.1, we obtain the following result, a first version of which had been given in the first author's thesis [Cad04].

Corollary 3.1. *Let $r \geqslant 0$ be an integer, k be a henselian field with finite residue field $\mathbb{F}_q$ with $(q, p|G_0|) = 1$ and n be an integer such that*

$$p^n > \mathrm{e}\,(2\sqrt{\mathrm{e}}\,\gamma)^{|G_0|-1}\, q^\gamma \quad \textit{with} \quad \gamma = 1 + |G_0|(r-2)/2$$

Then every k^{s}-G-cover $f_n : Y \to \mathbb{P}^1$ of group G_n with field of moduli k, with at most r branch points and with prime-to-p ramification indices necessarily has a singular branch divisor.

Proof. The result follows from theorem 2.1 applied to the p-subgroup $P = \widetilde{P}/\widetilde{P}_n$ of $G = \widetilde{G}/\widetilde{P}_n$. Note that $[G : P] = |G_0|$ and that $P^{\mathrm{ab}} \simeq (\mathbb{Z}/p^n\mathbb{Z})^\rho$. For the last isomorphism, just write

$$P^{\mathrm{ab}} \simeq \frac{\widetilde{P}}{\widetilde{P}_n[\widetilde{P}, \widetilde{P}]} \simeq \frac{\widetilde{P}/[\widetilde{P}, \widetilde{P}]}{\widetilde{P}_n[\widetilde{P}, \widetilde{P}]/[\widetilde{P}, \widetilde{P}]} \simeq \frac{\widetilde{P}^{\mathrm{ab}}}{(\widetilde{P}^{\mathrm{ab}})_n} \simeq (\mathbb{Z}/p^n\mathbb{Z})^\rho$$

where in the third isomorphism $(\widetilde{P}^{\mathrm{ab}})_n$ is the n-th term of the Frattini series of $\widetilde{P}^{\mathrm{ab}}$ and $(\widetilde{P}^{\mathrm{ab}})_n \simeq \widetilde{P}_n[\widetilde{P}, \widetilde{P}]/[\widetilde{P}, \widetilde{P}]$ is easily established by induction; the last isomorphism comes from $\widetilde{P}^{\mathrm{ab}} \simeq \mathbb{Z}_p^\rho$ (use the universal property of free pro-p groups). □

Assume for every $n \geqslant 0$ there is a G-cover $f_n : Y_n \to \mathbb{P}^1$ as in corollary 3.1 but with some number field as field of moduli (the same for each n, or, more generally, with a uniformly bounded degree). Corollary 3.1 yields this conclusion, which will be refined later (see corollary 3.9):

The set of primes $\ell \not| p|G_0|$ of bad reduction of the branch divisor class of f_n tends to the whole set of primes $\ell \not| p|G_0|$, that is, includes every prescribed finite set of primes $\ell \not| p|G_0|$ provided n is suitably large.

Conjecture 2.2 provides an even stronger conclusion; namely it implies the main conjecture of the Modular Tower program:

Modular Tower Realization Conjecture (Fried). *Let $r \geqslant 3$ be an integer and K be a number field. Then only finitely many groups G_n can be regularly realized over K with at most r branch points.*

More specifically we have the following.

Corollary 3.2. *This conjecture holds under conjecture 2.2, and more precisely under the variant in which $P \subset G$ is a p-subgroup (with a constant possibly depending on p).*

Proof. Consider as above the p-subgroup $P = \widetilde{P}/\widetilde{P}_n$ of $G = \widetilde{G}/\widetilde{P}_n$ and apply our conjecture 2.2 with $m_0 = |G_0|$. As $|P^{\mathrm{ab}}| \geqslant p^n$, the conclusion "$|P^{\mathrm{ab}}|$ is bounded in terms of r, $|G_0|$ and K" can only hold for finitely many integers n; the corresponding groups G_n are the only ones that can be regularly realized over K with at most r branch points and prime-to-p ramification. The result follows since it is already known that, as a consequence of the "branch cycle argument",
(Fried-Kopeliovich theorem) if infinitely many groups G_n can be regularly realized over K with at most r branch points, then it can be done with prime-to-p ramification [FK97, thm 4.4], [Dèb06, thm 2.5].[10] □

Corollary 2.9 and proposition 2.4 then yield the following.

Corollary 3.3. *The Modular Tower Realization Conjecture holds for covers with at most 3 branch points and it holds in general under the p-Torsion Conjecture.*

Remark 3.4 (dependence in K). If the constant involved in conjecture 2.2 or in the Torsion Conjecture only depends on K through its degree $[K : \mathbb{Q}]$, then this stronger conclusion for the Modular Tower Conjecture can be deduced: given an integer $d \geqslant 1$, only finitely many groups G_n can be regularly realized with at most r branch points over some number field of degree $\leqslant d$. (This requires extending the Fried-Kopeliovich theorem in the same direction. We leave the reader check that the same proof works over any field containing only finitely many roots of 1, and so in particular over the compositum of all number fields of degree $\leqslant d$, which is sufficient for our purposes).

3.2. **Modular formulation.** §3.1 can be rephrased in terms of moduli spaces. From now on, we assume the ground field is of characteristic 0.

[10] This shows in particular why the ramification condition can be removed in the statement of the Dihedral Group Conjecture.

3.2.1. *Moduli spaces.* An important discrete invariant to classify G-covers f is the *ramification type* (also called the *inertia canonical invariant*): it is the unordered r-tuple[11] $\{C_1, \dots, C_r\}$ of the conjugacy classes in the Galois group of the so-called distinguished generators of the inertia groups[12] of any geometric fiber of f.

Given a finite group G, an integer $r \geqslant 3$ and $\underline{C} = \{C_1, \dots, C_r\}$ an unordered r-tuple of conjugacy classes of G, we denote the *Hurwitz stack* of G-covers of $\mathbb{P}^1$ with r branch points, group G and ramification type $\underline{C}$ by $\mathcal{H}_r(G, \underline{C})$. We also denote the stack of r-marked projective lines by $\mathcal{U}_r$. There is a natural functor $\mathcal{H}_r(G, \underline{C}) \to \mathcal{U}_r$ sending each G-cover to $\mathbb{P}^1$ marked by its branch divisor. These stacks admit coarse moduli spaces which we denote respectively by $\mathsf{H}_r(G, \underline{C})$ (the *Hurwitz moduli space*) and U_r. The functor above induces a finite morphism $\Psi : \mathsf{H}_r(G, \underline{C}) \to \mathsf{U}_r$. For every field k of characteristic 0 k-rational points on $\mathcal{H}_r(G, \underline{C})$ (respectively, on $\mathsf{H}_r(G, \underline{C})$) correspond to k-G-covers (respectively, to $\overline{k}$-isomorphism classes of G-covers with k as field of moduli) with invariants r, $G, \underline{C}$. See [FV91], [Wew98] or [RW06] for more on Hurwitz spaces.

3.2.2. *Modular towers.* Retain the notation of §3.1. Assume in addition that the finite group G_0 is p-perfect, that is, G_0 is generated by its elements of prime-to-p order, or, equivalently, it admits no quotient isomorphic to $\mathbb{Z}/p\mathbb{Z}$[13]. Let then $r \geqslant 3$ be an integer and $\underline{C} = \{C_1, \dots, C_r\}$ be an unordered r-tuple of conjugacy classes of G_0 of prime-to-p order[14]. From the Schur-Zassenhaus lemma, each class C_i can be lifted in a unique way along the natural surjection $G_n \to G_0$ to a conjugacy class C_i^n of G_n with the same order as C_i to provide an unordered r-tuple $\underline{C}^n = \{C_1^n, \dots, C_r^n\}$ $(n \geqslant 0)$. Consider the associated Hurwitz spaces $\mathsf{H}_r(G_n, \underline{C}^n)$, which we denote for short by H^n $(n \geqslant 0)$. By functoriality, the canonical surjection $G_n \to G_{n-1}$ induces algebraic maps $\mathsf{H}^n \to \mathsf{H}^{n-1}$ $(n \geqslant 1)$. The collection $(\mathsf{H}^n)_{n \geqslant 0}$ given with these maps is the *modular tower* associated with the starting extension $\widetilde{G} \to G_0$, r and $\underline{C}$; we denote it by $\mathsf{H}(\widetilde{G} \to G_0, r, \underline{C})$. Hurwitz stacks $\mathcal{H}^n = \mathcal{H}_r(\widetilde{G}_n, \underline{C}^n)$ can be defined similarly $(n \geqslant 0)$. The collection $(\mathcal{H}^n)_{n \geqslant 0}$ with the corresponding maps $\mathcal{H}^n \to \mathcal{H}^{n-1}$ is the *stack tower* associated with $\widetilde{G} \to G_0$, r

[11] That is, an r-tuple regarded modulo the action of the symmetric group S_r.

[12] See [Dèb01, §2] for a definition of distinguished generator. The conjugacy class C_i can also be defined topologically: it is the conjugacy class of the monodromy branch cycles corresponding to single loops about the branch point t_i, $i = 1, \dots, r$.

[13] Theorem 2.1 and conjecture 2.2 with P a p-subgroup are trivial if the group G_0 is not p-perfect.

[14] By order, we mean the common order of the elements in the conjugacy class.

and $\underline{C}$; we denote it by $\mathcal{H}(\widetilde{G} \to G_0, r, \underline{C})$. For more on the construction of modular towers, which is due to Fried, we refer to [Fri95, part III]; see also [Dèb06] and [Sem06].

3.2.3. *Restatements.* Corollary 3.1 and the Modular Tower Conjecture can be rephrased as follows. Let $\widetilde{G} \to G_0$, r and $\underline{C}$ be as above.

Corollary 3.1 (reformulated). *Let k be a henselian field of characteristic 0 and with finite residue field $\mathbb{F}_q$ with $(q, p|G_0|) = 1$. Then for every integer n such that*

$$p^n > \mathrm{e}\,(2\sqrt{\mathrm{e}}\,\gamma)^{|G_0|-1}\, q^\gamma \quad \text{with} \quad \gamma = 1 + |G|(r-2)/2$$

all the k-rational points on the n-th level H^n of the modular tower $\mathsf{H}(\widetilde{G} \to G_0, r, \underline{C})$ correspond to G-covers with a singular branch divisor.

Remark 3.5. Using theorem 2.6, it is possible to drop the assumption $(q, p|G_0|) = 1$ in corollary 3.1 at the cost of a slight change in the bad reduction condition: more specifically, the conclusion becomes that all k-rational points on the n-th level H^n of the modular tower correspond to G-covers $f : Y \to \mathbb{P}^1$ such that the quotient curve $X := Y \bmod (\widetilde{P}/\widetilde{P}_n)$ does not have good reduction.

Modular Tower Diophantine Conjecture (Fried). *Let K be a number field. If n suitably large (depending on $\widetilde{G} \to G_0$, r and K),*
(for stacks) *there are no K-rational points on the n-th level $\mathcal{H}^n$ of the stack tower $\mathcal{H}(\widetilde{G} \to G_0, r, \underline{C})$.*
(for moduli spaces) *there are no K-rational points on the n-th level H^n of the modular tower $\mathsf{H}(\widetilde{G} \to G_0, r, \underline{C})$.*

The Modular Tower *Realization* Conjecture from §3.1 is equivalent to the stack version of this new *Diophantine* form (use again the Fried-Kopeliovich theorem mentioned above for the direct part).

The moduli space version is *a priori* stronger than the stack version, but is more useful in practice for moduli spaces are schemes. In the appendix to this paper, we show the two versions are actually equivalent if in addition the dependence in K of the constants involved is through $[K : \mathbb{Q}]$[15]. Consequently, the variant of conjecture 2.2 or of the Torsion Conjecture with dependence in K through $[K : \mathbb{Q}]$ implies the moduli space version of the Modular Tower Diophantine Conjecture (while the original variants are sufficient for the stack version).

[15]D. Semmen pointed out to us that the equivalence also holds, even without this strong dependence of the constants, in the case that $\widetilde{G}$ is the universal p-Frattini cover of G, that is in Fried's original context.

Remark 3.6 (relaxing the good reduction condition). Corollary 3.1 asserts there is necessarily bad reduction of the branch divisor corresponding to rational points over a henselian field k on suitably high levels of a modular tower. A natural question is whether there exist k-rational points at all on every level of a modular tower. Using Harbater's patching method over complete fields (which provides covers with bad reduction), the answer was shown to be positive under these assumptions: $\underline{C}$ is of Harbater-Mumford type (*i.e.* of the form $\underline{C} = \{C_1, C_1^{-1}, \ldots, C_s, C_s^{-1}\}$) and k contains Nth roots of 1 with N the l.c.m. of the orders of $C_1, \ldots, C_s$. It is even true then there exist projective systems of k-rational points on the modular tower $\mathsf{H}(\widetilde{G} \to G_0, r, \underline{C})$ (and even on the stack tower $\mathcal{H}(\widetilde{G} \to G_0, r, \underline{C})$) [DD04, §4].

3.3. PGL_2**-reduced variants.** Here we view G-covers $Y \to \mathbb{P}^1$ as objects of the category of k-G-covers of *some genus* 0 *curve*, with group G, ramification type $\underline{C}$ and with the following isomorphism relation: two k-G-covers $f_1 : Y_1 \to X_1$ and $f_2 : Y_2 \to X_2$ are isomorphic if there are k-curve isomorphisms $\beta : Y_1 \to Y_2$ and $\alpha : X_1 \to X_2$ such that $f_2 \circ \beta = \alpha \circ f_1$ and β is compatible with the actions of G. Let $\mathsf{H}_r^{\equiv}(G, \underline{C})$ denote the corresponding moduli space [BR06]. The morphism $\mathsf{H}_r(G, \underline{C}) \to \mathsf{H}_r^{\equiv}(G, \underline{C})$ induced by functoriality can be identified with the geometric quotient of $\mathsf{H}_r(G, \underline{C})$ by PGL_2 [CT06] and the finite morphism $\Psi : \mathsf{H}_r(G, \underline{C}) \to \mathsf{U}_r$ induces a finite morphism $\Psi^{\equiv} : \mathsf{H}_r^{\equiv}(G, \underline{C}) \to \mathsf{U}_r/\mathrm{PGL}_2$.

For $\widetilde{G} \to G_0$, r and $\underline{C}$ as in §3.2, set $\mathsf{H}^{n,\equiv} = \mathsf{H}_r^{\equiv}(G_n, \underline{C}^n)$ $(n \geqslant 0)$. The collection $(\mathsf{H}^{n,\equiv})_{n \geqslant 0}$ with the natural maps $\mathsf{H}^{n+1,\equiv} \to \mathsf{H}^{n,\equiv}$ is the PGL_2-reduced modular tower. We denote it by $\mathsf{H}(\widetilde{G} \to G_0, r, \underline{C})^{\equiv}$.

The analog of the Modular Tower Diophantine Conjecture for PGL_2-reduced modular towers is *a priori* stronger than the original one; from corollary 3.12 of [Cad07b] the two versions are actually equivalent if the dependence in K of the constants involved is through $[K : \mathbb{Q}]$.

Example 3.7. For $\widetilde{G} \to G_0$ taken to be the pro-dihedral extension $D_{p^\infty} = \mathbb{Z}_p \rtimes \mathbb{Z}/2\mathbb{Z} \to D_p$ (with p an odd prime), $r = 4$ and $\underline{C}$ consisting of 4 copies of the involution class of D_p, the PGL_2-reduced modular tower is isomorphic to the tower of modular curves $Y_1(p^{n+1})$ $(n \geqslant 0)$. A classical argument (recalled in corollary 3.9 (c) below) shows the Modular Tower Conjecture holds in this special case as a consequence of the fact that modular curves are geometrically irreducible and of genus $\geqslant 2$ for large n.

Given a field F (of characteristic 0) with a discrete valuation v, we say that a proper closed subset $D \subset \mathbb{P}^1_{\overline{F}}$ regarded modulo PGL_2

is *smooth* (or has *good reduction) at* v if some representative $\chi(D)$ with $\chi(D) \supset \{0, 1, \infty\}$ (for some linear fractional transformation χ) is smooth at v; as before we use the phrases *singular* or *bad reduction* in the opposite case. The following statement is a PGL_2-reduced variant of our weak form of the Modular Tower Conjecture (*i.e.* corollary 3.1).

Corollary 3.8. *Let* $\widetilde{G} \to G_0$, r *and* $\underline{C}$ *be as above. Let* k *be a henselian field of characteristic* 0 *and with residue field* $\mathbb{F}_q$ *with* $(q, p|G_0|) = 1$. *Then there exists a constant* $d(r)$ *depending only on* r *such that for every integer* n *satisfying*

$$p^n > \mathrm{e}\,(2\sqrt{\mathrm{e}}\,\gamma)^{|G_0|-1}\, q^{\gamma d(r)} \quad \textit{with} \quad \gamma = 1 + |G_0|(r-2)/2$$

all the k*-rational points on the* n*-th level* $\mathsf{H}^{n,\equiv}$ *of the* PGL_2*-reduced modular tower* $\mathsf{H}(\widetilde{G} \to G_0, r, \underline{C})^{\equiv}$ *correspond to classes modulo* PGL_2 *of* G*-covers of* $\mathbb{P}^1$ *with a singular branch divisor class modulo* PGL_2.

Proof. Let $h^{\equiv} \in \mathsf{H}^{n,\equiv}(k)$ with n as in the statement. From [Cad07b, corollary 3.12], there exists a constant $d(r)$ such that $h^{\equiv}$ can be lifted to some point h on the original Hurwitz space H^n that is rational, together with each of the associated branch points $t_1, \ldots, t_r$, over some extension k_0/k of degree $\leqslant d(r)$. If χ is some linear fractional transformation such that $\{0, 1, \infty\} \subset \{\chi(t_1), \ldots, \chi(t_r)\}$, then χ is defined over k_0. Thus if f is the $\overline{k}$-G-cover corresponding to h, then the G-cover $\chi \circ f$ has field of moduli k_0. It follows from corollary 3.1 that $\chi(D)$ is singular at v. □

The next result collects some implications to the Modular Tower Conjecture.

Corollary 3.9. *Let* $\widetilde{G} \to G_0$, r *and* $\underline{C}$ *be as above and* K *be a number field. Assume the* PGL_2*-reduced modular tower* $\mathsf{H}(\widetilde{G} \to G_0, r, \underline{C})^{\equiv}$ *has at least one* K*-rational point on every level* $\mathsf{H}^{n,\equiv}$. *Then this holds:*

(a) *The set of primes* $\ell \not| \, p|G_0|$ *of* $\mathbb{Q}$ *of bad reduction of the branch divisor class modulo* PGL_2 *of covers in* $\mathsf{H}^{n,\equiv}(K)$ *tends to the whole set of primes* $\ell \not| \, p|G_0|$ *when* $n \to \infty$, *uniformly in* $h \in \mathsf{H}^{n,\equiv}(K)$. *In particular, there is no projective system of* K*-rational points on the* PGL_2*-reduced modular tower.*

(b) *For every finite set* S *of primes* $\ell \not| p|G_0|$, *every level* $\mathsf{H}^{m,\equiv}$ *has* K*-rational points corresponding to covers with singular branch divisor class modulo every prime* $\ell \in S$ *(*$m \geqslant 0$*). In particular there are infinitely many* K*-rational points on every level.*

(c) *If in addition* $r = 4$, *then each level* $\mathsf{H}^{n,\equiv}$ *has an irreducible component that is a curve of genus* 0 *or* 1 *(*$n \geqslant 0$*). Furthermore, given a finite set* S *of primes* $\ell \not| p|G_0|$, *for every integer* n *such that*

$$p^n > \mathrm{e}\,(2\sqrt{\mathrm{e}}\,\gamma)^{|G_0|-1}\max(S)^{\gamma d(4)} \quad \textit{with} \quad \gamma = 1+|G_0|(r-2)/2$$

the image of the map $\Psi^{\equiv} : \mathsf{H}^{n,\equiv}(K) \to \mathbb{P}^1(K)\setminus\{0,1,\infty\}$ [16] *is contained in the subset* $\{|\lambda|_v \neq 1\}\cup\{|\lambda-1|_v<1\}$ *for every place* v *of* $\overline{K}$ *above some prime* $\ell \in S$.

Remark 3.10. The non-existence of projective systems of K-rational points on a modular tower first appeared in the Bailey-Fried paper [BF02]; the result was then refined and extended to more general situations by Kimura [Kim05] and the first author [Cad04] [Cad07c]. The case $r=4$ considered in statement (c) has been thoroughly studied by Fried [BF02], [Fri06].

Proof. (a) Let S be a finite set of primes $\ell \not| p|G_0|$. Apply corollary 3.8 with $k = K\mathbb{Q}_\ell$ and $\ell \in S$. For every integer n satisfying the inequality of the statement with $\ell = \max(S)$, we obtain that S is contained in the set of primes $\ell \not| p|G_0|$ of bad reduction of the branch divisor class modulo PGL_2 of any point in $\mathsf{H}^{n,\equiv}(K)$; such a K-rational point exists by assumption. The second part of (a) is immediate as the branch divisor class is constant in a projective system of points.

(b) Fix an integer $m \geqslant 0$ and a finite set S of primes $\ell \not| p|G_0|$. Use (a) to consider an integer $n \geqslant m$ such that all points in $\mathsf{H}^{n,\equiv}(K)$ have the property that the associated branch divisor classes modulo PGL_2 are singular modulo each prime in S. Such K-rational points induce K-rational points on $\mathsf{H}^{m,\equiv}$ with the same branch divisor, and so with the same property. This property guarantees existence of K-rational points on $\mathsf{H}^{m,\equiv}$ with a branch divisor class singular at some given prime not already in the finite list of primes of bad reduction of a given finite set of points on $\mathsf{H}^{m,\equiv}$. In particular $\mathsf{H}^{m,\equiv}(K)$ is infinite.

(c) Assume furthermore $r=4$. The reduced Hurwitz spaces $\mathsf{H}^{n,\equiv}$ are then of dimension $r-3=1$: they are curves. The first assertion then follows from Faltings' theorem [Fal83]. The rest of statement (c) follows straightforwardly from corollary 3.8 and the definition of bad reduction for some set $\{0,1,\infty,\lambda\}$. □

Remark 3.11. As for corollary 3.1, using theorem 2.6, it is possible to reformulate corollary 3.8 and corollary 3.9 without the assumptions $(q, p|G_0|) = 1$ and $\ell \not| p|G_0|$. More specifically, in statement (a) of theorem 3.9, the set of primes $\ell \not| p|G_0|$ of bad reduction of the branch divisor class modulo PGL_2 of covers $f : Y \to B \in \mathsf{H}^{n,\equiv}(K)$ can be replaced by the whole set of primes for which the quotient curve $X :=$

[16] We have identified $\mathsf{U}_4/\mathrm{PGL}_2$ with $\mathbb{P}^1\setminus\{0,1,\infty\}$.

Y mod $(\tilde{P}/\tilde{P}_n)$ does not have good reduction. The changes to be done in the other statements are similar.

Appendix

The goal is to prove the following statement.

Proposition 1. *Let $\widetilde{G}$ be an extension of a finite group G_0 by a free pro-p group $\widetilde{P}$ of finite rank $\geqslant 1$. These assertions are equivalent:*

(i) *For any integer $d \geqslant 1$, $\bigcup_{[k:\mathbb{Q}]\leqslant d} \mathcal{H}^n(k) = \emptyset$, for all suitably large n.*

(ii) *For any integer $d \geqslant 1$, $\bigcup_{[k:\mathbb{Q}]\leqslant d} \mathsf{H}^n(k) = \emptyset$, for all suitably large n.*

Proof. We prove *(i) $\Rightarrow$ (ii)*; the converse is straightforward. Recall [DD97, §3.2, §3.3] that to any G-cover $f : X \to \mathbb{P}^1_k$ can be attached a profinite group morphism $\overline{\phi}_f : \mathrm{Gal}(\overline{k}/k) \to G/Z(G)$ such that the G-cover $f : X \to \mathbb{P}^1_k$ is defined over an extension l/k if and only if the restriction of $\overline{\phi}_f$ to $\mathrm{Gal}(\overline{l}/l)$ lifts to a profinite group morphism $\phi_f : \mathrm{Gal}(\overline{l}/l) \to G$ or, equivalently, if the cohomological obstruction $[\omega_f] \in \mathrm{H}^2(k, Z(G))$ associated with the embedding problem

$$\begin{array}{ccccccccc} & & & & & & \mathrm{Gal}(\overline{k}/k) & & \\ & & & & & & \downarrow{\scriptstyle \overline{\phi}_f} & & \\ 1 & \longrightarrow & Z(G) & \longrightarrow & G & \longrightarrow & G/Z(G) & \longrightarrow & 1 \end{array}$$

lies in $\ker(\mathrm{Res}^l_k : \mathrm{H}^2(k, Z(G)) \to \mathrm{H}^2(l, Z(G)))$. We distinguish 2 cases.

1st case: $\widetilde{P} \cap Z(\widetilde{G}) \neq \{0\}$. As a free pro-$p$ group of rank $\geqslant 2$ is centerless, we have $\mathrm{rank}(\widetilde{P}) = 1$ and so $\widetilde{P} \cap Z(\widetilde{G}) = p^{n_Z}\widetilde{P}$ for some $n_Z \geqslant 0$. Let $n \geqslant n_Z$ be an integer. From $Z(G_n) \supset (\widetilde{P} \cap Z(\widetilde{G}))\widetilde{P}_n/\widetilde{P}_n$ we get $|Z(G_n)| \geqslant p^{n-n_Z}$. From above, a G-cover $f_n : X_n \to \mathbb{P}^1_k$ with group G_n and field of moduli k is automatically defined over the fixed field k_n of $\ker(\overline{\phi}_{f_n})$ in $\overline{k}$, which satisfies $[k_n : k] \leqslant [G_n : Z(G_n)] = p^{n_Z}|G_0|$. This shows that for every fixed integer $d \geqslant 1$,

$$\bigcup_{[k:\mathbb{Q}]\leqslant dp^{n_Z}|G_0|} \mathcal{H}^n(k) = \emptyset, \;\; n \geqslant n_1 \implies \bigcup_{[k:\mathbb{Q}]\leqslant d} \mathsf{H}^n(k) = \emptyset, \;\; n \geqslant \max(n_Z, n_1)$$

2nd case: $\widetilde{P} \cap Z(\widetilde{G}) = \{0\}$. Write $s_{n_2,n_1} : G_{n_2} \twoheadrightarrow G_{n_1}$ for the canonical projection ($n_2 \geqslant n_1 \geqslant 0$). It follows from the assumption,

rewritten as $\varprojlim (\widetilde{P}/\widetilde{P}_n) \cap Z(G_n) = \{0\}$, that for every $n \geqslant 0$, there exists an integer $N(n) \geqslant n$ such that $(\widetilde{P}/\widetilde{P}_N) \cap Z(G_N)$ lies in the kernel of $s_{N,n} : G_N \twoheadrightarrow G_n$ for every $N \geqslant N(n)$. We will prove that for every fixed integer $d \geqslant 1$,

$$\bigcup_{[k:\mathbb{Q}]\leqslant d|G_0|} \mathcal{H}^n(k) = \emptyset, \;\; n \geqslant n_1 \implies \bigcup_{[k:\mathbb{Q}]\leqslant d} \mathsf{H}^n(k) = \emptyset, \;\; n \geqslant n_2 = N(n_1)$$

Assume, contrary to the conclusion, that there exist a number field k with $[k : \mathbb{Q}] \leqslant d$ and a G-cover $f_{n_2} : X_{n_2} \to \mathbb{P}^1_k$ with group G_{n_2} and field of moduli k. Denote the obstruction to k being a field of definition by $[\omega_{n_2}] \in \mathrm{H}^2(k, Z(G_{n_2}))$. Consider the following commutative diagram where the rows and the first column are short exact sequences:

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & & \uparrow & & & & \\
1 & \longrightarrow & s_{n_2,0}(Z(G_{n_2})) & \longrightarrow & G_0 & \longrightarrow & G_0/s_{n_2,0}(Z(G_{n_2})) & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle s_{n_2,0}} & & \uparrow{\scriptstyle s_{n_2,0}} & & \uparrow{\scriptstyle \overline{s}_{n_2,0}} & & \\
1 & \longrightarrow & Z(G_{n_2}) & \longrightarrow & G_{n_2} & \longrightarrow & G_{n_2}/Z(G_{n_2}) & \longrightarrow & 1 \\
 & & \uparrow & & & & \uparrow{\scriptstyle \overline{\phi}_{n_2}} & & \\
 & & (\widetilde{P}/\widetilde{P}_{n_2}) \cap Z(G_{n_2}) & & & & \mathrm{Gal}(\overline{k}/k) & & \\
 & & \uparrow & & & & & & \\
 & & 1 & & & & & &
\end{array}$$

Let l be the fixed field of $\ker(\overline{s}_{n_2,0} \circ \overline{\phi}_{n_2})$ in $\overline{k}$. Then $[l : k] \leqslant |G_0|$ and the restriction $\mathrm{Res}^l_k(s_{n_2,0}([\omega_{n_2}]))$ is trivial in $\mathrm{H}^2(l, s_{n_2,0}(Z(G_{n_2})))$. But the long exact sequence in cohomology associated with the first column of the above diagram yields the following exact sequence:

$$\cdots \mathrm{H}^2(l, (\widetilde{P}/\widetilde{P}_{n_2}) \cap Z(G_{n_2})) \to \mathrm{H}^2(l, Z(G_{n_2})) \to \mathrm{H}^2(l, s_{n_2,0}(Z(G_{n_2}))) \cdots$$

So $\mathrm{Res}^l_k([\omega_{n_2}])$ actually lies in the image of $\mathrm{H}^2(l, (\widetilde{P}/\widetilde{P}_{n_2}) \cap Z(G_{n_2}))$ in $\mathrm{H}^2(l, Z(G_{n_2}))$. Now the map $\mathrm{H}^2(l, (\widetilde{P}/\widetilde{P}_{n_2}) \cap Z(G_{n_2})) \to \mathrm{H}^2(l, Z(G_{n_1}))$ is the zero morphism, from the definition of n_2. Hence the quotient $f_{n_1} : X_{n_1} \to \mathbb{P}^1_k$ of $f_{n_2} : X_{n_2} \to \mathbb{P}^1_k$ modulo $\widetilde{P}_{n_1}/\widetilde{P}_{n_2}$ is actually defined over l, which contradicts the definition of n_1. $\square$

Comments. (a) (2nd case holds in Fried's original setting). The contents of this first comment is undoubtably known to experts (see for

instance [Fri06, §2.1] referring to [Bro82, p. 97]). We give it for self-containedness.

The condition $\widetilde{P} \cap Z(\widetilde{G}) = \{0\}$ is always satisfied when $\widetilde{G}$ is the universal p-Frattini cover of a p-perfect finite group G_0. To prove this we need a few group theoretical preliminaries about universal p-Frattini covers. Recall that if G is a perfect group then its universal central extension [Rot95, §11] is a Frattini cover of G. There is a version of this for p-perfect groups.

Lemma. *Let G be a p-perfect finite group. Then G admits a universal central p-extension*

$$1 \to M(G)_p \to \widehat{G} \stackrel{\widehat{\phi}}{\to} G \to 1$$

with kernel the p-part $M(G)_p$ of the Schur-multiplier $M(G)$ of G. Furthermore, this extension is Frattini.

Proof. By [Rot95, §11, p.361-363], given any extension $1 \to K \to F \stackrel{v}{\to} G \to 1$ with F a free group of finite type, we have $M(G) \simeq K \cap [F,F]/[F,K]$ is the torsion part of the abelian group $K/[F,K]$ and there exists a normal subgroup $S \lhd F$ such that

(i) $[F,K] \subset S \subset K$.

(ii) $M(G) \simeq (K \cap [F,F])/[F,K] \simeq K/S$.

(iii) $K/[F,K] \simeq M(G) \oplus S/[F,K]$.

(iv) The induced extension $1 \to M(G) \to F/S \stackrel{\overline{v}}{\to} G \to 1$ is central with $M(G) \subset [F/S, F/S]$.

As $M(G)$ is an abelian finite group of exponent dividing $|G|$, $M(G)$ can be written as the direct product $M(G) = M(G)_p \times M(G)_{p'}$ of its p- and p'-parts. Furthermore, as the extension in (iv) is central, $M(G)_{p'}$ is normal in F/S and the extension $1 \to M(G)_p \to \widehat{G} := (F/S)/M(G)_{p'} \stackrel{\widehat{\phi}}{\to} G \to 1$ is a well-defined p-central extension. Let us check it satisfies the universal property. If $1 \to N \to E \stackrel{e}{\to} G \to 1$ is a p-central finite extension[17] then there exists a profinite group morphism $\varepsilon : F \to E$ such that $e \circ \varepsilon = v$. As the extension is central $\varepsilon([F,K]) \subset [E,N] = \{1\}$ thus we have a factorization

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K/[F,K] & \longrightarrow & F/[F,K] & \xrightarrow{\overline{v^0}} & G & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle \overline{\varepsilon^0}} & & \| & & \\
1 & \longrightarrow & N & \longrightarrow & E & \xrightarrow{e} & G & \longrightarrow & 1
\end{array}$$

[17] As usual, it is enough to check the universal property for finite extensions.

Now, N being a finite p-group and $S/[F,K]$ being torsion free we also have a factorization

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M(G)_p & \longrightarrow & (F/[F,K]/S/[F,K])/M(G)_{p'} & \overset{\overline{v}}{\simeq} & \widehat{G} & \longrightarrow & G \longrightarrow 1 \\ & & \downarrow & & \downarrow{\scriptstyle \overline{\varepsilon}} & & & & \| \\ 1 & \longrightarrow & N & \longrightarrow & E & \xrightarrow{\quad e \quad} & G & \longrightarrow & 1 \end{array}$$

whence the existence part of the universal property.

The uniqueness results from p-perfectness of G. Indeed, the containments $M(G)_p \subset Z(\widehat{G}) \cap [\widehat{G},\widehat{G}] \subset \Phi(\widehat{G})$ [Rot95, Th.5.49] (with $\Phi(\widehat{G})$ the Frattini subgroup of $\widehat{G}$) imply that $\widehat{\phi}$ is p-Frattini and this, conjoined with Schur-Zassenhauss, entails that $\widehat{G}$ is p-perfect (lift generators of G of prime-to-p order to elements of $\widehat{G}$ with the same order; from the Frattini property, these generate $\widehat{G}$). Now let $\varepsilon_i : \widehat{G} \to E$ such that $e \circ \varepsilon_i = \overline{v}$, $i = 1, 2$. As N is abelian, the map $\delta : \widehat{G} \to N$, $x \to \varepsilon_1(x)\varepsilon_2(x)^{-1}$ is a well-defined group morphism. If δ is non trivial then $\mathrm{Im}(\delta) \subset N$ admits a quotient isomorphic to $\mathbb{Z}/p\mathbb{Z}$ hence so does $\widehat{G}$: a contradiction. □

Corollary. *Let p be a prime number and let G be a p-perfect finite group. Write $\widetilde{\phi} : \widetilde{G} \twoheadrightarrow G$ for the universal p-Frattini cover of G and $\widetilde{P}$ for its kernel. Then $Z(\widetilde{G}) \cap \widetilde{P} = \{0\}$.*

Proof. If $\mathrm{rank}(\widetilde{P}) \geqslant 2$ this is straightforward since a free pro-p group of rank $\geqslant 2$ has trivial center. If $\mathrm{rank}(\widetilde{P}) = 1$ then $\widetilde{P} \simeq \mathbb{Z}_p$ so, if $Z(\widetilde{G}) \cap \widetilde{P} \neq \{0\}$ we have $Z(\widetilde{G}) \cap \widetilde{P} = p^n\widetilde{P} \subset Z(\widetilde{G})$. The above lemma provides a map $\varepsilon : \widehat{G_n} \to \widetilde{G}$ and a commutative diagram as follows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M(G)_p & \longrightarrow & \widehat{G_n} & \xrightarrow{\widehat{\phi}_n} & G_n & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \varepsilon} & & \| & & \\ 1 & \longrightarrow & p^n\widetilde{P} & \longrightarrow & \widetilde{G} & \xrightarrow{\widetilde{\phi}_n} & G_n & \longrightarrow & 1 \end{array}$$

But as $M(G)_p$ is finite and $\widetilde{P}$ is torsion-free, $M(G)_p \subset \ker(\varepsilon)$, which yields a splitting of $\widetilde{\phi}_n$ and contradicts its Frattini property. □

Comments. (b) (abelian variant). There is a variant of the modular tower theory in which the assumption that $\widetilde{P}$ is a free pro-p group is replaced by the assumption that $\widetilde{P}$ is a free abelian pro-p group. In that case, the following analog of proposition 1 remains valid (note however the extension $1 \to \widetilde{P} \to \widetilde{G} \to G_0 \to 1$ is not fixed here).

Proposition 2. *The following statements are equivalent:*

(i) *For any integer $d \geqslant 1$ and any extension $\widetilde{G}$ of a finite group G_0 by a free abelian pro-p group $\widetilde{P}$ of finite rank $\geqslant 1$, we have $\bigcup_{[k:\mathbb{Q}]\leqslant d} \mathcal{H}^n(k) = \emptyset$, for all suitably large n.*
(ii) *For any integer $d \geqslant 1$ and any extension $\widetilde{G}$ of a finite group G_0 by a free abelian pro-p group $\widetilde{P}$ of finite rank $\geqslant 1$, we have $\bigcup_{[k:\mathbb{Q}]\leqslant d} \mathsf{H}^n(k) = \emptyset$, for all suitably large n.*

Proof. To prove *(i) $\Rightarrow$ (ii)* we distinguish two cases.

$\circ$ $[\widetilde{P} : \widetilde{P} \cap Z(\widetilde{G})]$ *is finite.* Then $\widetilde{P} \cap Z(\widetilde{G}) \supset p^{n_Z}\widetilde{P}$ for some $n_Z \geqslant 0$ and one can proceed as in the 1st case of the proof of proposition 1.

$\circ$ $[\widetilde{P} : \widetilde{P} \cap Z(\widetilde{G})]$ *is infinite.* Then either $Z(\widetilde{G}) \cap \widetilde{P} = \{0\}$ and one can proceed as in the 2nd case of the proof of proposition 1 or $Z(\widetilde{G}) \cap \widetilde{P}$ is a free abelian pro-p group of rank $\leqslant \rho - 1$ (where ρ denotes the rank of $\widetilde{P}$). In this case $\widetilde{P}^1 := \widetilde{P}/(Z(\widetilde{G}) \cap \widetilde{P}) \simeq \mathbb{Z}_p^{r_1} \oplus \mathrm{Tors}(\widetilde{P}^1)$ with $r_1 \geqslant 1$ and as $\mathrm{Tors}(\widetilde{P}^1)$ is normal in $\widetilde{G}^1 := \widetilde{G}/(Z(\widetilde{G}) \cap \widetilde{P})$ one can consider the quotient $\widetilde{G}^2 := \widetilde{G}^1/\mathrm{Tors}(\widetilde{P}_1)$ of $\widetilde{G}$, which is an extension of $\mathbb{Z}_p^{r_1}$ by G_0 and has the property that $Z(\widetilde{G}) \cap \widetilde{P}$ maps to $\{0\}$ in $\widetilde{G} \twoheadrightarrow \widetilde{G}^2$.

We now use a refinement of the argument of the 2nd case of the proof of proposition 1. Namely, write $\widetilde{P}^2_n = p^n\widetilde{P}^2$ and $G^2_n = \widetilde{G}^2/\widetilde{P}^2_n$ $(n \geqslant 0)$ and $s^2_{n_2,n_1} : G^2_{n_2} \twoheadrightarrow G^2_{n_1}$ for the canonical projection $(n_2 \geqslant n_1 \geqslant 0)$; finally let $(\mathcal{H}^{2,n})_{n\geqslant 0}$ denote the corresponding stack tower. Then the quotient map $\widetilde{G} \twoheadrightarrow \widetilde{G}^2$ induces an epimorphism of projective systems

$$\begin{array}{ccc} G_{n+1} & \twoheadrightarrow & G_n \quad n \geqslant 0 \\ \downarrow{\scriptstyle \pi_{n+1}} & & \downarrow{\scriptstyle \pi_n} \\ G^2_{n+1} & \twoheadrightarrow & G^2_n \end{array}$$

such that $\varprojlim \pi_n((\widetilde{P}/\widetilde{P}_n) \cap Z(G_n)) = \{0\}$. In other words, for any $n \geqslant 0$ there exists an integer $N(n) \geqslant n$ such that $\pi_N((\widetilde{P}/\widetilde{P}_N) \cap Z(G_N))$ lies in $\ker(s^2_{N,n} : G^2_N \twoheadrightarrow G^2_n)$, $N \geqslant N(n)$. By assumption, there exists an integer $n_1 \geqslant 0$ such that $\bigcup_{[k:\mathbb{Q}]\leqslant d|G_0|} \mathcal{H}^{2,n}(k) = \emptyset$ $(n \geqslant n_1)$. Setting again $n_2 = N(n_1)$ one can show, using the method of the proof of proposition 1 that $\bigcup_{[k:\mathbb{Q}]\leqslant d} \mathrm{H}^n(k) = \emptyset$, $n \geqslant n_2$. $\square$

References

[BF02] Paul Bailey and Michael D. Fried. Hurwitz monodromy, spin separation and higher levels of a modular tower. In *Arithmetic fundamental groups and noncommutative algebra (Berkeley, 1999)*, volume 70 of *Proc. Sympos. Pure Math.*, pages 79–220. Amer. Math. Soc., Providence, RI, 2002.

[BLR90] S. Bosch, W. Lutkebohmert, and M. Raynaud. *Neron models*, volume 21 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, 1990.

[BR06] José Bertin and Matthieu Romagny. Champs de Hurwitz. *preprint*, 2006.

[Bro82] Kenneth S. Brown. *Cohomology of groups*, volume 87 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[Cad04] Anna Cadoret. *Théorie de Galois inverse et arithmétique des espaces de Hurwitz*. Thèse de doctorat, Université Lille 1, 2004.

[Cad07a] Anna Cadoret. A boundedness result for G-covers of curves. *preprint*, 2007.

[Cad07b] Anna Cadoret. Lifting results for rational points on Hurwitz moduli spaces. *Isr. J. Math.*, to appear, 2007.

[Cad07c] Anna Cadoret. On the profinite regular inverse galois problem. *preprint*, 2007.

[CT06] Anna Cadoret and Akio Tamagawa. Stratification of Hurwitz spaces by closed modular subvarieties. *preprint*, 2006.

[CXar] Pete L. Clark and Xavier Xarles. Local bounds for torsion points of abelian varieties. *Canadian J. Math*, (to appear).

[DD97] Pierre Dèbes and Jean-Claude Douai. Algebraic covers: field of moduli versus field of definition. *Annales Sci. E.N.S.*, 30:303–338, 1997.

[DD04] Pierre Dèbes and Bruno Deschamps. Corps ψ-libres et théorie inverse de Galois infinie. *J. Reine Angew. Math.*, 574:197–218, 2004.

[Dèb01] Pierre Dèbes. Théorème d'existence de Riemann. In *Arithmétique des revêtements algébriques*, volume 5 of *Séminaires et Congrès*, pages 27–41. SMF, 2001.

[Dèb06] Pierre Dèbes. An introduction to the modular tower program. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Séminaires et Congrès*, pages 127–144. SMF, 2006.

[DF94] Pierre Dèbes and Michael D. Fried. Nonrigid constructions in Galois theory. *Pacific J. Math.*, 163(1):81–122, 1994.

[DH98] Pierre Dèbes and David Harbater. Fields of definition of p-adic covers. *J. Reine Angew. Math.*, 498:223–236, 1998.

[Ems99] Michel Emsalem. On reduction of covers of arithmetic surfaces. In *Applications of Curves over Finite Fields*, volume 245 of *Contemp. Math.*, pages 117–132. Amer. Math. Soc., Providence, RI, 1999.

[Fal83] Gerd Faltings. Endlichkeitssätzes für abelesche varietäten über zhalenkörpen. *Invent. Math.*, 73:349–366, 1983.

[FJ04] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, Berlin, 2004. (first edition 1986).

[FK97] Michael D. Fried and Yaacov Kopeliovich. Applying modular towers to the inverse Galois problem. In *Geometric Galois actions, 2*, volume 243

of *London Math. Soc. Lecture Note Ser.*, pages 151–175. Cambridge Univ. Press, Cambridge, 1997.

[Fri95] Michael D. Fried. Introduction to modular towers: generalizing dihedral group–modular curve connections. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 111–171. Amer. Math. Soc., Providence, RI, 1995.

[Fri06] Michael D. Fried. The main conjecture of modular towers and its higher rank generalization. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Séminaires et Congrès*, pages 165–233. SMF, 2006.

[Ful69] William Fulton. Hurwitz schemes and irreducibility of moduli of algebraic curves. *Ann. of Math.*, 90:542–575, 1969.

[FV91] Michael D. Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.*, 290(4):771–800, 1991.

[Kim05] Kinya Kimura. *Modular towers for finite groups that may not be center-free*. Master Thesis, RIMS, 2005.

[KM85] Nicholas M. Katz and Barry Mazur. Arithmetic moduli of elliptic curves. *Annals of Math. Studies*, 1985.

[LMD90] Gilles Lachaud and Mireille Martin-Deschamps. Nombre de points des jacobiennes sur un corps fini. *Acta Arith.*, 56:329–340, 1990.

[Mil86] James S. Milne. Jacobian varieties. In *Arithmetic Geometry*, pages 167–212. Springer-Verlag, New York, 1986.

[Rot95] Joseph Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[RW06] Matthieu Romagny and Stefan Wewers. Hurwitz spaces. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Séminaires et Congrès*, pages 313–341. SMF, 2006.

[RZ00] Luis Ribes and Pavel Zalesskii. *Profinite Groups*, volume 40 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer-Verlag, 2000.

[Sem06] Darren Semmen. The group theory behind modular towers. In *Groupes de Galois arithmétiques et différentiels*, volume 13 of *Séminaires et Congrès*, pages 343–366. SMF, 2006.

[Ser59] Jean-Pierre Serre. *Groupes algébriques et corps de classes*. Hermann, Paris, 1959.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[Völ96] Helmut Völklein. *Groups as Galois Groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 1996.

[Wew98] Stefan Wewers. *Construction of Hurwitz spaces*. PhD Thesis, Essen, 1998.

E-mail address: Anna.Cadoret@math.u-bordeaux1.fr

Laboratoire A2X, Université Bordeaux 1 351, cours de la Libération, 33405 Talence cedex, France

E-mail address: Pierre.Debes@math.univ-lille1.fr

Laboratoire Paul Painlevé, Mathématiques, Université Lille 1, 59655 Villeneuve d'Ascq Cedex, France