MODULAR TOWERS

PIERRE DÈBES

ABSTRACT. A modular tower is a tower $(\mathsf{H}_r(G_n, \mathbf{C}_n)))_{n\geq 0}$ of Hurwitz spaces (with maps going down); the branch point number $r \geq 3$ is fixed, the groups and the conjugacy classes in the projective sequence $(G_n, \mathbf{C}_n)_{n\geq 0}$ come from a universal Frattini construction starting with a finite group G, r conjugacy classes of G and a prime p. The tower of modular curves $(X^1(p^n))_{n>0}$ is the original example: G is then the dihedral group D_p given with the involution class repeated 4 times. The first parts of the paper are devoted to the foundations of the modular tower theory. Persistence of rational points on high levels $\mathsf{H}_r(G_n, \mathbf{C}_n)$ is the main diophantine question of the theory. It corresponds to the possibility of realizing regularly all groups G_n with a bounded number of branch points and inertia groups of prime-to-p order. There are deep diophantine obstructions related to boundedness results on torsion on abelian varieties when the base field is a number field. Over ℓ-adic fields, the tendancy is the opposite. The last parts of the paper focus on these diophantine questions.

CONTENTS

1. Hurwitz spaces vade mecum 2
1.1. Covers and their equivalences 2
1.2. Hurwitz spaces as complex varieties 3
1.3. Topological viewpoint 4
1.4. Geometric construction 5
1.5. Hurwitz stacks 6
1.6. Reduced variants 6
2. Foundations of Modular Towers 6
2.1. p-universal Frattini cover 6
2.2. Characteristic quotients and lifting lemma 10
2.3. Towers of moduli spaces 11
2.4. The dihedral group example 12
3. The Modular Tower Conjecture 13
3.1. The Main Conjecture 13
3.2. The dihedral group example 14

Date: June 5, 2008.

3.3. The Fried-Kopeliovich theorem 14
3.4. Moduli space and stack versions of the MT conjecture 17
3.5. Original and reduced forms of the MT conjecture 18
4. Galois Covers, Abelian Varieties and Modular Towers 18
4.1. Central Results 19
4.2. Torsion of abelian varieties 22
4.3. Application to the MT conjecture 22
4.4. ℓ-adic points on Harbater-Mumford modular towers 26
4.5. Generalization of the central theorem 29
References 32

Prerequisites: we freely use basics from algebraic geometry, field arithmetic, finite and profinite group theory and arithmetic of curve covers. We will sometimes use more advanced results from these areas or other areas like abelian varieties; we will then give statements, explain them, sometimes sketch the proof and give some references. Our lectures also rest on previous lectures on Hurwitz spaces. Our *vade mecum* in §1 recapitulates what we will be using.

1. Hurwitz spaces vade mecum

1.1. **Covers and their equivalences.** Hurwitz spaces are moduli spaces of covers of $\mathbb{P}^1$ with fixed *group*[1] G (given as a subgroup of the symmetric group S_d with d the degree of the cover) and with a fixed number $r \geq 3$ of branch points. The basic notation for it is $\mathsf{H}_r(G)$ and a point representing a cover f, or more exactly its equivalence class, is denoted by $[f]$. There are several variants of Hurwitz spaces, depending

first, on whether one is interested in

- *the mere cover situation:* the covers are not necessarily Galois, or
- *the G-cover situation:* the covers are Galois covers given with an isomorphism between their automorphism group and the group G, and,

second, on which cover equivalence is used:

- *the original equivalence*: two covers $f : X \to \mathbb{P}^1$ and $g : Y \to \mathbb{P}^1$ are equivalent if there exists an isomorphism $\chi : X \to Y$ such that $g \circ \chi = f$, or

[1]that is, the topological monodromy group of the cover, or, equivalently, the Galois group of the Galois closure of the associated function field extension.

- *the* PGL_2*-reduced equivalence*: $f : X \to \mathbb{P}^1$ and $g : Y \to \mathbb{P}^1$ [2] are equivalent if there exist two isomorphisms $\chi : X \to Y$ and $\alpha : \mathbb{P}^1 \to \mathbb{P}^1$ such that $g \circ \chi = \alpha \circ f$,

with for both equivalences the extra condition that $\chi : X \to Y$ be compatible with the actions of G in the G-cover situation.

1.2. **Hurwitz spaces as complex varieties.** Covers are first considered over the complex field $\mathbb{C}$ and for the original equivalence. The corresponding moduli space is then a complex smooth quasi-projective variety, denoted by $\mathsf{H}_r^\infty(G)$. The central moduli space property is that

(*) *There is a bijective correspondence between the set of complex points*[3] *on* $\mathsf{H}_r^\infty(G)$ *and the set of isomorphism classes of complex covers with group* G *and* r *branch points. Moreover, this correspondence is functorial in the group* G*.*

Given an *unordered* r*-tuple*[4] $\mathbf{C} = \{C_1, \dots, C_r\}$ of conjugacy classes of G, we let $\mathsf{H}_r^\infty(G, \mathbf{C})$ be the union of all components[5] of $\mathsf{H}_r^\infty(G)$ whose points correspond to covers with ramification type[6] equal to $\mathbf{C}$. Fixing the ramification type can be regarded analogous to fixing the genus in the theory of curves and their moduli spaces.

For each $\tau \in \mathrm{Aut}(\mathbb{C})$, the conjugate space $\mathsf{H}_r^\infty(G, \mathbf{C})^\tau$ is still a Hurwitz space, which only depends on the restriction $\tau|_{\mathbb{Q}^{\mathrm{ab}}} \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$; namely it is $\mathsf{H}_r^\infty(G, \mathbf{C}^{\chi(\tau)})$, where χ is the cyclotomic character and $\mathbf{C}^{\chi(\tau)} = \{C_1^{\chi(\tau)}, \dots, C_r^{\chi(\tau)}\}$. Thus the (generally reducible) varieties $\mathsf{H}_r^\infty(G)$ and $\mathsf{H}_r^\infty(G, \mathbf{C})$ can be defined over $\mathbb{Q}$ and $\mathbb{Q}^{\mathrm{ab}}$ respectively, in the sense that their components are permuted transitively by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

[2] over a non algebraically closed field, the base space should really be *some* genus 0 curve.

[3] more generally, the complex field can be replaced by any algebraically closed field k of characteristic 0.

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

[5] by component we mean irreducible or connected components; due to smoothness of $\mathsf{H}_r^\infty(G)$, these coincide.

[6] the ramification type is the r-tuple of conjugacy classes (in the monodromy group G) of the monodromy branch cycles associated to sample loops revolving about the r branch points. It is locally constant on $\mathsf{H}_r^\infty(G)(\mathbb{C})$, thus is constant on each connected component of $\mathsf{H}_r^\infty(G)(\mathbb{C})$. More arithmetically, the ramification type corresponds to the *inertia canonical invariant*. This invariant is the collection $(C_t)_t$ of conjugacy classes C_t (in the Galois group of the Galois closure) of distinguished generators of inertia groups above t as t ranges over the branch points of the cover. The distinguished generator of some inertia group I, say of order e, is the generator that corresponds to $e^{2i\pi/e}$ in the natural isomorphism between I and the group μ_e of e-th roots of 1. For more details see [Dèb07, §3].

and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})$ respectively. Furthermore $\mathsf{H}_r^\infty(G,\mathbf{C})$ is itself defined over $\mathbb{Q}$ if $\mathbf{C}$ is a *rational union of conjugacy classes* of G, *i.e.*, if for every integer m prime to $|G|$, there exists $\sigma \in S_r$ such that $C_i^m = C_{\sigma(i)}$. More generally, given a field $k \subset \mathbb{Q}^{\mathrm{ab}}$, the tuple $\mathbf{C}$ is said to be a *k-rational union* of conjugacy classes of G if the same property holds for all integers $m \equiv \chi(\tau)$ modulo $|G|$ with $\tau \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/k)$. Under this condition, the Hurwitz space $\mathsf{H}_r^\infty(G,\mathbf{C})$ is defined over k. For example, the field generated by all roots of unity of order $|G|$ is a rationality field for $\mathbf{C}$. For arithmetical use, the main point of Hurwitz spaces is that

(**) *For any field k of characteristic 0, any k-rational point $[f]$ on $\mathsf{H}_r^\infty(G)(k)$ and any $\tau \in \mathrm{Gal}(\overline{k}/k)$, we have $[f]^\tau = [f^\tau]$. In particular, the set $\mathsf{H}_r^\infty(G)(k)$ is in bijection with the set of isomorphism classes of covers $[f]$ with r branch points, group G and field of moduli[7] k.*

1.3. **Topological viewpoint.**

1.3.1. *Nielsen classes.* Denote the configuration space for finite subsets of $\mathbb{P}^1$ of cardinality r by U_r and then by $\Psi_r : \mathsf{H}_r^\infty(G) \to \mathsf{U}_r \otimes_{\mathbb{Z}} \mathbb{C}$ the map sending each point $[f] \in \mathsf{H}_r^\infty(G)(\mathbb{C})$ to the branch point set $\mathbf{t} = \{t_1,\dots,t_r\} \in \mathsf{U}_r(\mathbb{C})$ of the cover f. A key to the theory, based on Riemann's existence theorem, is that this map is an etale cover (of algebraic varieties); furthermore there is a one-one correspondence between the fiber $\Psi_r^{-1}(\mathbf{t})$ and the set called the *Nielsen class*:

$$\mathrm{ni}(G,\mathbf{C})^\bullet = \left\{ (g_1,\dots,g_r) \in G^r \;\middle|\; \begin{array}{l} g_1\cdots g_r = 1 \\ < g_1,\dots,g_r > = G \\ g_i \in C_{\sigma(i)}, i = 1,\dots,r \\ \quad \text{for some } \sigma \in S_r \end{array} \right\} \;/\; \sim$$

Here by "$/\sim$", we mean that the tuples $(g_1,\dots,g_r)$ are regarded up to componentwise conjugation by elements of a certain subgroup of S_d (depending on the situation: for example it is G for G-covers with the original equivalence, it is the normalizer $\mathrm{Nor}_{S_d}(G)$ for mere covers, etc.). The related *straight Nielsen class* $\mathrm{sni}(G,\mathbf{C})^\bullet$ is sometimes more practical: compared to $\mathrm{ni}(G,\mathbf{C})^\bullet$, the only change in the definition is that the third condition is replaced by "$g_i \in C_i, i = 1,\dots,r$".

[7] that is the fixed field in $\overline{k}$ of the subgroup of $\mathrm{Gal}(\overline{k}/k)$ of all τ such that f and f^τ are isomorphic (*i.e.* $[f]^\tau = [f^\tau]$). The field of moduli is a field of definition in many circumstances though it is not in general.

1.3.2. *Hurwitz braid action.* The identification $\Psi_r^{-1}(\mathbf{t}) \simeq \mathrm{ni}(G,\mathbf{C})^\bullet$ is given by the monodromy representation: for any choice of a topological bouquet[8] $\underline{\Gamma} = (\Gamma_1,\dots,\Gamma_r)$ for $\mathbb{P}^1 \setminus \{\mathbf{t}\}$ based at some point $t_0 \notin \mathbf{t}$, the map $\mathrm{BCD}_{\underline{\Gamma}}$ [9], sending each complex cover $f : X \to \mathbb{P}^1$ to the r-tuple with entries the monodromy permutations of $f^{-1}(t_0)$ associated with $\Gamma_1,\dots,\Gamma_r$, provides the correspondence $\Psi_r^{-1}(\mathbf{t}) \to \mathrm{ni}(G,\mathbf{C})^\bullet$. There is a classical outer action of the Hurwitz braid group[10] $H_r = \pi_1^{\mathrm{top}}(\mathsf{U}_r,\mathbf{t})$ on $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0)$, which induces an action on the fiber $\Psi_r^{-1}(\mathbf{t})$, and on $\mathrm{ni}(\mathbf{C})^\bullet$ *via* maps $\mathrm{BCD}_{\underline{\Gamma}}$. This induced action on $\Psi_r^{-1}(\mathbf{t})$ is the monodromy action corresponding to the topological cover $\Psi_r : \mathsf{H}_r^\infty(G)(\mathbb{C}) \to \mathsf{U}_r(\mathbb{C})$. It can be explicitly determined: $\pi_1(\mathsf{U}_r,\mathbf{t})^{\mathrm{top}}$ has generators $Q_1,\dots,Q_{r-1}$ whose action on $\Psi_r^{-1}(\mathbf{t})$, when computed relative to some suitable topological bouquet $\underline{\Gamma}$, corresponds to the following action on $\mathrm{ni}(G,\mathbf{C})^\bullet$:

$$(g_1,\dots,g_r) \xrightarrow{Q_i} (g_1,\dots,g_{i-1},g_ig_{i+1}g_i^{-1},g_i,g_{i+2},\dots,g_r)$$
$$(i = 1,\dots,r-1)$$

Components of $\mathsf{H}_r^\infty(G,\mathbf{C})$ correspond to orbits of the Hurwitz braid group action.

1.4. **Geometric construction.** There is a more geometric construction of Hurwitz spaces, which leads to a definition of $\mathsf{H}_r(G)$ and of some compactification $\overline{\mathsf{H}_r(G)}$ as schemes over $\mathrm{Spec}(\mathbb{Z}[1/|G|])$. For each prime p not dividing $|G|$, the corresponding fibers above p are denoted by $\mathsf{H}_r^p(G)$ and $\overline{\mathsf{H}_r^p(G)}$. This includes the case $p = \infty$ for which one recovers the space $\mathsf{H}_r^\infty(G)$.

There is good reduction of $\mathsf{H}_r(G)$ at those primes $p \not| |G|$: the fiber $\mathsf{H}_r^p(G)$ is a (reducible) smooth variety defined over $\overline{\mathbb{F}}_p$ and its components correspond to those of $\mathsf{H}_r^\infty(G)$ through the reduction process. Furthermore, each $\mathsf{H}_r^p(G)$ is a moduli space, for covers of $\mathbb{P}^1$ with r branch points and monodromy group G, over algebraically closed fields of characteristic p.

Components in $\overline{\mathsf{H}_r(G)}$ are closures of components in $\mathsf{H}_r^\infty(G)$. The natural étale morphism $\Psi_r : \mathsf{H}_r(G) \to \mathsf{U}_r$ extends to a ramified cover $\overline{\mathsf{H}_r(G)} \to \overline{\mathsf{U}}_r$. Points on the boundary $\overline{\mathsf{U}}_r \setminus \mathsf{U}_r$ represent degenerations

[8] *i.e.*, a r-tuple $\underline{\Gamma} = (\Gamma_1,\dots,\Gamma_r)$ of homotopy classes of sample loops based at some point $t_o \notin \mathbf{t}$ generating the topological fundamental group $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0)$ with the unique relation $\Gamma_1 \cdots \Gamma_r = 1$ (plus some other technical conditions).

[9] where BCD stands for "branch cycle description".

[10] the Hurwitz braid group H_r has a classical presentation: it is the group on $r-1$ generators $Q_1,\dots,Q_r$ with relations $Q_iQ_j = Q_jQ_i$ for $|i-j| > 1$, $Q_{i+1}Q_iQ_{i+1} = Q_iQ_{i+1}Q_i$ for $1 \le i \le r-2$ and $Q_1 \cdots Q_{r-1}Q_{r-1} \cdots Q_1 = 1$.

of tuples $\mathbf{t} = (t_1, \ldots, t_r)$ for which two or more of the t_i "coalesce" (*i.e.* become equal). More formally they correspond to stable marked curves of genus 0 with a root, *i.e.* trees of curves of genus 0 with a distinguished component T_0 — the *root* — equipped with an isomorphism $\mathbb{P}^1 \simeq T_0$ and at least three marked points (including the double points) on any component but the root. Points on the boundary $\overline{\mathsf{H}_r(G)} \setminus \mathsf{H}_r(G)$ represent *admissible covers* (in a certain sense) of stable marked curves of genus 0.

1.5. **Hurwitz stacks.** Covers of $\mathbb{P}^1$ with r branch points and group G actually constitute a stack — the Hurwitz stack — which is denoted by $\mathcal{H}_r(G)$, and the substack of covers with ramification type $\mathbf{C}$ is denoted by $\mathcal{H}_r(G, \mathbf{C})$. We also denote the stack of r-marked projective lines by $\mathcal{U}_r$. The stacks $\mathcal{H}_r(G)$, $\mathcal{H}_r(G, \mathbf{C})$ and $\mathcal{U}_r$ have coarse moduli spaces, which are respectively $\mathsf{H}_r(G)$, $\mathsf{H}_r(G, \mathbf{C})$ and U_r. There is a natural functor $\mathcal{H}_r(G) \to \mathcal{U}_r$ sending each cover to the projective line $\mathbb{P}^1$ marked by its branch divisor. This functor induces the previously defined morphism $\Psi : \mathsf{H}_r(G, \mathbf{C}) \to \mathsf{U}_r$. For every field k of characteristic 0, k-rational points on $\mathcal{H}_r(G, \mathbf{C})$ correspond to k-covers while k-rational points on $\mathsf{H}_r(G, \mathbf{C})$ correspond to $\overline{k}$-isomorphism classes of covers with k as field of moduli.

1.6. **Reduced variants.** Moduli spaces also exist for the PGL_2-reduced equivalence. The corresponding moduli space, for covers with group G and r branch points, is denoted by $\mathsf{H}_r^{\equiv}(G)$. The subspace corresponding to covers with ramification type $\mathbf{C}$ is denoted by $\mathsf{H}_r^{\equiv}(G, \mathbf{C})$. These spaces are called PGL_2-reduced Hurwitz spaces. The induced morphism $\mathsf{H}_r(G, \mathbf{C}) \to \mathsf{H}_r^{\equiv}(G, \mathbf{C})$ can be identified with the geometric quotient of $\mathsf{H}_r(G, \mathbf{C})$ by PGL_2 and the finite morphism $\Psi : \mathsf{H}_r(G, \mathbf{C}) \to \mathsf{U}_r$ induces a finite morphism $\Psi^{\equiv} : \mathsf{H}_r^{\equiv}(G, \mathbf{C}) \to \mathsf{U}_r/\mathrm{PGL}_2$.

The map $\mathsf{H}_r(G, \mathbf{C}) \to \mathsf{H}_r^{\equiv}(G, \mathbf{C})$ has these further properties:

(*) The components of the PGL_2-reduced Hurwitz space $\mathsf{H}_r^{\equiv}(G, \mathbf{C})$ are in bijection with the components of the Hurwitz space $\mathsf{H}_r(G, \mathbf{C})$.

(**) There exists a constant $d(r)$ such that every point on the PGL_2-reduced Hurwitz space $\mathsf{H}_r^{\equiv}(G, \mathbf{C})$, rational over some field k, can be lifted to some point on the original Hurwitz space $\mathsf{H}_r(G, \mathbf{C})$ rational, together with the associated branch points, over some extension of k of degree $\leq d(r)$. [Cada, corollary 3.12]

2. Foundations of Modular Towers

2.1. **p-universal Frattini cover.** Our main reference here is [FJ04].

2.1.1. *Preliminaries.* We recall some definitions and classical results from the profinite group theory.

A surjective profinite group homomorphism $\psi : H \to G$ is often called a *cover* and the group H a cover of G. If p is a prime, a *p-cover* is a cover with kernel a pro-p-group.

A profinite group G is said to be *projective* if every embedding problem of profinite groups for G is weakly solvable. If p is a prime, a pro-p group G is said to be *p-projective* if every embedding problem of profinite groups for G with kernel a pro-p-group is weakly solvable.

The *Frattini subgroup* of a profinite group G is defined to be the intersection of all maximal open subgroups of G and is denoted by $\Phi(G)$. An equivalent definition is: if $H \subset G$ is a closed subgroup such that $\langle H, \Phi(G)\rangle = G$, then $H = G$. The Frattini subgroup $\Phi(G)$ is a pro-nilpotent group [FJ04, 22.1.2] [11]. A cover $\psi : H \to G$ is said to be a *Frattini cover* if its kernel is contained in $\Phi(H)$, or, equivalently, if for each closed subgroup H' of H, $\psi(H') = G \Rightarrow H' = H$. A Frattini cover that is also a p-cover is called a *p-Frattini cover*.

For pro-p groups, we have this basic result [FJ04, 22.7.4].

Lemma 2.1. *Let G be a pro-p-group of rank m. Then $\Phi(G) = G^p[G,G]$ and $G/\Phi(G)$ is isomorphic to the vector space $\mathbb{F}_p^m$.*

Sketch of proof. Maximal open subgroups of the pro-p group G are open normal subgroups of index p. It follows that there is a canonical embedding $G/\Phi(G) \to \prod G/N$ where N ranges over all open normal subgroups of index p. The product can be regarded as a vector space over $\mathbb{F}_p$. As a subspace, so does $G/\Phi(G)$. Whence $G/\Phi(G) \simeq \mathbb{F}_p^\rho$ with $\rho = \mathrm{rank(G/\Phi(G))}$. But from the Frattini property, $\mathrm{rank(G/\Phi(G))} = \mathrm{rank(G)}$ [FJ04, 22.5.3].

It follows next from $G/\Phi(G) \simeq \mathbb{F}_p^m$ that the subgroup $G_0 = G^p[G,G]$ maps to $\{1\}$ modulo $\Phi(G)$. Whence $G_0 \subset \Phi(G)$. The quotient group G/G_0 is a product of copies of $\mathbb{Z}/p\mathbb{Z}$. If $x \notin G_0$, there is at least one such copy where x does not go to 0, *i.e.*, is not in the kernel of the corresponding map $G \to \mathbb{Z}/p\mathbb{Z}$, which is a maximal open subgroup of G. Thus $x \notin \Phi(G)$, which proves the other containment $\Phi(G) \subset G_0$. □

An important consequence is Tate's theorem [FJ04, 22.7.6 & 22.7.7].

[11] Here is the argument, in the case G is finite. If P is a p-Sylow subgroup of $\Phi(G)$, then for each $g \in G$, P^g is also a p-Sylow subgroup of $\Phi(G)$. Hence there exists $a \in \Phi(G)$ such that $P^g = P^a$. Therefore ga^{-1} is in the normalizer $\mathrm{Nor}_G(P)$. This shows that $G = \mathrm{Nor}_G(P)\Phi(G)$. From the Frattini property, we deduce $G = \mathrm{Nor}_G(P)$, that is, P is normal in G, and so also in $\Phi(G)$. Classically, the p-Sylow subgroups being normal subgroups characterize nilpotent groups.

Theorem 2.2. *A pro-p group is projective if and only if it is free pro-p. A closed subgroup of a free pro-p-group is free pro-p. In particular, a projective pro-p-group has no non-trivial element of finite order.*

Sketch of proof. A free pro-p group F is projective [FJ04, 22.4.5]. If G is a closed subgroup of a free pro-p group F, it is projective as a closed subgroup of a projective group [FJ04, 22.4.7], and it is a pro-p group [FJ04, 17.3.1]. Let m be the rank of the projective pro-p group G. Lemma 2.1 provides $G/\Phi(G) \simeq \mathbb{F}_p^m$ which rewrites $G/\Phi(G) \simeq \hat{F}_m(p)/\Phi(\hat{F}_m(p))$, where $\hat{F}_m(p)$ is the free pro-p group of rank m [FJ04, §17.4]. Now due to the Frattini property and the projectivity of G, this implies $G \simeq \hat{F}_m(p)$ [FJ04, 22.5.10]. □

We also recall two classical and useful results.

Lemma 2.3 (Nielsen-Schreier)**.** *Let $\mathcal{C}$ be a full formation of finite groups (i.e., a family of finite groups closed under taking quotients, subgroups and extensions). Let F be a free pro-$\mathcal{C}$-group (i.e., an inverse limit of groups in $\mathcal{C}$). Then every open subgroup $H \subset F$ is a free pro-$\mathcal{C}$-group. Moreover* $\mathrm{rank}(H) = 1 + [F : H]\,(\mathrm{rank}(F) - 1)$ *if* $\mathrm{rank}(F)$ *is finite and* $\mathrm{rank}(H) = \mathrm{rank}(F)$ *if* $\mathrm{rank}(F)$ *is infinite. Consequently, an open subgroup of index n of a profinite group of rank $\leq e$ is of finite rank $\leq 1 + n(e-1)$.*

Proof. see [FJ04, 17.6.2 & 17.6.3] □

Lemma 2.4 (Schur-Zassenhaus)**.** *Let N be a closed normal subgroup of a profinite group G. Assume $|N|$ and $[G : N]$ are relatively prime. Then N has a complement in G. Furthermore, all complements to N in G are conjugate.*

Proof. see [FJ04, 22.10.1] □

2.1.2. *p-universal Frattini cover.* The following statement summarizes the definition and properties of the universal Frattini cover and of the universal p-Frattini cover.

The covers of a group G are partially ordered as follows. Given two covers $\theta_i : H_i \to G$, $i = 1, 2$ we write $\theta_2 \geq \theta_1$ if there is a cover $\theta : H_2 \to H_1$ with $\theta_1 \circ \theta = \theta_2$.

Theorem 2.5. *Each profinite group G has a cover $\tilde{\varphi} : \tilde{G} \to G$ and, for each prime p, a p-cover ${}_p\tilde{\varphi} : {}_p\tilde{G} \to G$, all unique, up to an isomorphism, respectively called the universal Frattini cover and the universal p-Frattini cover of G, that satisfy the following equivalent conditions:*

for $\tilde{\varphi} : \tilde{G} \to G$:

(a) $\tilde{\varphi} : \tilde{G} \to G$ *is a projective Frattini cover of* G.
(b) $\tilde{\varphi} : \tilde{G} \to G$ *is the largest Frattini cover of* G.
(c) $\tilde{\varphi} : \tilde{G} \to G$ *is the smallest projective cover of* G.

for ${}_p\tilde{\varphi} : {}_p\tilde{G} \to G$*:*

${}_p$(a) ${}_p\tilde{\varphi} : {}_p\tilde{G} \to G$ *is a* p*-projective Frattini* p*-cover of* G.
${}_p$(b) ${}_p\tilde{\varphi} : {}_p\tilde{G} \to G$ *is the largest Frattini* p*-cover of* G.
${}_p$(c) ${}_p\tilde{\varphi} : {}_p\tilde{G} \to G$ *is the smallest* p*-projective* p*-cover of* G.

The groups $\tilde{G}$ *and* ${}_p\tilde{G}$ *are profinite groups of rank equal to* $\mathrm{rank}(G)$. *The subgroup* $\ker({}_p\tilde{\varphi})$ *and the* p*-Sylow subgroups of* ${}_p\tilde{G}$ *are open and free pro-*p *of finite rank.*

For example, for $G = \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$, we have $\tilde{G} = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$ and ${}_{p_1}\tilde{G} = \mathbb{Z}_{p_1} \times \mathbb{Z}/p_2\mathbb{Z} \cdots \times \mathbb{Z}/p_r\mathbb{Z}$.

From the Schur-Zassenhaus lemma (2.4) and the Frattini property, for p not dividing $|G|$ there is no non-trivial Frattini cover of G with p-group kernel, and so the universal p-Frattini cover of G is trivial.

Proof. The equivalences to be shown are rather straightforward. For example, if $\tilde{\varphi} : \tilde{G} \to G$ satisfies (a) and $h : H \to G$ is a Frattini cover, then from the projectivity of $\tilde{\varphi} : \tilde{G} \to G$, there exists a morphim $\theta : \tilde{G} \to H$ such that $h \circ \theta = \tilde{\varphi}$; from the Frattini property of $\tilde{\varphi} : \tilde{G} \to G$, we have $\theta(\tilde{G}) = H$, which proves (b). For a detailed proof of the other equivalences, we refer to [FJ04, §22.6 & §22.11]. Below we focus on the construction of $\tilde{G}$ and ${}_p\tilde{G}$ and their main properties.

Classically, there exists an epimorphism $\varphi : F \to G$ with F a free profinite group [FJ04, §17.4.8]. Using Zorn's lemma, one can show F has a minimal closed subgroup H such that $\varphi(H) = G$: indeed if $(H_i)_{i \in I}$ is a decreasing chain of closed subgroups of F such that $\varphi(H_i) = G$ $(i \in I)$, then $\varphi(\bigcap_{i \in I} H_i) = G$. The restriction $\varphi|_H : H \to G$ is a Frattini cover and as H is projective (as a closed subgroup of a projective group), it satisfies condition (a).

Set then $K = \ker(\tilde{\varphi})$ where $\tilde{\varphi}$ is the universal Frattini cover of G, for example the cover just constructed. Then $K \subset \Phi(\tilde{G})$ and so is pro-nilpotent, as $\Phi(\tilde{G})$ is [FJ04, §22.1.2] (see also footnote 2.1.1). Therefore K is the direct product $\prod_\ell K_\ell$ of its ℓ-Sylows K_ℓ, which are normal in $\tilde{G}$. Since $\tilde{G}$ is projective, each K_ℓ is projective, hence free pro-ℓ.

Set $K'_p = \prod_{\ell \neq p} K_\ell$. Then K'_p is a closed normal subgroup of $\tilde{G}$. Put $\hat{G} = \tilde{G}/K'_p$, $\bar{K} = K/K'_p$ and $\hat{\varphi} : \hat{G} \to G$ the epimorphism induced by $\tilde{\varphi}$. Then $\bar{K} = \ker(\hat{\varphi})$, $\bar{K} \simeq K_p$ is free pro-p and $\bar{K} \subset \Phi(\hat{G})$. In particular

$\hat{\varphi}:\hat{G}\to G$ is a Frattini p-cover. The argument below shows that $\hat{G}$ is p-projective and so $\hat{\varphi}:\hat{G}\to G$ satisfies condition ${}_p$(a).

Consider an embedding problem for $\hat{G}$ with kernel a p-group N. Using the map $\tilde{G}\to\hat{G}$, extend it to an embedding problem for $\tilde{G}$. As $\tilde{G}$ is projective, this embedding problem has a weak solution ψ. Now we have $\psi(K_p')=\{1\}$: indeed we have both $\psi(K_p')\cap N=\{1\}$ (as N is a p-group) and $\psi(K_p')=1$ modulo N (as the embedding problem for $\tilde{G}$ factors through $\tilde{G}/K_p'=\hat{G}$). Therefore the solution ψ factors through $\tilde{G}/K_p'$ to provide a weak solution to the original embedding problem.

Finally let $\tilde{G}_p$ be a p-Sylow of $\tilde{G}$; it is projective as a closed subgroup of a projective group. We have $\tilde{G}_p\cap K_p'=\{1\}$, hence $\tilde{G}_pK_p'/K_p'\simeq\tilde{G}_p$. Now $\tilde{G}_pK_p'/K_p'$ is a p-Sylow of $\tilde{G}/K_p'=\hat{G}$ [FJ04, §22.9.2]. It is projective hence a free pro-p group, and it is of finite index in $\hat{G}$ as $\tilde{G}_pK_p'\supset K_pK_p'=K$ and K/K_p' is of finite index in $\hat{G}=\tilde{G}/K_p'$. That it is of finite rank follows from the Nielsen-Schreier lemma (2.3). □

2.2. **Characteristic quotients and lifting lemma.** 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 $\rho\geq 1$.

For example, $\widetilde{G}\to G_0$ can be taken to be the universal p-Frattini cover of G_0 (§2.1). In the sequel, we talk of this special situation as *Fried's original context*.

Consider next the Frattini series $(\widetilde{P}_n)_{n\geq 0}$ of $\widetilde{P}$ defined by:

$$\begin{cases}\widetilde{P}_0=\widetilde{P}\\ \widetilde{P}_n=\Phi(\widetilde{P}_{n-1})=\widetilde{P}_{n-1}^p[\widetilde{P}_{n-1},\widetilde{P}_{n-1}] & (n\geq 1)\end{cases}$$

For example, for $\widetilde{G}\to G_0$ the map $\mathbb{Z}_p\to\mathbb{Z}/p\mathbb{Z}$, we have $\widetilde{P}_n=p^{n+1}\mathbb{Z}_p$.

Lemma 2.6. *The groups $\widetilde{P}_n$ are characteristic free pro-p subgroups of $\widetilde{P}$ and form a fundamental system of open neighborhoods of* 1. *Consequently the quotients $G_n=\widetilde{G}/\widetilde{P}_n$ are finite and $\widetilde{G}$ is the inverse limit of its "characteristic quotients" G_n.*

Proof. The groups $\widetilde{P}_n$ are clearly characteristic closed subgroups of $\widetilde{P}$. In particular, they are pro-p groups [FJ04, 17.3.1]. From lemma 2.1, $[\widetilde{P}_{n-1}:\widetilde{P}_n]<\infty$, which, joint to $[\widetilde{G}:\widetilde{P}]=|G_0|<\infty$, shows the subgroups $\widetilde{P}_n$ are of finite index in $\widetilde{P}$. Thus they are open subgroups and so from lemma 2.3, they are free pro-p subgroups of $\widetilde{P}$. If U is

an open normal subgroup of $\widetilde{P}$, then $\widetilde{P}/U$ is a finite p-group and so $\Phi^n(\widetilde{P}/U) = \{1\}$ for some n. Check then that $\Phi^n(\widetilde{P}/U) = \Phi^n(\widetilde{P})U/U$ and conclude that $\Phi^n(\widetilde{P}) = \widetilde{P}_n \subset U$. This shows the groups $\widetilde{P}_n$ form a fundamental system of open neighborhoods of 1. The final assertion, *i.e.* $\widetilde{G} = \varprojlim G_n$, then follows [FJ04, 1.2.4]. □

Fix an integer $r \geq 3$ and an unordered r-tuple $\mathbf{C} = \{C_1, \ldots, C_r\}$ of conjugacy classes of G_0 of prime-to-p order[12]. We will always assume $\mathrm{sni}(G_0, \mathbf{C})^\bullet \neq \emptyset$. In particular, G_0 is of rank $\leq r$ and it is *p-perfect*, *i.e.*, it is generated by its elements of prime-to-p order, or, equivalently, G_0 has no $\mathbb{Z}/p\mathbb{Z}$ quotient (for example, this excludes p-groups).

Lemma 2.7 (Lifting Lemma)**.** *If C is a conjugacy class of G_n of order ρ prime to p, then there exists a unique conjugacy class of G_{n+1} that lifts C and is of order ρ.*

Proof. Let $\phi_n : G_{n+1} \to G_n$ be the natural surjection. Let $g \in C$ and $H = \phi_n^{-1}(\langle g \rangle)$. We have an exact sequence $1 \to \widetilde{P}_n/\widetilde{P}_{n+1} \to H \to \langle g \rangle \to 1$. From the Schur-Zassenhaus lemma (2.4), since g is of order prime to p, the sequence splits; furthermore, the section $\langle g \rangle \to H$ is unique, up to conjugation. □

2.3. **Towers of moduli spaces.**

2.3.1. *Hurwitz towers.* Suppose given a projective system $(G_n)_{n\geq 0}$ of finite groups with limit a profinite group $\widetilde{G}$. Suppose also given an unordered tuple $\widetilde{\mathbf{C}} = \{\widetilde{C}_1, \ldots, \widetilde{C}_r\}$ of conjugacy classes of $\widetilde{G}$. For each integer $n \geq 0$, denote by C_{in} the conjugacy class of G_n naturally obtained from $\widetilde{C}_i$, $i = 1, \ldots, r$, and the corresponding tuple by $\mathbf{C}_n$.

Consider the associated Hurwitz spaces $\mathsf{H}_r(G_n, \mathbf{C}_n)$, which we denote for short by H^n. By functoriality, the canonical surjections $G_n \to G_{n-1}$ induce algebraic maps $\mathsf{H}^n \to \mathsf{H}^{n-1}$ $(n \geq 1)$.

Definition 2.8. The collection $(\mathsf{H}^n)_{n\geq 0}$ given with the maps $\mathsf{H}^n \to \mathsf{H}^{n-1}$ is called a *Hurwitz tower*. It is denoted by $\mathsf{H}_r(\widetilde{G}, \widetilde{\mathbf{C}})$.

Hurwitz stacks $\mathcal{H}^n = \mathcal{H}_r(G_n, \mathbf{C}_n)$ are defined similarly. The collection $(\mathcal{H}^n)_{n\geq 0}$ with the corresponding maps $\mathcal{H}^n \to \mathcal{H}^{n-1}$ is the *stack tower* associated with $\widetilde{G}$, r and $\widetilde{\mathbf{C}}$; we denote it by $\mathcal{H}_r(\widetilde{G}, \widetilde{\mathbf{C}})$.

[12]by order, we mean the common order of the elements in the conjugacy class.

2.3.2. *Modular towers.* Modular towers are defined in the context of §2.2, that is, we fix a prime p, 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 $\rho \geq 1$, fix an integer $r \geq 3$ and an unordered r-tuple $\mathbf{C} = \{C_1, \dots, C_r\}$ of conjugacy classes of G_0 of prime-to-p order such that $\mathrm{sni}(G_0, \mathbf{C})^\bullet \neq \emptyset$.

From the lifting lemma (2.7), each class C_i can be uniquely lifted *via* 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 $\mathbf{C}^n = \{C_1^n, \dots, C_r^n\}$ of conjugacy classes of G_n. When in turn n tends to ∞, $\mathbf{C}^n$ determines an unordered r-tuple $\widetilde{\mathbf{C}} = \{\widetilde{C}_1, \dots, \widetilde{C}_r\}$ of conjugacy classes of $\widetilde{G}$.

Definition 2.9. In this situation, the Hurwitz tower $\mathsf{H}_r(\widetilde{G}, \widetilde{\mathbf{C}})$ from §2.3.1 is called the *modular tower* associated with $\widetilde{G} \to G_0$, r, p and $\mathbf{C}$. It is denoted by $\mathsf{H}_r(\widetilde{G} \to G_0, p, \mathbf{C})$. The corresponding stack tower is denoted by $\mathcal{H}_r(\widetilde{G} \to G_0, p, \mathbf{C})$. In Fried's original context, that is for $\widetilde{G} \to G_0$ the universal p-Frattini cover ${}^p\tilde{G}_0 \to G_0$, the modular tower is denoted by $\mathsf{H}_r(G_0, p, \mathbf{C})$ and the stack tower by $\mathcal{H}_r(G_0, p, \mathbf{C})$.

There is a *reduced* variant of Hurwitz towers, for which the Hurwitz spaces H^n should be replaced by the PGL_2-reduced versions $\mathsf{H}^{n,\equiv}$.

Definition 2.10. The collection $(\mathsf{H}^{n,\equiv})_{n\geq 0}$ with maps $\mathsf{H}^{n+1,\equiv} \to \mathsf{H}^{n,\equiv}$ is called PGL_2-*reduced modular tower* and denoted by $\mathsf{H}_r^{\equiv}(\widetilde{G} \to G_0, p, \mathbf{C})$, and by $\mathsf{H}_r^{\equiv}(G_0, p, \mathbf{C})$ in Fried's original context.

The natural morphisms $\mathsf{H}^n \to \mathsf{H}^{n,\equiv}$ induce a morphism of towers $\mathsf{H}_r(\widetilde{G} \to G_0, p, \mathbf{C}) \to \mathsf{H}_r^{\equiv}(\widetilde{G} \to G_0, p, \mathbf{C})$.

2.4. **The dihedral group example.** Take $\widetilde{G} \to G_0$ to be the pro-dihedral extension $D_{p^\infty} = \mathbb{Z}_p \rtimes \mathbb{Z}/2\mathbb{Z} \to D_p$ (p an odd prime), $r = 4$ and $\mathbf{C}$ consisting of 4 copies of the involution class of D_p. Then the PGL_2-reduced modular tower, in the G-cover situation, is isomorphic to the tower of modular curves $Y_1(p^{n+1})$ ($n \geq 0$).

We recall below the origin of the isomorphism $Y_1(p^{n+1}) \simeq \mathsf{H}_r^{\equiv}(G_n, \mathbf{C}^n)$, that is how modular curves can be presented as Hurwitz spaces of dihedral covers of $\mathbb{P}^1$ branched at 4 points. For more details, see [Fri78, §2.B] and [Fri80].

For each $n \geq 0$, G_n is the dihedral group $D_{p^{n+1}} = \mathbb{Z}/p^{n+1} \rtimes \mathbb{Z}/2$ and the $r = 4$ classes C_i^n are the involution class C^n of G_n.

Suppose given a cover $f : E \to \mathbb{P}^1$ defined and Galois over some field k, of group G_n, with 4 branch points and with inertia $\mathbf{C}^n$. The Riemann-Hurwitz formula yields the genus g of E: $2g-2 = 2p^{n+1}(-2)+$

$4p^{n+1}$, that is $g = 1$. The Jacobian $\mathrm{Pic}^o(E)$ has a k-rational point and so is an elliptic curve over k. Elements of order p^{n+1} in G_n are automorphisms of $\mathrm{Pic}^o(E)$ of order p^{n+1} defined over k. Thus they are translations by some p^{n+1}-torsion point $\mathcal{P}$ defined over k. The data $(\mathrm{Pic}^o(E), \mathcal{P})$ classically corresponds to some point on the modular curve $Y_1(p^{n+1})$ different from the cusps.

Conversely, let $(E, \mathcal{P})$ be an elliptic curve given with a p^{n+1}-torsion point, both defined over k. The cover $E \to E/ < \mathcal{P} >$ is cyclic of degree p^{n+1}. The curve $E_o = E/ < \mathcal{P} >$ is an elliptic curve over k. Composing the above cover with the cover $E_o \to E_o/ < -1 >= \mathbb{P}^1$ (where -1 is the canonical involution of E), gives a cover $E \to \mathbb{P}^1$ defined and Galois over k, of group $D_{p^{n+1}}$, with 4 branch points and with inertia $\mathbf{C}^n$.

3. The Modular Tower Conjecture

To state the main conjectures, we place ourselves in Fried's original context: the group $\widetilde{G}$ is the p-universal Frattini cover of some finite group G_0. This is a special case of the more general context for which is given an extension $1 \to \widetilde{P} \to \widetilde{G} \to G_0 \to 1$ of a finite group by a pro-p group of finite positive rank. The conjectures below can be understood in this more general context (see remark 3.3).

We use the notation introduced in §2.2 and §2.3.

We often abbreviate "Modular Towers" as "MT".

We only consider the G-cover situation in this section.

3.1. **The Main Conjecture.** There are two forms *a priori* but we show in §3.3 that they are essentially equivalent.

In addition to the above, fix an integer $r \geq 3$ and an unordered r-tuple $\mathbf{C} = \{C_1, \ldots, C_r\}$ of conjugacy classes of G_0 of prime-to-p order. Associated with the data, we have a modular tower $\mathsf{H}_r(G_0, p, \mathbf{C})$; its levels are the Hurwitz spaces $\mathsf{H}^n = \mathsf{H}_r(G_n, \mathbf{C}^n)$, which correspond to the characteristic quotients $G_n = \widetilde{G}/\widetilde{P}_n$.

Conjecture 3.1 (Modular Tower Realization Conjecture)**.** *Let K be a number field. Then only finitely many groups G_n can be regularly realized over K with at most r branch points.*

Conjecture 3.2 (Modular Tower Diophantine Conjecture)**.** *Let K be a number field. If n suitably large (depending on 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 $\mathcal{H}_r(G_0, p, \mathbf{C})$.*

(for moduli spaces) *there are no K-rational points on the n-th level H^n of the modular tower $\mathsf{H}_r(G_0, p, \mathbf{C})$.*

Remark 3.3. As said above, these conjectures can be understood in the more general context from §2.2. They are then stronger than in Fried's original context. The conjectures are stated in an even more general context in [CT07]: there the modular towers are replaced by general Hurwitz towers as in §2.3.1, with the only assumption of $\widetilde{G}$ that it contains an open subgroup admitting a quotient isomorphic to $\mathbb{Z}_p$.

The moduli space version of conjecture 3.2 is *a priori* stronger than the stack version but they can be shown to be equivalent; and they also are in the more general context from §2.2 if the dependence in K of the constants is through $[K:\mathbb{Q}]$ (see §3.4).

There is an analog of the MT Diophantine Conjecture for PGL_2-reduced modular towers. It is *a priori* stronger than the original one but the two versions are equivalent if the dependence in K of the constants is through $[K:\mathbb{Q}]$ (see §3.5).

3.2. **The dihedral group example.** Consider the dihedral group situation from §2.4: $\widetilde{G} \to G_0$ is the extension $D_{p^\infty} \to D_p$ (p an odd prime) and $\mathbf{C}$ consists of r copies of the involution class of D_p.

Conjecture 3.1 implies the following statement, which is still open for $r > 5$. The proof for $r \leq 5$, originally in [DF94], is given in §4.3 (corollary 4.11).

Conjecture 3.4 (Dihedral Group Conjecture)**.** *Given a number field K and an integer $r \geq 3$, only finitely many groups $G = D_{p^n}$ with p an odd prime and $n \geq 1$ can be regularly realized over K with at most r branch points.*

For $r = 4$ the reduced form of the MT Diophantine Conjecture amounts to the classical result that there are no K-rational points on the modular curve $Y_1(p^{n+1})$ is n is suitably large.

3.3. **The Fried-Kopeliovich theorem.** The following result originally appeared in [FK97].

Theorem 3.5. *Let $r_0 \geq 3$ be an integer and K be a number field. Suppose each characteristic quotient G_n of $\widetilde{G}$ can be regularly realized over $K(T)$ with no more than r_o branch points ($n \geq 0$). Then there exists an integer $r \leq r_0$ and an r-tuple $\mathbf{C}$ of conjugacy classes of G_0 of prime-to-p order such that the stack tower $\mathcal{H}_r(G_0, p, \mathbf{C})$ has K-rational points at every level.*

Consequently, in order to prove the MT Realization Conjecture 3.1 with K, G_0, p and $r_0 \geq 3$ given, it is sufficient to prove the stack form of the MT Diophantine Conjecture 3.2 for K, G_0, p and every $r \leq r_0$. The converse is clear so we have the following.

Corollary 3.6. *The MT Realization Conjecture 3.1 is equivalent to the stack version of the MT Diophantine Conjecture 3.2.*

A basic ingredient of the proof is the classical *Branch Cycle Lemma* which we recall below; for more details, we refer to [Dèb07, §3], [Völ96, p.34] or [DF08].

Denote the cyclotomic character of K by χ_K: for each root of unity ζ, say of order $n \geq 1$, and $\tau \in \mathrm{Gal}(\overline{K}/K)$, $\chi(\tau)$ is the element of $(\mathbb{Z}/n\mathbb{Z})^\times$ such that $\zeta^\tau = \zeta^{\chi(\tau)}$. This defines the cyclotomic character χ_K as a morphism from $\mathrm{Gal}(\overline{K}/K)$ to the group $\widehat{\mathbb{Z}}$ (the inverse limit of all groups $(\mathbb{Z}/n\mathbb{Z})$ $(n \geq 1)$).

Lemma 3.7 (Branch Cycle Lemma)**.** *Let K be a field of characteristic 0 and $f : X \to \mathbb{P}^1$ be a G-cover defined over K. Let G, $\mathbf{t} = \{t_1, \ldots, t_r\}$ and $\mathbf{C} = \{C_1, \ldots, C_r\}$ be respectively the group, the branch point set and the ramification type of the cover. Assume moreover that C_i is the conjugacy class corresponding to the branch point t_i, $i = 1, \ldots, r$. Then for each $\tau \in \mathrm{Gal}(\overline{K}/K)$, we have*

$$\{(t_1^\tau, C_1^{1/\chi_K(\tau)}), \ldots, (t_r^\tau, C_r^{1/\chi_K(\tau)})\} = \{(t_1, C_1), \ldots, (t_r, C_r)\}$$

Proof of theorem 3.5. We reproduce here the proof given in [Dèb06]. However, for a later use, we weaken the assumption on K to only suppose it is any field of characteristic 0 with cyclotomic closure of infinite degree.

As for each level $n \geq 0$, there are only finitely many possible choices of tuples $\mathbf{C}_n$ of conjugacy classes of G_n with no more than r_0 entries and that any regular realization of G_n with ramification type $\mathbf{C}_n$ yields a realization of G_{n-1} with ramification type the tuple induced from $\mathbf{C}_n$ by the map $G_n \to G_{n-1}$ $(n > 1)$, the assumption of theorem 3.5 implies that all characteristic quotients G_n of $\widetilde{G}$ can be regularly realized over $K(T)$ with some ramification types $\mathbf{C}_n = (C_{n1}, \ldots, C_{nr})$ that are compatible all along the tower; in particular, the number r of branch points is the same for all $n \geq 0$. We suppose given such a set of realizations.

We now make the following hypothesis and show that it leads to a contradiction:

(H) *There exists an integer $n_0 \geq 0$ such that for all $n \geq n_0$ at least one inertia group is of order divisible by p in the given realization of G_n.*

We may and will assume that $C_{n_o 1}$ is of order divisible by p; then so is C_{n1} for all $n \geq n_o$. Fix $\mathbf{g} = (g_n)_{n \geq 0} \in \widetilde{G}$ such that $g_n \in C_{n1}$ for all $n \geq 0$. For each $n \geq 0$, let $\nu_n = \nu_n(\mathbf{g})$ be the number of non-conjugate

$g_n^{\chi_K(\tau)}$ in G with τ ranging over $\chi_K(\mathrm{Gal}(\overline{K}/K))$. The Branch Cycle Lemma (lemma 3.7) yields

$$(*) \qquad \nu_n(\mathbf{g}) \leq r_o \text{ for all } n \geq 0$$

Write the order of g_0 in the form αp^{k_0} with $k_0 \geq 0$, $\alpha \geq 1$ and $(p, \alpha) = 1$. We will show (*) is impossible. To do so, one may, up to changing $\mathbf{g}$ into $\mathbf{g}^{\alpha p^{k_0}}$, assume that $\mathbf{g}$ is an element of $\widetilde{P}$ of p-power order: just note that $\nu_n(\mathbf{g}^{\alpha p^{k_0}}) \leq \nu_n(\mathbf{g})$ for all $n \geq 0$. Also note that for each $n \geq 0$, g_n is of order αp^{k_n} with $k_n \geq k_0$ (as $g_n^{\alpha p^{k_0}}$ lies in $\widetilde{P}_0/\widetilde{P}_n$ which is a p-group) and that the sequence $(k_n)_{n\geq 0}$ is unbounded. Otherwise, $\mathbf{g}^\alpha$ would be an element of finite p-power order and non-trivial (p divides the order of g_{n_0}), but the p-Sylows of $\widetilde{G}$ are free-pro-p (theorem 2.5).

Let $\nu_0 = \max_{n\geq 0}\nu_n(\mathbf{g})$, and, for some level k with $\nu_k(\mathbf{g}) = \nu_0$, let $g_k^{\mu_1}, \ldots, g_k^{\mu_{\nu_0}}$ be some representatives of the $g_k^{\chi_K(\tau)}$ ($\tau \in \mathrm{Gal}(\overline{K}/K)$) modulo conjugation in G_k. As at higher levels $n \geq k$, $g_n^{\mu_1}, \ldots, g_n^{\mu_{\nu_0}}$ remain non-conjugate, for every level $n \geq 0$ and for each $\tau \in \mathrm{Gal}(\overline{K}/K)$,

(**) $g_n^{\chi_K(\tau)}$ is conjugate to $g_n^{\mu_i}$ for some $i \in \{1, \ldots, \nu_0\}$.

As condition (**) at level n with some conjugation factor $h_{\tau,n}$ implies the same condition at lower levels with the same exponent μ_i and with conjugation factors those induced by $h_{\tau,n}$ and that both the exponents μ_i and the conjugation factors vary in finite sets, we obtain that for each $\tau \in \mathrm{Gal}(\overline{K}/K)$, there exist $i(\tau) \in \{1, \ldots, \nu_0\}$ and $\mathbf{h}_\tau = (h_{\tau,n})_{n\geq 0} \in \widetilde{G}$ such that

$$(***) \qquad \mathbf{g}^{\chi_K(\tau)} = \mathbf{h}_\tau\, \mathbf{g}^{\mu_{i(\tau)}}\, \mathbf{h}_\tau^{-1} \text{ in } \widetilde{G}.$$

From above the order of g_n tends to ∞ with n. Let $\kappa \geq 0$ be the smallest integer such that $\mathbf{g} \in \widetilde{P}_\kappa \setminus \widetilde{P}_{\kappa+1}$. From the assumption on K, the set $\chi_K(\mathrm{Gal}(\overline{K}/K))$ is infinite. So if n is suitably large, there exist $\tau, \tau' \in \mathrm{Gal}(\overline{K}/K)$ such that $g_n^{\chi(\tau)} \neq g_n^{\chi(\tau')}$ with $i(\tau) = i(\tau')$ and $h_{\tau,\kappa} = h_{\tau',\kappa}$. This yields

$$(****) \qquad \mathbf{g}^{\chi_K(\tau')} = (\mathbf{h}_{\tau'}\mathbf{h}_\tau^{-1})\, \mathbf{g}^{\chi_K(\tau)}\, (\mathbf{h}_{\tau'}\mathbf{h}_\tau^{-1})^{-1} \text{ with } \mathbf{h}_{\tau'}\mathbf{h}_\tau^{-1} \in \widetilde{P}_\kappa$$

Complement $\mathbf{g}$ with elements $\mathbf{g}_2, \ldots, \mathbf{g}_l$ so that the profinite subgroups $B = \langle \mathbf{g} \rangle$ and $D = \langle \mathbf{g}_2, \ldots, \mathbf{g}_l \rangle$ freely generate $\widetilde{P}_\kappa$ [RZ00, 7.6.10]. From (****), for $\mathbf{h}' = \mathbf{h}_{m'}\mathbf{h}_m^{-1}$, we have $\mathbf{h}' B (\mathbf{h}')^{-1} = B$. In this situation, we get $\mathbf{h}' \in B$ [RZ00, 9.1.12]. But as $B = \langle \mathbf{g} \rangle$ is abelian, (****) would rewrite $\mathbf{g}^{\chi(\tau')} = \mathbf{g}^{\chi(\tau)}$ — a contradiction.

Conclude that (H) does not hold. Therefore, in the given set of regular realizations over $K(T)$ of groups G_n ($n \geq 0$), there exists infinitely many levels $n \geq 0$ such that all inertia classes $C_{n1}, \ldots, C_{nr}$ are of prime-to-p order. Obviously, this is then true for all levels $n \geq 0$. In addition, as the kernels of the maps $G_{n+1} \to G_n$ are p-groups, for each $i = 1, \ldots, r$, C_{ni} has the same order as C_{0i} ($n \geq 0$). But then, it follows from the Lifting Lemma (lemma 2.7) that the conjugacy classes $C_{n1}, \ldots, C_{nr}$ are the unique lifts of the conjugacy classes $C_{01}, \ldots, C_{0r}$ of G (respectively), *i.e.*, with the notation of §2.3, $C_{ni} = C_{0i}^n$, $i = 1, \ldots, r$, $n \geq 0$. Setting $\mathbf{C} = (C_{0i}, \ldots, C_{0r})$, we have obtained that there are K-rational points on each level of the stack tower $\mathcal{H}_r(G_0, p, \mathbf{C})$. □

Remark 3.8. If the starting realizations of the groups G_n are by G-covers with field of moduli K (but not necessarily defined over K), the conclusion of theorem 3.5 holds with the stack tower $\mathcal{H}_r(G_0, p, \mathbf{C})$ replaced by the modular tower $\mathsf{H}_r(G_0, p, \mathbf{C})$. The proof is the same; just note that the Branch Cycle Lemma holds under the more general "field of moduli" assumption. Finally we have this result of M. Fried [Fri02, theorem 2.10]: if G_0 is p-perfect and has trivial center, than so do all the G_n. So then, at each level, the field of moduli is a field of definition [DD97]. The same Fried's result has this further conclusion: suppose p divides the order of $g \in G_k$. Then, any lift $\tilde{g} \in G_{k+1}$ has order p times the order of g. This is more precise than the argument we used in the proof above to show that the order of g_n tends to ∞.

3.4. **Moduli space and stack versions of the MT conjecture.** Notation is that of §3.1.

Theorem 3.9. *The moduli space and stack versions of the MT diophantine conjecture are equivalent in Fried's original context. They also are equivalent in the more general context from §2.2 if the dependence in K of the constants involved is through $[K : \mathbb{Q}]$.*

Proof. For the first part, we refer to [Fri06, proposition 3.3 and remark 3.4], [Fri08, appendix C] and [Kim05]. Here is a sketch of the method. Start from a modular tower $\mathsf{H}(-)$ with levels corresponding to the characteristic quotients G_n of the p-universal Frattini cover of some p-perfect G_0. The main point is that a p-perfect group G_0 has a quotient $\overline{G}_0$ such that the characteristic quotients $\overline{G}_n$ of the p-universal Frattini cover of $\overline{G}_0$ have trivial center. This makes it possible, using the natural epimorphisms $G_n \to \overline{G}_n$, to construct a modular tower $\overline{\mathsf{H}}(-)$, with the property that the levels, which correspond to the groups $\overline{G}_n$, are fine moduli spaces. Thus under the MT diophantine conjecture for stacks, rational points over some number field K disappear beyond a certain

level of the modular tower $\overline{\mathsf{H}}(-)$. This property holds *a fortiori* for the modular tower $\mathsf{H}(-)$ as $\overline{\mathsf{H}}(-)$ is a quotient of $\mathsf{H}(-)$.

For the second part, we refer to [CD07, appendix]. □

3.5. **Original and reduced forms of the MT conjecture.** Notation is that of §3.1.

Proposition 3.10. *The reduced MT Diophantine Conjecture is equivalent to the original form if the dependence in K of the constants involved is through $[K:\mathbb{Q}]$.*

Proof. The proof follows from [Cada, corollary 3.12] (§1.6 (**)). □

4. Galois Covers, Abelian Varieties and Modular Towers

This section reproduces parts of the paper [CD07] by A. Cadoret and the author. In addition to the material of this Summer School, are used some classical results from the theory of abelian varieties and Jacobian varieties. References are given.

The central idea 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 $\mathrm{Jac}(X)$. This leads to interesting conclusions in the context of modular towers.

Unless otherwise specified, fields are of arbitrary characteristic. The separable closure of a field k is denoted by k^{s} and its absolute Galois group by $\mathrm{Gal}(k^{\mathrm{s}}/k)$.

The following definition is used throughout the section. Suppose given a field F with a discrete valuation v with valuation ring R and a F-curve B [13] with a model B_R over $\mathrm{Spec}(R)$ with good reduction.

Definition 4.1. A proper closed subset $D \subset B_{\overline{F}}$ is said to be *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}.

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

For $B = \mathbb{P}^1$, this last condition can be rephrased more explicitly: View $\mathbb{P}^1_{F^{\rm s}}$ as the t-line and consider two geometric points $\alpha = (t = a)$ and $\alpha' = (t = a')$, where $a, a' \in F^{\rm s} \cup \{\infty\}$. Then α, α' coalesce at a prime $\mathfrak{p}^{\rm s}$ of $R^{\rm s}$ over $\mathfrak{p}$ if $|a|_{\mathfrak{p}^{\rm s}} \leq 1$, $|a'|_{\mathfrak{p}^{\rm s}} \leq 1$, and $|a - a'|_{\mathfrak{p}^{\rm s}} < 1$, or else if $|a|_{\mathfrak{p}^{\rm s}} \geq 1$, $|a'|_{\mathfrak{p}^{\rm s}} \geq 1$, and $|a^{-1} - a'^{-1}|_{\mathfrak{p}^{\rm s}} < 1$. 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.

4.1. **Central Results.**

4.1.1. *Statements.*

Theorem 4.2. *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 $k^{\rm s}$-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 $e_1, \dots, e_r$ of f and $P^{\rm ab}$ is its abelianization, then we have*

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

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

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 4.2 that $|P^{\rm ab}|$ 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 4.3. *Let $m_0 \geq 1$ and $r \geq 0$ 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 $e_1, \dots, e_r$ of f and of index $[G : P] \leq m_0$, then the order of its abelianization $P^{\rm ab}$ 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 $P^{\rm ab}$, 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.

4.1.2. *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 $P^{\rm ab}$ is $\geq p$ (and even $\geq p^2$ if $|P| \geq p^2$). 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 4.3 predicts that p^n should be bounded in terms of r, $m = [G : P]$ and K. Theorem 4.2 yields the following.

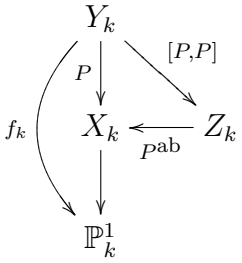
Corollary 4.4. *The branch divisor of f is singular modulo every prime $\ell \not| |G|$ such that $\mathrm{e}\,(2\sqrt{\mathrm{e}}\,\gamma)^{m-1}\,\ell^{\gamma[K:\mathbb{Q}]} < p^n$ [14], where $\gamma = 1+m(r-2)/2$. This includes at least one prime ℓ if p^n is bigger than some constant depending only on r, m and $[K : \mathbb{Q}]$.*

For instance, if $|G| = 3\,.\,97^N$ with $N \geq 2$, 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. The modular tower context will provide other more structured examples.

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 4.4 is a new constraint.

4.1.3. *Proof of theorem 4.2.* 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

[14] 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 4.2 independent of the place v above ℓ. That is why we may use primes of $\mathbb{Q}$ here.

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} [Cadb, lemma 1.4] [15]; 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 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 $[G:P]$ [16]. The value of g given in the statement comes from the Riemann-Hurwitz formula. □

4.1.4. *The conjecture for $r = 3$.* The case $r \leq 2$ is trivial both in theorem 4.2 and in conjecture 4.3. From now on we will always assume $r \geq 3$. We consider here the case $r = 3$.

Corollary 4.5. *Conjecture 4.3 with $P \subset G$ a p-subgroup holds for 3 branch point covers.*

Using a stronger form of theorem 4.2, the restriction "with $P \subset G$ a p-subgroup" can be removed: conjecture 4.3 with P any subgroup of G holds for 3 branch point covers (see [CD07]).

Proof. Let $f : Y \to \mathbb{P}^1$ be a G-cover as in the statement of conjecture 4.3 with at most 3 branch points. These branch points are defined over an extension K_0/K of degree ≤ 6. Up to composing f with a linear fractional transformation defined over K_0, one may assume they are 0,

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

[16] 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 $|\overline{\mathrm{Jac}(X_k)}(\mathbb{F}_q)| \leq (q+1+2\sqrt{q})^g$ is better than this one; it can be used alternatively.

1 or ∞. Let $P \subset G$ be a p-subgroup with p not dividing any of the ramification indices $e_1, \ldots, e_r$ and of index $\leq m_0$. Pick a prime $\ell \neq p$ bigger than m_0. Thus ℓ does not divide $|G|$. Theorem 4.2 applies with $k = \mathbb{Q}_\ell K_0$ to give $|P^{\mathrm{ab}}| \leq e\,(2\sqrt{e}\,\gamma)^{m_0-1}\,\ell^{6\gamma[K:\mathbb{Q}]}$ with $\gamma = 1+m_0/2$. $\square$

4.2. **Torsion of abelian varieties.** A central point of the proof of theorem 4.2 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 $e_1, \ldots, e_r$ of f, then a K-curve X_K of genus $g = 1+\frac{1}{2}[G:P](r-2-\sum_{i=1}^r 1/e_i) \geq 1$ 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}.*

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 $g \geq 1$ 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.

Proposition 4.6. *The Torsion Conjecture implies conjecture 4.3. The p-Torsion Conjecture implies the weaker form of conjecture 4.3 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.*

The Torsion Conjecture is known in the case $g = 1$, *i.e.* for elliptic curves: this is the Mazur-Merel theorem; furthermore, the constants involved only depend on $[K:\mathbb{Q}]$.

4.3. **Application to the MT conjecture.** Let $\widetilde{G} \to G_0$, r and $\mathbf{C}$ be as in §3.1.

4.3.1. *The weak MT Conjecture.* As a consequence of theorem 4.2, we obtain the following results.

Corollary 4.7 (weak MT Realization Conjecture)**.** *Let $r \geq 0$ 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 4.2 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). □

In modular terms, corollary 4.7 restates as follows.

Corollary 4.8 (weak MT Diophantine Conjecture)**.** *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*

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

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

Assume for every $n \geq 0$ there is a G-cover $f_n : Y_n \to \mathbb{P}^1$ as in corollary 4.7 but with some number field as field of moduli (the same for each n, or, more generally, with a uniformly bounded degree). Corollary 4.7 yields this conclusion, which will be refined later (see corollary 4.13):

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 4.3 provides a stronger conclusion than theorem 4.2.

Corollary 4.9. *Conjecture 4.3 (and more precisely its version with $P \subset G$ a p-subgroup and a constant possibly depending on p), implies the MT Diophantine Conjecture (both for stacks and moduli spaces) and so also the MT Realization Conjecture.*

Proof. Consider as above the p-subgroup $P = \widetilde{P}/\widetilde{P}_n$ of $G = \widetilde{G}/\widetilde{P}_n$ and apply conjecture 4.3 with $m_0 = |G_0|$. As $|P^{\mathrm{ab}}| \geq p^n$, 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 then follows from the Fried-Kopeliovich theorem (corollary 3.6) and theorem 3.9). □

Remark 4.10 (dependence in K). If the constant involved in conjecture 4.3 only depends on K through $[K : \mathbb{Q}]$, then we have this stronger conclusion for the MT Realization Conjecture: given an integer $d \geq 1$, only finitely many groups G_n can be regularly realized with at most r branch points over some number field of degree $\leq d$. This requires the version of the Fried-Kopeliovich theorem that we proved in §3.3 for which the base field K is a field of characteristic 0 with a cyclotomic closure of infinite degree: the field K can then be taken to be the compositum $\mathbb{Q}(d)$ of all number fields of degree $\leq d$ [17].

Corollary 4.11. *The MT Realization Conjecture holds in each of these situations:*

(a) *if the p-Torsion Conjecture holds,*

(b) *for covers with at most 3 branch points,*

(c) *in the Dihedral Group situation with $r \leq 5$. In other words, the Dihedral Group Conjecture holds for $r \leq 5$.*

Proof. (a) follows from corollary 4.9 and proposition 4.6, (b) from corollary 4.9 and corollary 4.5. Consider the dihedral group situation from §2.4 with $r \leq 5$. Assume each dihedral group D_{p^n} is regularly realized with $r \leq 5$ branch points. From the Fried-Kopeliovich theorem (theorem 3.5), one may restrict to the case that all inertia classes $C_1, \dots C_r$ are the involution class. Observe then that $r \neq 2$ (D_{p^n} not cyclic) and $r \neq 3, 5$ (an odd product of involutions of D_{p^n} cannot be 1). Thus $r = 4$ but then the genus of the curve X_K from §4.2 (*) is $g = 1$, and in this case, the Torsion Conjecture is known[18]. □

[17] Indeed the Galois group of the Galois closure of any number field k of degree d is of order $\leq d!$ and so the Galois group $\mathrm{Gal}(\mathbb{Q}(d)/\mathbb{Q})$ is a $(d!)!$-torsion group. Therefore the cyclotomic closure $\mathbb{Q}(d)^{\mathrm{cycl}}$ is an infinite degree extension of $\mathbb{Q}(d)$, for otherwise the Galois group $\mathrm{Gal}(\mathbb{Q}(d)^{\mathrm{cycl}}/\mathbb{Q})$ would be a torsion group and the same would then be true of the Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{cycl}}/\mathbb{Q})$.

[18] More explicitly: using the correspondence from §2.4, the starting realization of D_{p^n} yields some elliptic curve E defined over K with a K-rational point of order p^n on E, which, from the Mazur-Merel theorem cannot exist if $p^n > 7$.

4.3.2. *The weak reduced MT Conjecture.* Given a field F (of characteristic 0) with a discrete valuation v, we say that a proper closed subset $D \subset \mathbb{P}^1_F$ 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 MT Conjecture (corollary 4.7).

Corollary 4.12 (weak reduced MT Conjecture)**.** *Let $\widetilde{G} \to G_0$, r and $\mathbf{C}$ 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 $\mathsf{H}^{\equiv}_r(\widetilde{G} \to G_0, p, \mathbf{C})$ 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 [Cada, corollary 3.12] (§1.6 (**)), 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 $t_1, \dots, t_r$, over some extension k_0/k of degree $\le d(r)$. If χ is some linear fractional transformation such that $\{0, 1, \infty\} \subset \{\chi(t_1), \dots, \chi(t_r)\}$, 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 4.7 that $\chi(D)$ is singular at v. □

Further implications to the MT Conjecture are collected in this result.

Corollary 4.13 (weak reduced MT Conjecture (continued))**.** *Let $\widetilde{G} \to G_0$, r and $\mathbf{C}$ be as above and K be a number field. Assume the PGL_2-reduced modular tower $\mathsf{H}^{\equiv}_r(\widetilde{G} \to G_0, p, \mathbf{C})$ 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 $\ell \in S$ ($m \ge 0$). 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 ($n \geq 0$). 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 $\Psi^{\equiv} : \mathsf{H}^{n,\equiv}(K) \to \mathbb{P}^1(K) \setminus \{0,1,\infty\}$ [19] *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 4.14. 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] [Cadb]. The case $r = 4$ has been thoroughly studied by Fried [BF02], [Fri06]. A proof of the MT Diophantine Conjecture in this case has recently been announced by the first author and A. Tamagawa [CT07].

Proof. (a) Let S be a finite set of primes $\ell \not| p|G_0|$. Apply corollary 4.12 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 $m \geq 0$ and a finite set S of primes $\ell \not| p|G_0|$. Use (a) to consider an integer $n \geq m$ 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 4.12 and the definition of bad reduction for some set $\{0, 1, \infty, \lambda\}$. □

4.4. **ℓ-adic points on Harbater-Mumford modular towers.** Corollary 4.7 asserts there is necessarily bad reduction of the branch divisor

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

of covers corresponding to rational points over a henselian field k on 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. We explain below that, under some assumptions, the answer is positive, and even more is true, namely, there exist projective systems of k-rational points.

As before fix a finite group G_0, a prime divisor p of $|G_0|$ and an unordered r-tuple $\mathbf{C} = \{C_1, \dots, C_r\}$ of conjugacy classes of G_0 of prime-to-p order such that $\mathrm{sni}(G_0, \mathbf{C})^\bullet \neq \emptyset$. Assume further that $\mathbf{C}$ is of H(arbater)-M(umford) type, *i.e.* has the shape $(C_1, C_1^{-1}, \dots, C_s, C_s^{-1})$.

Fix a henselian field k (for a rank 1 valuation) of characteristic 0, of residue characteristic $\ell \geq 0$ and containing all N-th roots of 1 with N the l.c.m. of the orders of $C_1, \dots, C_s$, *e.g.* $k = \mathbb{Q}_\ell(\zeta_N)$ or $k = \mathbb{Q}(\zeta_N)((x))$ where $\zeta_N = \exp(2i\pi/N)$.

Theorem 4.15. *There exist projective systems of k-rational points on the associated modular stack tower $\mathcal{H}_r(G_0, p, \mathbf{C})$.*

Comments on proof. The proof is given in a bigger generality in [DD04]. It consists in constructing a tower $(K_n)_{n\geq 0}$ of regular Galois extensions of $k(T)$ that realizes the projective system $(G_n)_{n\geq 0}$ of characteristic quotients of $\widetilde{G} = {}^p\tilde{G}_0$. For each level n of the tower, patching methods can be used. However it should be done in such a way that the invariants of the extensions $K_n/k(T)$ (branch points, ramification type) be compatible all along the tower. This however does not guarantee that the extensions themselves are compatible. The strategy is to throw in further constraints on the required realizations so as to leave only finitely many possibilities (but at least one) for the extensions $K_n/k(T)$ ($n \geq 0$): we request that the fiber above some fixed unramified point $t_0 \in \mathbb{P}^1(k)$ in every extension $K_n/k(T)$ consist only of k-rational points. That is what makes "passing to infinity" possible, *via* the classical compactness argument (a projective limit of non-empty finite sets is non-empty).

We note a condition of importance that makes the construction possible and which is satisfied in the modular tower context:

(*) for each $i = 1, \dots, n$, the conjugacy classes C_i^n, $n \geq 0$ have the same (prime-to-p) order.

The Branch Cycle Lemma (lemma 3.7) shows this kind of asssumption cannot be removed in general: the classical example is the profinite group $\mathbb{Z}_p$ which is not the Galois group of a regular Galois extension $E/\mathbb{Q}_\ell(T)$ (see e.g. [Dèb07, ch.3]). In the construction from [DD04], this obstruction corresponds to Hypothesis (iii) there. We refer to [Cadb]

for a thorough study of similar obstructions and the proof of a wide class of profinite groups not being regular Galois groups over $k(T)$.

Furthermore, ζ_N being in k makes it possible to choose the branch points in $\mathbb{P}^1(k)$. Condition (*) above also guarantees Hypothesis (iv) of the general construction: if $\ell > 0$, the ℓ-part of the orders of the classes C_i^n, $i = 1, \dots, r$, $n \geq 0$ is bounded. This makes it possible to choose the branch points organized in pairs of sufficiently close points, as requested by the patching methods. □

Consider the modular tower $\mathsf{H}_r(G_0, p, \mathbf{C})$ from theorem 4.15. The varieties H_n are reducible in general. A next motivation is to obtain a similar result but with the H_n geometrically irreducible and defined over $\mathbb{Q}$ ($n \geq 0$). This was achieved in [DE06].

Recall first these definitions. An unordered tuple $\mathbf{C} = \{C_1, \dots, C_r\}$ of conjugacy classes of a group G is said to be *g-complete* if it satisfies "$g_i \in C_i$, $i = 1, \dots, r \Rightarrow \langle g_1, \dots, g_r \rangle = G$". A tuple $\mathbf{C}$ with the shape $\{C_1, C_1^{-1}, \dots, C_s, C_s^{-1}\}$ is *HM-g-complete* if it has this property: if any pair C_i, C_i^{-1} is removed then what remains is g-complete.

Theorem 4.16. *In addition to the assumptions of theorem 4.15, suppose* $\mathbf{C}$ *is HM-g-complete and is* $\mathbb{Q}$*-rational (§1.2). Then there exists a projective system* $(\mathrm{HM}_n)_{n\geq 0}$ *of* $\mathbb{Q}$*-components of* $(\mathsf{H}_n)_{n\geq 0}$ *(respectively) with the following property:*

If k *is any henselian field of characteristic* 0*, of residue characteristic* $\ell \geq 0$ *and containing all* N*-th 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 tower* $(\mathrm{HM}_n)_{n\geq 0}$*.*

Comments on proof. The key is to take for HM_n the *Harbater-Mumford component* of H_n. Recall it is defined as the component of all points representing complex covers with the property that some of its monodromy branch cycle descriptions (relative to some standard topological bouquet of paths) are of the form $(g_1, g_1^{-1}, \dots, g_s, g_s^{-1})$. It is a theorem of M. Fried that if $\mathbf{C}$ is HM-g-complete, all these covers fall into a single component [Fri95, theorem 3.21]. Furthermore using Wewers' description of the boundary of Hurwitz spaces [Wew98], this HM-component can be characterized by the way the covers it carries degenerate: their stable reduction should be a cover of a "comb" of $\mathbb{P}^1$s unramified at singular points [DE06]. It follows this component is defined over $\mathbb{Q}$. We also use this characterization to show that the ℓ-adic covers constructed thanks to the patching methods in [DD04] lie on this HM-component. □

Finally one would like to have an analog of theorem 4.16 with the r-dimensional varieties HM_n replaced by varieties of low dimension. Such results have been obtained by A. Cadoret [Cad05]. The new varieties are obtained as subvarieties of the HM-components HM_n by specializing all branch points but one or two; thus they are curves or surfaces. The main problem is to preserve irreducibility, which amounts to checking an intricate transitivity condition of some braid group action. This can be achieved with some restriction on the group G. For example, she obtains the following result.

Theorem 4.17. *Let G be a finite non-abelian simple group and let p and ℓ be two primes with p dividing $|G|$ and ℓ not dividing $|G|$. Assume there is a g-complete couple (C, D) of conjugacy classes of G of prime-to-p order. Let μ be the l.c.m. of the orders of C and D and let ζ_μ be a primitive μ-th root of 1. Then one can construct*

- unordered r-tuples $\mathbf{C} = \{C_1, C_1^{-1}, \dots, C_s, C_s^{-1}\}$ made of repetitions of the classes C and D,

- degree $r-1$-divisors $\mathbf{t} \in \mathsf{U}_{r-1}(\mathbb{Q})$,

such that on the modular tower $\mathsf{H}(G_0, p, \mathbf{C})$, there is, above the sublocus of U_r of degree r divisors with $r-1$ entries in $\mathbf{t}$, a projective system $(\mathcal{C}_{\mathbf{t},n})_{n\geq 0}$ of curves, geometrically irreducible and defined over $\mathbb{Q}(\zeta_\mu)$, with projective systems of $\mathbb{Q}_\ell(\zeta_\mu)$-rational points on it.

The assumptions on G are satisfied for quite a few simple groups: alternating groups A_p with $p \geq 5$ prime, $p \neq \ell$, Mathieu groups M_{11}, M_{22}, M_{23}, Janko groups J_2, J_3, the Suzuki group $Sz(8)$, the groups $\mathrm{PSL}_2(\mathbb{F}_p)$ with $p \equiv 3$ [mod 4].

4.5. **Generalization of the central theorem.** We give here a generalization[20] of theorem 4.2 where we let the base space of the cover f be a more general curve B than $\mathbb{P}^1$ and drop the assumption that the ramification indices are prime to $|P|$. The bound we obtain depends on the index $[G : P]$ of the subgroup $P \subset G$, the number r of branch points, the genus g_B of B and the order q of the residue field.

Theorem 4.18. *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 B a k-curve of genus g_B with good reduction and $f : Y \to B$ be a k^{s}-G-cover of group G, field of moduli k and branch divisor smooth at v. Then there exists a constant $C(m, r, q, g_B)$ such that if P is any subgroup of G and P^{ab} is its abelianization, we have*

$$|P^{\mathrm{ab}}| \leq C([G : P], r, q, g_B)$$

[20] An even more general version is given in [CD07].

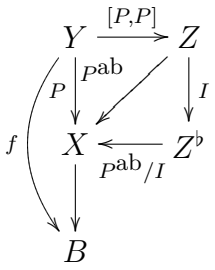
The special case with $G = P$ abelian yields the following.

Corollary 4.19. *Let k be as above and B be a k-curve with good reduction. Then only finitely many abelian groups with prime-to-ℓ order occur as the Galois group of some k-G-cover of B with r branch points.*

Using results of Clark-Xarles [CXar], the prime-to-ℓ condition on $|G|$ can be removed if k is of characteristic 0 [Cad07].

Proof of theorem 4.18. From [Ems99], which generalizes [DH98], it remains true that, due to the assumptions $(q, |G|) = 1$ and "branch divisor smooth at v", the field of moduli of f is a field of definition. So we may just as well assume that $f : Y \to B$ is a k-G-cover.

Similarly as in the proof of theorem 4.2, factor $f : Y \to B$ as follows:



with $I \subset P^{\mathrm{ab}}$ the subgroup generated by all inertia subgroups of $Z \to X$. 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.

The same reduction argument as for theorem 4.2 leads to

$$|P^{\mathrm{ab}}|/|I| \leq [q + 1 + 2\sqrt{q}]^g$$

where $g = 1 + \frac{1}{2}[G : P](r + 2g_B - 2 - \sum_{1 \leq i \leq r} 1/e_i)$ is the genus of X. Here we have used Weil's bounds (rather than those from Lachaud and Martin-Deschamps).

It remains to bound $|I|$. Using that the group I is an abelian quotient of the fundamental group of the curve $Z^\flat$ with the ramification points of $Z \to Z^\flat$ removed, we obtain

$$|I| \leq \exp(I)^{2g_{Z^\flat} + rD}$$

where $D = [G : P]\,|P^{\mathrm{ab}}|/|I|$, $\exp(I)$ is the exponent of I and $g_{Z^\flat}$ is the genus of $Z^\flat$. Using the Riemann-Hurwitz formula, the genus $g_{Z^\flat}$ can be bounded by a constant γ depending only on r, g_B and D.

We explain next how to bound, for each prime p, the p-part, say p^{n_p}, of $\exp(I)$. Fix a prime p. For each point $\mathfrak{p} \in Z^\flat(k^{\mathrm{sep}})$ above some branch point t_i of f $(i = 1, \ldots, r)$, let $I_{\mathfrak{p}}$ be some inertia group of $Z \to$

$Z^\flat$ above $\mathfrak{p}$, and write its order $|I_\mathfrak{p}| = p^{n_p(\mathfrak{p})} m_p(\mathfrak{p})$ with $(p, m_p(\mathfrak{p})) = 1$. The group I is generated by all the subgroups $I_\mathfrak{p}$ and the p-Sylow subgroup $I[p^\infty]$ of I is generated by the subgroups $I_\mathfrak{p}^{m_p(\mathfrak{p})}$. In particular, there exists a point $\mathfrak{p}$ such that $I_\mathfrak{p}^{m_p(\mathfrak{p})}$ and $I[p^\infty]$ have the same exponent, that is $p^{n_p(\mathfrak{p})} = p^{n_p}$. Write then $I[p^\infty] = I_\mathfrak{p}^{m_p(\mathfrak{p})} \oplus N$ and consider the quotient covers: $f_1 : Z_1 = Z/(\oplus_{q \neq p} I[q^\infty]) \to Z^\flat$ of group $I[p^\infty]$ and $f_2 : Z_2 = Z_1/N \to Z^\flat$ of group $I_\mathfrak{p}^{m_p(\mathfrak{p})}$. The cover f_2 is totally ramified above $\mathfrak{p}$ and so the residue fields at $\mathfrak{p} \in Z^\flat$ and at the unique point on Z_2 above $\mathfrak{p}$ are equal. Lemma 4.20 below shows that this residue field contains the $p^{n_p(\mathfrak{p})}$-th roots of 1. It follows that $p^{n_p} \mid q^{\overline{D}} - 1$ where $\overline{D}$ is the degree of that residue field over k. Bound $\overline{D}$ by $rD = r[G : P]\,|P^{\mathrm{ab}}|/|I|$ and use the bound for $|P^{\mathrm{ab}}|/|I|$ from the first part of the proof. □

Lemma 4.20. *Let k be any field, X be a k-curve and $f : Y \to X$ be a G-cover defined over k and tamely ramified at a point $P \in X$ with ramification index e. Let $Q \in Y$ be a point in the fiber above P. Then the residue field of $Q \in Y$ contains the e-th roots of unity.*

Proof. The following proof is given in [Cadb]. Denote by $\widetilde{k(X)}_P$ (resp. $\widetilde{k(Y)}_Q$) the completion of the function fields $k(X)$ at P (resp. $k(Y)$ at v). The extension $\widetilde{k(Y)}_Q / \widetilde{k(X)}_P$ is Galois with group the decomposition group of $f : Y \to X$ at Q. Denote the fixed field of the corresponding inertia group I_Q in $\widetilde{k(Y)}_Q$ by $\widetilde{k(X)}_P^{\mathrm{ur}}$. The extension $\widetilde{k(Y)}_Q / \widetilde{k(X)}_P^{\mathrm{ur}}$ is totally ramified. In particular, the associated residue field extension at Q is trivial. Denote by κ the residue field of $Q \in Y$.

We claim that there exists $y \in \widetilde{k(Y)}_Q$ such that $y^e \in \widetilde{k(X)}_P^{\mathrm{ur}}$ and $\widetilde{k(Y)}_Q = \widetilde{k(Y)}_Q / \widetilde{k(X)}_P^{\mathrm{ur}}(y)$. Indeed, let a and b be some uniformizing parameters of the places/points P and Q respectively. Then we have $b^e = wa$ for some unit $w \in \widetilde{k(Y)}_Q$ relative the place/point Q (in other words, the value $w(Q)$ of w at Q in the residue field κ is non-zero). From above, κ is also the residue field of the restriction of the place/point Q to $\widetilde{k(X)}_P^{\mathrm{ur}}$. So up to replacing w by $u^{-1}w$ with $u \in \widetilde{k(X)}_P^{\mathrm{ur}}$ such that $w(Q) = u(Q)$, one may assume $w(Q) = 1$. Then, applying Hensel's lemma to $X^e - w$ produces an element $w_0 \in \widetilde{k(Y)}_Q$ such that $w_0^e = w$ and then $y = w_0^{-1} b$ has the expected property. Consequently $\widetilde{k(Y)}_Q$ contains the e-th roots of unity, hence so does κ. □

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.

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

[Cadb] Anna Cadoret. On the profinite regular inverse Galois problem. *Publ. R.I.M.S.*, to appear.

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

[Cad05] Anna Cadoret. Harbater-mumford subvarieties of moduli spaces of covers. *Math. Ann.*, 333, No. 2:355–391, 2005.

[Cad07] Anna Cadoret. A boundedness result for G-covers of curves. *preprint*, 2007.

[CD07] Anna Cadoret and Pierre Dèbes. Abelian constraints in inverse galois theory. *preprint*, 2007.

[CT07] Anna Cadoret and Akio Tamagawa. Uniform boundedness of p-primary torsion on abelian schemes. *preprint*, 2007.

[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.

[DE06] Pierre Dèbes and Michel Emsalem. Harbater-mumford components and Hurwitz towers. *J. Math. Inst. Jussieu*, 5(3):351–371, 2006.

[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.

[Dèb07] Pierre Dèbes. Arithmétique des revêtements de la droite. 2007. at http://math.univ-lille1.fr/˜pde/ens.html.

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

[DF08] Pierre Dèbes and Michael D. Fried. Arithmetic of covers and Hurwitz spaces definitions. 2008. at http://math.uci.edu/ mfried/deflist-cov.html.

[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.

[Fri78] Michael Fried. Galois groups and complex multiplication. *Trans. Amer. Math. Soc.*, 235:141–163, 1978.

[Fri80] Michael D. Fried. Exposition on an arithmetic-group theoretic connection via riemann's existence theorem. In *The Santa Cruz conference on finite groups*, volume 37 of *Proc. Sympos. Pure Math.*, pages 571–602. Amer. Math. Soc., Providence, RI, 1980.

[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.

[Fri02] Michael D. Fried. Moduli of relatively nilpotent extensions. In *Communications in Arithmetic Fundamental Group*, volume 1267 of *Inst. of Math. Science Analysis*, pages 70–94. RIMAS, Kyoto, Japan, 2002.

[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.

[Fri08] Michael D. Fried. Connectedness of families of sphere covers of a_n-type. *Preprint*, 2008.

[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.

[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.

[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: Pierre.Debes@math.univ-lille1.fr

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