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 provides a new viewpoint on Fried's Modular Tower program and a weak form of its main conjecture.

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. Assume first for simplicity that the ramification indices are relatively 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}. Theorem 2.1 uses known estimates for the number of rational torsion points on a Jacobian variety over finite fields and over ℓ-adic fields. 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

Date: October 24, 2008.

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.

conjectural bound, which only depends on r and m: conjecture 2.2 relies on standard conjectures on the torsion of abelian varieties.

These bounds for the order p^n of P^{ab} can be regarded as new constraints in inverse Galois theory: from theorem 2.1, 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 be bounded in terms of r and m. Dihedral groups D_{p^n} are typical examples: if r is bounded, possible realizations $Y \to \mathbb{P}^1_{\mathbb{Q}}$ 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. 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 theorem 2.1, 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. 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 §2.4. In §2.5 we discuss the connection with the torsion of abelian varieties. Section 3 is devoted to the Modular Tower program. After recalling the construction of modular towers in §3.1, the Modular Tower conjecture is stated in §3.1.4 and, in §3.2, weak forms of it are deduced from theorem 2.1 (corollaries 3.5 and 3.7).

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 $\mathrm{Gal}(k^{\mathrm{s}}/k)$.

A k-curve X is a smooth projective and geometrically connected k-scheme of dimension 1; we denote by g_X its genus.

Given a finite group G, a k-G-curve with group G is a k-curve X together with a fixed embedding of G into its automorphism group[1]. An

[1]We always omit this embedding in our notation though it is part of the data. Similarly, for G-covers below, we always omit the isomorphism beween G and the automorphism group of the cover.

isomorphism of k-G-curves X and Y with the same group G is an isomorphism $\chi : X \tilde{\to} Y$ of k-curves compatible with the given embeddings of G in the automorphism group of X and Y respectively.

Suppose given, in addition, a k-curve B. 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. An isomorphism between two k-G-covers $f : X \to B$ and $g : Y \to B$ is an isomorphism $\chi : X \tilde{\to} Y$ of k-curves such that $g \circ \chi = f$ and which is compatible with the actions of G.

Suppose a discrete valuation v is given on k with valuation ring R. Then a divisor $D \subset B$ is said to have good reduction at v if there is a model B_R of B over R with good reduction such that the Zariski closure D_R of D in B_R is finite etale over R.

2.1. **Central statements.** We consider a more general situation than in the introduction: the base space is any k-curve (and not just the projective line $\mathbb{P}^1$), P is any subgroup of G (and not just a p-Sylow subgroup) and the ramification is not necessarily prime to $|P|$. We denote the abelianization of P by P^{ab}.

By *local field* we mean a complete valued field for a discrete valuation v with finite residue field. We fix a subfield k of some local field, given with the valuation v; we say a *sub-local field*. We let $\ell > 0$ be the characteristic of the residue field, $q = \ell^f$ be its cardinality and $e = v(\ell)$ be its absolute ramification index. When k has characteristic 0, k is a subfield of some finite extension of $\mathbb{Q}_\ell$; we say a sub-ℓ-adic field.

Theorem 2.1. *Let B be a k-curve, G be a finite group, $f : Y \to B$ be a k-G-cover of curves with group G and ramification indices $e_1, \dots, e_r$ and P be any subgroup of G of index m. Assume that:*

(GR) *The branch divisor of $f : Y \to B$ has good reduction and $\ell \nmid (|G|, m!)$.*

Then we have the following:

(a) *If k is of characteristic 0 or if $\ell \nmid |P^{\mathrm{ab}}|$, there exists a constant C depending only on m, r, q, e and g_B (but not on the ramification indices $e_1, \dots, e_r$) such that P^{ab} is of order $\leqslant C$.*

(b) *If k is of arbitrary characteristic and $\ell \nmid |P^{\mathrm{ab}}|$, then*

$$|P^{\mathrm{ab}}| \leqslant (e'_1 \cdots e'_r)^m \, (1 + \sqrt{q})^{2g}$$

where $e'_i = \gcd(e_i, |P^{\mathrm{ab}}|)$ and $g = 1 + \frac{m}{2}(r + 2g_B - 2 - \sum_{i=1}^{r} 1/e_i)$.

Theorem 2.1 is proved in §2.3.

Assume G has a regular realization over some number field K, *i.e.* there exists a K-G-cover $f : Y \to \mathbb{P}^1$ with group G. For any valuation v of K, e and f can be bounded by $d = [K : \mathbb{Q}]$. If P is a subgroup of G, then from theorem 2.1, $|P^{\mathrm{ab}}|$ can be bounded in terms of K, $[G : P]$, r and the smallest prime $\ell \not| \, |G|$ of good reduction of the branch divisor[2]. We conjecture the last dependence is unnecessary.

Conjecture 2.2. *Let $m \geqslant 1$ and $r \geqslant 0$ be two integers. Let G be the Galois group of some K-G-cover $f : Y \to \mathbb{P}^1$ with at most r branch points. If P is any subgroup of G of index m, then the order of its abelianization P^{ab} can be bounded by a constant depending only on r, m 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.

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 show below that the case $r = 3$ of conjecture 2.2 follows from theorem 2.1.

Corollary 2.3. *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 index m. Pick a prime $\ell > m$ and a place v of K_0 above ℓ. Condition (GR) is satisfied. Use theorem 2.1 (a) to bound $|P^{\mathrm{ab}}|$ by a constant depending only on m, r and K. □

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 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. Conjecture 2.2 predicts that p^n should be bounded in terms of r, $m = [G : P]$ and K. Theorem 2.1 implies the following:

[2]Here the integral model of $\mathbb{P}^1$ is implicitly taken to be $\mathbb{P}^1_R$. Good reduction of the branch divisor at the prime ℓ means that, for any place v above ℓ, no two geometric branch points $a, a' \in \overline{K} \cup \{\infty\}$ *coalesce at* v (that is, a, a' do not satisfy ($|a|_{\bar{v}} \leqslant 1$, $|a'|_{\bar{v}} \leqslant 1$ and $|a - a'|_{\bar{v}} < 1$) or ($|a|_{\bar{v}} \geqslant 1$, $|a'|_{\bar{v}} \geqslant 1$ and $|a^{-1} - a'^{-1}|_{\bar{v}} < 1$), where $\bar{v}$ is any extension to $\overline{K}$ of v).

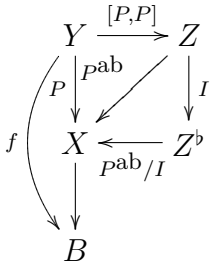
(*) *there exists a constant* $C(\ell, m, r, d)$ *such that the branch divisor of* f *has bad reduction at every prime* $\ell \nmid m$ *such that* $C(\ell, m, r, d) < p^n$. *If in addition the ramification indices* $e_1, \ldots, e_r$ *are prime-to-*p *and* $\ell \nmid |G|$ *then one can take* $C(\ell, m, r, d) = (\ell^{\frac{d}{2}} + 1)^{2g}$ *with* $g = 1 + \frac{m(r-2)}{2}$.

For instance, if $|G| = 3p^N$ ($N \geqslant 2$), then every 4-branch-point regular realization of G over $\mathbb{Q}$ with prime-to-p ramification necessarily has a branch point divisor with bad reduction at 2 if $p \geqslant 37$. The same holds without the prime-to-p ramification restriction if 37 is replaced by some suitably large constant.

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]). Theorem 2.1 points out a new constraint on the reduction of the branch divisor.

2.3. **Proof of theorem 2.1.** We may and will assume that the field k itself is a local field.

The k-G-cover $f : Y \to B$ factors as shown on the diagram



where for example $Y \xrightarrow{P} X$ means the k-G-Galois cover obtained by modding out the curve Y by the subgroup $P \subset \mathrm{Aut}_k(Y)$. We have also introduced the subgroup $I \subset P^{\mathrm{ab}}$ generated by all the inertia subgroups of $Z \to X$.

The k-G-cover $Z^\flat \to X$ is an abelian etale cover with group P^{ab}/I. Assume $P^{\mathrm{ab}} \neq I$, so in particular X is of genus $g_X \geqslant 1$. Denoting the jacobian variety of X by $\mathrm{Jac}(X)$, the cover $Z^\flat \to X$ induces a k-isogeny $\alpha : A \to \mathrm{Jac}(X)$ 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}/I [Cad08b, lemma

2.4 & remark 2.5][3]; in particular, $\ker(\alpha)(k^{\mathrm{s}})$ is contained both in the $|P^{\mathrm{ab}}/I|$-torsion part of A and in $A(k)$.

Furthermore, from [Ful69, theorem 3.3], assumption (GR) guarantees that the cover $X \to B$ has good reduction (note that the order of the Galois group of the Galois closure of $f : X \to B$ divides both $|G|$ and $m!$). Consequently so do the curve X and its Jacobian $\mathrm{Jac}(X)$ [Mil86, corollary 12.3].

2.3.1. *Proof of* (b). As we assume $\ell \not| |P^{\mathrm{ab}}|$, the isogeny α reduces modulo v to an isogeny $\overline{\alpha} : \overline{A} \to \overline{\mathrm{Jac}(X)}$ [BLR90, proposition 7.3.6]; in particular, $|\overline{A}(\mathbb{F}_q)| = |\overline{\mathrm{Jac}(X)}(\mathbb{F}_q)|$ [Tat66]. Furthermore reduction modulo v is injective on the $|P^{\mathrm{ab}}/I|$-torsion part of A [BLR90, lemma 7.3.2] and so also on $\ker(\alpha)(k^{\mathrm{s}}) \subset A(k)$. Whence

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

The term $(1+\sqrt{q})^{2g}$ in the desired inequality corresponds to the standard upper bound in Weil's inequality for the number of $\mathbb{F}_q$-rational points on an abelian variety of dimension g over $\mathbb{F}_q$. The value of g given in the statement comes from the Riemann-Hurwitz formula.

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 inequality $|I| \leqslant (e'_1 \cdots e'_r)^m$ which yields the announced result (both in the cases $P^{\mathrm{ab}} \neq I$ and $P^{\mathrm{ab}} = I$).

2.3.2. *Proof of* (a). When k has characteristic 0, we use the uniform bound (2) for $|A(k)_{\mathrm{tors}}|$ given in the main theorem of [CX08] when A has good reduction (note that A has good reduction since it is isogenous to $\mathrm{Jac}(X)$ [BLR90, chap.VII, prop.6.6]):

$$|P^{\mathrm{ab}}/I| \leqslant |A(k)_{\mathrm{tors}}| \leqslant (\ell e/(\ell-1))^{2g}\,(1+\sqrt{q})^{2g}$$

If k is of positive characteristic, then by assumption $\ell \not| |P^{\mathrm{ab}}|$ and the bound for $|P^{\mathrm{ab}}/I|$ obtained in §2.3.1 is available.

In order to bound $|I|$, we use here the following method that leads to some bound independent of the indices $e_1, \ldots, e_r$ (and also works in the case $P^{\mathrm{ab}} = I$).

The group I is a quotient of the fundamental group of the curve $Z^\flat$ with all points above the branch points of f removed. Consequently

[3]This is classical when k is algebraically closed [Ser59, Chap.6, §2.12] [Mil86, Prop.9.1]. The paper [Cad08b] extends this result to arbitrary fields.

it can be generated by less than $\nu = 2g_{Z^\flat} + rm(|P^{\mathrm{ab}}|/|I|)$ elements (recall, when k has positive characteristic, that $\ell \not| \ |P^{\mathrm{ab}}|$) and so we have $|I| \leqslant \exp(I)^\nu$ where $\exp(I)$ is the exponent of I and $g_{Z^\flat}$ is the genus of $Z^\flat$. Use the Riemann-Hurwitz formula to bound $g_{Z^\flat}$ in terms of m, r, g_B and $|P^{\mathrm{ab}}|/|I|$.

For each prime p, use [Cad08b, Lemma 2.1] 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. It follows that for $p \neq \ell$, we have $p^{n_p} \,|\, q^D - 1$ where D is the degree of that residue field over k. For $p = \ell$, then k is an ℓ-adic field and only a bounded number of ℓ^n-roots of 1 can be in some extension of k of degree $\leqslant D$. Specifically we have $\ell^{n_\ell} - \ell^{n_\ell - 1} \leqslant efD$, whence $\ell^{n_\ell} \leqslant 2eqD$.

Bound D by $m|P^{\mathrm{ab}}|/|I|$ to conclude that $|I|$ can be bounded in terms of m, r, q, e, g_B and $|P^{\mathrm{ab}}|/|I|$. Finally use the bound for $|P^{\mathrm{ab}}|/|I|$ previously obtained (or bound it by 1 in the case $P^{\mathrm{ab}} = I$). □

Remark 2.4. The argument given above to bound $|I|$ is independent of the assumption (GR). If k is a number field, it can be used for any finite place of k.

2.4. **On the good reduction hypothesis (GR).** As the proof shows, hypothesis (GR) can be more generally replaced in theorem 2.1 by

(GR-) *The quotient curve X of Y modulo P has good reduction.*

(which is also implied by the condition that Y itself has good reduction [Ray90]). In the special case $G = P$ is abelian and $e_1 = \cdots = e_r = 1$, theorem 2.1 with assumption (GR-) yields the following.

Corollary 2.5. *Let k be a sub-local field and B be a k-curve with good reduction. If k is 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 k is of arbitrary characteristic.*

When X has bad reduction, our method fails because the torsion part of $\mathrm{Jac}(X)(k)$ cannot be estimated efficiently. More specifically the following may occur (and does occur, see remark 3.6). Let j^0 denote the neutral component of the special fiber j of the Néron model of $\mathrm{Jac}(X)$. Then $j^0(\mathbb{F}_q)$ can be bounded uniformly in terms of g_X, q and e since it is an extension of an abelian variety by the product of a torus and a unipotent group. If the torus does not contains $\mathbb{G}_m$, then $j/j^0(\mathbb{F}_q)$ can also be bounded uniformly in terms of g_X, q and e but when the torus contains $\mathbb{G}_m$, then $j/j^0(\mathbb{F}_q)$ can be arbitrarily large. So,

as the reduction of a torsion point of $\mathrm{Jac}(X)(k)$ of order p^n can fall in j/j^{04}, there is no hope to get a uniform constraint on p^n.

2.5. **Torsion of abelian varieties.** The following statement can be drawn from the proof of theorem 2.1.

(*) *Given a G-cover $Y \to B$ over a sub-ℓ-adic field k with group G and r branch points, if $P \subset G$ is a subgroup of index m, there exist a k-curve X_k of genus $g_X \leqslant 1 + \frac{m(r-2)}{2}$ and a subgroup $I \subset P^{\mathrm{ab}}$ of order bounded in terms of m, r, q, e, g_B and $|P^{\mathrm{ab}}/I|$ such that:*
- either $g_X = 0$ and then $P^{\mathrm{ab}} = I$ has order bounded only in terms of m, r, q, e and g_B,
- or $g_X \geqslant 1$ and a k-isogeny $\alpha : A \to \mathrm{Jac}(X_k)$ can be constructed such that its geometric kernel $\ker(\alpha)(\overline{k})$ is isomorphic to the trivial $\mathrm{Gal}(\overline{k}/k)$-module P^{ab}/I.

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

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 $[K : \mathbb{Q}]$.

It directly follows from (*), conjoined with remark 2.4, that 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 2.6 (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 yields that any regular realization of D_{p^n} over a sub-local field k with a bounded number of branch points necessarily has a branch divisor with bad reduction if p^n is suitably large. As for conjecture 2.2, it implies the following conjecture, still open for $r > 5$.

Dihedral Group Conjecture [DF94] [Dèb06]. *Given a number field K and an integer $r \geqslant 0$, only finitely many groups D_{p^n} with p an odd*

[4]Note that this reduction still has order p^n since the p-primary torsion of the Néron model of $\mathrm{Jac}(X)$ is etale over the valuation ring R.

prime and $n \geqslant 1$ can be regularly realized over K with at most r branch points.

For $r \leqslant 5$ it was proved in [DF94, §5.1]. The main case is $r = 4$. The genus g_X of the curve X_K from (*) above is then $g_X = 1$ 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 which we will now consider.

3. Application to the Modular Tower Program

In this section, we will use theorem 2.1 in the following special situation: the base space of the covers is $B = \mathbb{P}^1$ and (GR) is replaced by the stronger hypothesis

(GR+) *The branch divisor of f has good reduction and $\ell \not| |G|$.*

Recall (GR+) also guarantees that, over local fields, the field of moduli of a G-cover $f : Y \to \mathbb{P}^1$ of group G is a field of definition [DH98].

Specifically, we will use the following special case of theorem 2.1.

Corollary 3.1. *Let G be a finite group, k be a sub-local field and $f : Y \to \mathbb{P}^1$ be a k^s-G-cover of group G and field of moduli k. Assume condition* (GR+) *above holds. If P is any subgroup of G of order prime to each of the ramification indices $e_1, \dots, e_r$ of f and with index $m = [G : P]$, then we have $|P^{\mathrm{ab}}| \leqslant (1 + \sqrt{q})^{2g}$ where $g = 1 + \frac{m(r-2)}{2}$.*

3.1. **Modular towers.** Assume the ground field has characteristic 0.

3.1.1. *Hurwitz spaces.* An important discrete invariant to classify G-covers is the *ramification type*: it is the unordered r-tuple[5] $\{C_1, \dots, C_r\}$ of the conjugacy classes in the Galois group of the so-called distinguished generators of the inertia groups [Dèb01, §2].

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 stack of G-covers of $\mathbb{P}^1$ with group G and ramification type $\underline{C}$ by $\mathcal{H}_r(G, \underline{C})$. Similarly, we denote the stack of G-curves with group G such that the resulting G-cover has ramification type $\underline{C}$ by $\mathcal{H}_r^{\equiv}(G, \underline{C})$. We also denote the stack of r-marked projective lines by $\mathcal{U}_r$ and the stack of genus 0 curves with a degree r etale divisor by $\mathcal{M}_{0,[r]}$. These stacks admit coarse moduli schemes, that we denote by $\mathsf{H}_r(G, \underline{C})$, $\mathsf{H}_r^{\equiv}(G, \underline{C})$, U_r and $\mathsf{M}_{0,[r]}$ respectively. The natural commutative diagram of stacks:

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

$$\begin{array}{ccc} \mathcal{H}_r(G,\underline{C}) & \longrightarrow & \mathcal{H}_r^{\equiv}(G,\underline{C}) \\ \downarrow & & \downarrow \\ \mathcal{U}_r & \longrightarrow & \mathcal{M}_{0,[r]} \end{array}$$

induces a similar commutative diagram at the level of coarse moduli schemes, in which the horizontal arrows can be identified with the geometric quotient modulo PGL_2 [CT08a].

Recall that, in our situation, for every field k of characteristic 0, k-rational points on stacks correspond to objects defined over k whereas k-rational points on coarse moduli schemes corresponds to $\overline{k}$-isomorphisms classes of objects defined over $\overline{k}$ and with field of moduli k.

These stacks and coarse moduli schemes are generically called *Hurwitz stacks* and *Hurwitz spaces*. See [Wew98] or [BR06] for more on Hurwitz spaces.

3.1.2. *Characteristic quotients.* Fix a finite group G_0 and a prime divisor p of $|G_0|$ and consider the universal p-Frattini cover $\widetilde{G}$ of G_0 [FJ04, §22.11]. The profinite group $\widetilde{G}$ is an extension

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

of the finite group G_0 by a free pro-p group $\widetilde{P}$ of finite rank $\rho \geqslant 1$[6]. 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], the quotients $G_n = \widetilde{G}/\widetilde{P}_n$ are finite and $\widetilde{G}$ is the inverse limit of the groups G_n.

3.1.3. *Modular towers.* Retain the notation of §3.1.2. 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 $\mathbb{Z}/p\mathbb{Z}$ [7]. Let then $r \geqslant 3$ be an integer and $\underline{C} = \{C_1, \ldots, C_r\}$ be an unordered r-tuple of conjugacy classes of G_0 of prime-to-p order[8]. 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 $\underline{C}^n = \{C_1^n, \ldots, C_r^n\}$ $(n \geqslant 0)$.

[6]This more general context is in fact sufficient for our main results: corollaries 3.3, 3.5 and 3.7 and their proof, hold under this more general condition on $\widetilde{G}$.

[7]Corollary 3.1 and conjecture 2.2 with P a p-subgroup are trivial if G_0 is not p-perfect: there are no cover of group G_0 with prime-to-p ramification in this case.

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

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 G_0, p, r and $\underline{C}$; we denote it by $\mathsf{H}_r(G_0, p, \underline{C})$.

Similarly 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 $\mathsf{H}_r(G_0, p, \underline{C})^{\equiv}$.

For more on the construction of modular towers, which is due to Fried, see [Fri95, part III] or [Dèb06].

3.1.4. The following statement is the main conjecture of the Modular Tower program.

Modular Tower Conjecture (Fried) *Let K be a number field. If n is suitably large (depending on G_0, r and K), there are no K-rational points on the n-th level $\mathsf{H}^{n,\equiv}$ of the* PGL_2*-reduced modular tower $\mathsf{H}_r(G_0, r, \underline{C})^{\equiv}$.*

There are several versions of the conjecture depending on whether it is stated for reduced moduli spaces (like here) or for the original moduli spaces H^n or for the corresponding stacks. The reduced version stated above is *a priori* the strongest version. But all these variants can actually be shown to be equivalent if the dependence in K of the constants involved is through $[K : \mathbb{Q}]$ [Kim05], [Cad08a, corollary 3.12].

Example 3.2. For $G_0 = D_p$ the dihedral group (p an odd prime), the PGL_2-reduced modular tower is isomorphic to the tower of modular curves $Y_1(p^{n+1})$ ($n \geqslant 0$). Since the $Y_1(p^n)$ are geometrically irreducible and of genus $\geqslant 2$ ($n \geqslant 0$), the Mordell conjecture [Fal83] shows the Modular Tower Conjecture holds in this special case.

3.2. **Weak form of the Modular Tower Conjecture.** Let G_0, p, r and $\underline{C}$ be as above.

3.2.1. *First version.* As a consequence of corollary 3.1, we obtain the following result, which is a first version of our *weak form of the Modular Tower conjecture* and which in some form appeared first in [Cad04].

Corollary 3.3. *Let $r \geqslant 0$ be an integer, k be a sub-local field with residue field $\mathbb{F}_q$ such that $(q, p|G_0|) = 1$ and n be an integer such that*

$$p^n > (1 + \sqrt{q})^{2g} \quad \textit{with} \quad g = 1 + \frac{|G_0|(r-2)}{2}$$

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 branch divisor with bad reduction.

Proof. The result follows from corollary 3.1 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). □

Using conjecture 2.2 instead of corollary 3.1 in the proof above leads to the following. The conjectures involved are considered in their variant for which the dependence in K of the constants is through $[K : \mathbb{Q}]$.

Corollary 3.4. *The Modular Tower Conjecture holds under conjecture 2.2, and more precisely under the variant in which $P \subset G$ is a p-subgroup. Consequently it holds under the p-Torsion Conjecture.*

3.2.2. *Reduced version.* Given a discrete valuation v on a field k (of characteristic 0) with valuation ring R, we say that a divisor $D \subset \mathbb{P}^1_{\overline{k}}$ has *good reduction modulo* PGL_2 if some representative $\chi(D)$ with $\chi(D) \supset \{0, 1, \infty\}$ (for some linear fractional transformation χ) has good reduction at v in the sense that $\chi(D)$ is defined over k and its Zariski closure $\chi(D)_R$ in $\mathbb{P}^1_R$ is finite etale over R.

Corollary 3.5. *Let G_0, p, r and $\underline{C}$ be as above. Let k be a sub-local field of characteristic 0 and of 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*

$$p^n > (1 + q^{d(r)/2})^{2g} \quad \textit{with} \quad g = 1 + \frac{|G_0|(r-2)}{2}$$

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

Proof. Let $h^{\equiv} \in \mathsf{H}^{n,\equiv}(k)$ with n as in the statement. From [Cad08a, 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 3.3 that $\chi(D)$ has bad reduction at v. □

Remark 3.6 (the good reduction condition). Corollary 3.5 asserts there is necessarily bad reduction of the branch divisor corresponding to rational points over a local 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), it was shown that if $\underline{C}$ is of the form $\underline{C} = \{C_1, C_1^{-1}, \dots, C_s, C_s^{-1}\}$ and k contains Nth roots of 1 with N the l.c.m. of the orders of $C_1, \dots, C_s$ then there exist projective systems of k-rational points on the stack tower $\mathcal{H}_r(G_0, p, \underline{C})$ [DD04, §4]. This shows in particular that the good reduction hypothesis (GR) cannot be removed in theorem 2.1.

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

Corollary 3.7. *Let G_0, p, r and $\underline{C}$ be as above and K be a number field. Assume the* PGL_2*-reduced modular tower $\mathsf{H}_r(G_0, r, \underline{C})^{\equiv}$ 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*

$$p^n > (1 + \max(S)^{gd(4)/2})^{2g} \text{with} \quad g = 1 + |G_0|(r-2)/2$$

the image of the map $\Psi^{\equiv} : \mathsf{H}^{n,\equiv}(K) \to \mathbb{P}^1(K) \setminus \{0, 1, \infty\}$ [9] *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 3.8. The non-existence of projective systems of K-rational points on a modular tower first appeared in [BF02]; the result was then refined and extended to more general situations in [Kim05], [Cad04] and [Cad08b]. The case $r = 4$ has been thoroughly studied by Fried [BF02],

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

[Fri06]. A proof of the Modular Tower Conjecture in this case has recently been given by the first author and Tamagawa [CT08c]. They deduce it from a proof of the p-Torsion conjecture for special fibers of abelian schemes over K-curves. In [CT08b], they extend their result to prove the strong variant of the p-Torsion conjecture (where the bound depends only on $[K:\mathbb{Q}]$) for special fibers of abelian schemes over K-curves. This implies in particular that the corresponding strong variant of the 1-dimensional Modular Tower conjecture also holds.

Proof. (a) Let S be a finite set of primes $\ell \not| p|G_0|$. Apply corollary 3.5 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 3.5 and the definition of bad reduction for some set $\{0, 1, \infty, \lambda\}$. □

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.

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

[Cad08a] Anna Cadoret. Lifting results for rational points on Hurwitz moduli spaces. *Isr. J. Math.*, 164, 2008.

[Cad08b] Anna Cadoret. On the profinite regular inverse Galois problem. *Publ. R.I.M.S.*, 44, 2008.

[CT08a] Anna Cadoret and Akio Tamagawa. Stratification of Hurwitz spaces by closed modular subvarieties. *Pure and Applied Mathematics Quarterly (to appear)*, 2008.

[CT08b] Anna Cadoret and Akio Tamagawa. Strong uniform boundedness results for abelian schemes. *preprint*, 2008.

[CT08c] Anna Cadoret and Akio Tamagawa. Uniform boundedness of p-primary torsion on abelian schemes. *preprint*, 2008.

[CX08] Pete L. Clark and Xavier Xarles. Local bounds for torsion points on abelian varieties. *Canadian J. Math*, 60:532–555, 2008.

[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.

[Fal83] Gerd Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *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).

[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.

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

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

[Ray90] Michel Raynaud. p-groupes et réduction semi-stable des courbes. In *The Grothendieck Festschrift*, volume III of *Modern Birkhäuser Classics*, pages 179–197. SMF, 1990.

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

[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