Modular Towers
Construction and Diophantine Questions

Pierre Dèbes

Abstract. Modular towers, a notion due to M. Fried, are towers of Hurwitz spaces, with levels corresponding to the characteristic quotients of the p-universal Frattini cover of a fixed finite group G (with p a prime divisor of $|G|$). The tower of modular curves $X^1(p^n)$ ($n>0$) is the original example: the group G is then the dihedral group D_p. There are diophantine conjectures on modular towers, inspired by modular curves: the spirit is that over a number field, rational points do not exist beyond a certain level. In this paper, which is the first of a series of three on this topic in this volume, after defining modular towers, we discuss the significance of these conjectures and explain some known results.

Contents

Modular towers, which are due to M. Fried, constitute a vertical development of the Hurwitz space theory. A modular tower is a tower of moduli Hurwitz spaces $(\mathcal{H}_{G_n}(\mathbf{C}_n))_{n\geq 0}$ (with maps going down) where the branch point number $r \geq 3$ is fixed and the projective sequence $(G_n, \mathbf{C}_n)_{n\geq 0}$ of groups G_n given with an r-tuple $\mathbf{C}_n$ of conjugacy classes comes from a universal construction associated to a fixed finite group G given with r conjugacy classes. The motivating example is the tower of modular curves $(X^1(p^n))_{n>0}$: the group G is then the dihedral group D_p given with the involution class repeated 4 times. The foundations of the modular tower theory and the main dihedral group example are recalled in the first part of the paper. There is an important group-theoretic aspect which is further developed in Semmen's paper [Se] in this volume.

Persistence of rational points on levels $\mathcal{H}_{G_n}(\mathbf{C}_n)$ is the main diophantine question on modular towers. It corresponds to the possibility of realizing regularly all groups G_n with a bounded number of branch points. The dihedral group example suggests that there are deep diophantine obstructions when the base field is a number field. On the other hand, over ℓ-adic fields, the tendancy is the opposite. The second part of the paper focuses on these diophantine questions. After stating and discussing the main conjectures, we give a proof (based on the original papers) of some significant results of Fried-Kopeliovich and Bailey-Fried in the number field case. In particular we pave the way to the proof of the main diophantine conjecture in the special case of $r = 4$ branch point covers. The missing stage is outlined in Fried's paper [Fr4] in this volume. A final section is devoted to the similar questions over ℓ-adic fields. We describe some recent results due to Cadoret, Deschamps, Emsalem and the author.

We conclude this introduction with a seemingly unrelated example which was yet the first step of the modular tower theory.

The original Fried-Serre example. Take $G = A_n$ and $\underline{\sigma} = (\sigma_1, \ldots, \sigma_r)$ an r-tuple of 3-cycles generating A_n and such that $\sigma_1 \cdots \sigma_r = 1$. Let

$$1 \to \{\pm 1\} \to \widetilde{A}_n \to A_n \to 1$$

be the unique non-split degree 2 extension of A_n. Each 3-cycle $\sigma \in A_n$ has a unique lift $\widetilde{\sigma} \in \widetilde{A}_n$ of order 3. The *lifting invariant* $\widetilde{\sigma}_1 \cdots \widetilde{\sigma}_r$ is ± 1. Serre asked whether it is 1 or -1, initially in case $n = 5$, $r = 4$. Fried offered the following answer: the lifting invariant is constant because the Hurwitz monodromy group H_r leaves the lifting invariant unchanged

(a straightforward observation) and acts transitively on tuples $\underline{\sigma}$ (an easy check). As it is obviously 1 for $\underline{\sigma}$ of the form $(\sigma, \sigma^{-1}, \tau, \tau^{-1})$, it is always 1.

More generally the lifting invariant depends only on the H_r-orbit of $\underline{\sigma}$, thus defining an invariant of the corresponding component of the associated Hurwitz space. It can be used to distinguish between two such components. For example, if there is a unique component with lifting invariant 1, it is defined over $\mathbb{Q}$; see §1.4.

Fried checked that there are 1 or 2 components (depending on whether $g = r + 1 - n$ is 0 or not). In the latter case, they have distinct lifting invariant so are both defined over $\mathbb{Q}$. In the former ($n = r + 1$ *e.g.* $n = 5$, $r = 4$), the whole Hurwitz space is defined over $\mathbb{Q}$ (and the invariant is 1 if (and only if) n is odd). See [Fr1], [Ser1], [Ser2] for more on this example.

This example shows a basic idea of modular towers: for studying Hurwitz spaces $\mathcal{H}_G$, it is interesting to consider extensions $\widetilde{G} \twoheadrightarrow G$ and the associated Hurwitz spaces $\mathcal{H}_{\widetilde{G}}$. The modular tower theory focuses on special extensions though: those that have the Frattini property (as the extension $\widetilde{A}_n \to A_n$ does).

1. Construction and motivations

1.1. p-universal Frattini cover and lifting lemma. Given a finite group G and a prime divisor p of $|G|$ [1], denote the universal p-Frattini cover of G by ${}_p\tilde{G}$.

Recall (see [FrJa] for more details) that a surjective group homomorphism (a group cover) $\psi : H \to G$ is said to be a Frattini cover if for each subgroup H' of H, $\psi(H') = G \Rightarrow H' = H$, or, equivalently, if its kernel is contained in every maximal subgroup of G. For example, the homomorphism $\mathbb{Z}/(p_1^{\alpha_1} \cdots p_r^{\alpha_r})\mathbb{Z} \to \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$ is a Frattini cover $(\alpha_1, \ldots, \alpha_r > 0)$. There is a universal object for Frattini covers of a given group G. It is denoted by $\tilde{G}$ and can be shown to be a projective profinite cover of G [FrJa] proposition 20.33]. For example, for $G = \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$, we have $\tilde{G} = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$. There also exists a universal object for Frattini covers $\psi : H \to G$ of G with kernel a p-group. This group is called the universal p-Frattini cover of G and is denoted by ${}_p\tilde{G}$. It is a profinite group of rank equal to rank(G) which has this p-projectivity property: every embedding problem for ${}_p\tilde{G}$ with a p-group kernel has a weak solution [BaFr] p.117. As a consequence, its p-Sylows are projective, hence are free pro-p groups (by [FrJa] proposition 20.37) of finite

[1] From the Schur-Zassenhaus lemma and the Frattini property, for p not dividing $|G|$ there is no non-trivial Frattini cover of G with p-group kernel, making this case uninteresting.

rank (by Nielsen-Schreier [FrJa] corollary 15.28). For example, for $G = \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$, we have ${}_{p_1}\tilde{G} = \mathbb{Z}_{p_1} \times \mathbb{Z}/p_2\mathbb{Z} \cdots \times \mathbb{Z}/p_r\mathbb{Z}$.

One then defines, from the kernel ker of the homomorphism ${}_p\tilde{G} \to G$, a sequence of characteristic subgroups of ${}_p\tilde{G}$:

$$\ker_0 = \ker,\ \ker_1 = \ker_0^p[\ker_0, \ker_0], \ldots,\ \ker_n = \ker_{n-1}^p[\ker_{n-1}, \ker_{n-1}], \ldots$$

and for each $n \geq 0$, one denotes by ${}^n_p\tilde{G}$ the quotient ${}_p\tilde{G}/\ker_n$. Kernels $\ker_n$ are free pro-p groups of ${}_p\tilde{G}$ of finite rank and groups ${}^n_p\tilde{G}$ are finite (from [FrJa] Lemma 20.36, $\ker_{n-1}/\ker_n$ is isomorphic to $\mathbb{F}_p^m$ with $m = \mathrm{rank}(\ker_{n-1})$) of rank $\leq \mathrm{rank}(G)$. For example, for $G = \mathbb{Z}/p\mathbb{Z}$, we have $\ker_n = p^{n+1}\mathbb{Z}_p$ and ${}^n_p\tilde{G} = \mathbb{Z}/p^{n+1}\mathbb{Z}$.

Lifting Lemma 1.1 — *If C is a conjugacy class ${}^n_p\tilde{G}$ of order[2] ρ prime to p, then there exists a unique conjugacy class ${}^{n+1}_p\tilde{G}$ that lifts C and is of order ρ.*

Proof. Let $\phi_n : {}^{n+1}_p\tilde{G} \to {}^n_p\tilde{G}$ be the natural surjection. Let $g \in C$ and $H = \phi_n^{-1}(< g >)$. We have an exact sequence $1 \to \ker_n/\ker_{n+1} \to H \to < g > \to 1$. From the Schur-Zassenhaus lemma, since g is of order prime to p, the sequence splits; furthermore, the section $< g > \to H$ is unique, up to conjugation. □

1.2. Definition of modular towers. Suppose further given an integer $r \geq 2$ and an r-tuple $\mathbf{C} = (C_1, \ldots, C_r)$ of conjugacy classes of G of prime-to-p order. We will always assume $\mathrm{sni}_G(\mathbf{C}) \neq \emptyset$, where the *straight Nielsen class* $\mathrm{sni}_G(\mathbf{C})$ is as usual the set of all r-tuples $(g_1, \ldots, g_r) \in G^r$ such that (a) $g_1 \cdots g_r = 1$, (b) $< g_1, \ldots, g_r >= G$ and (c) $g_i \in C_i, i = 1, \ldots, r$. In particular, G 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 has no $\mathbb{Z}/p\mathbb{Z}$ quotient (for example, this excludes p-groups).

Thanks to the lifting lemma, one can define, for each integer $n \geq 0$, an r-tuple $\mathbf{C}^n = (C_1^n, \ldots, C_r^n)$ of conjugacy classes of ${}^n_p\tilde{G}$ such that C_i^{n+1} is the lifting of C_i^n of the same order, $i = 1, \ldots, r$. This definition provides, for each $n \geq 0$, a map

$$\mathrm{ni}_{{}^{n+1}_p\tilde{G}}(\mathbf{C}^{n+1}) \to \mathrm{ni}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$$

where the *Nielsen class* $\mathrm{ni}_G(\mathbf{C})$ is defined as $\mathrm{sni}_G(\mathbf{C})$ above except that condition (c) should hold only up to some permutation $\sigma \in S_r$.

---

[2] By order of a conjugacy class, we mean the common order of its elements.

Introduce next the associated Hurwitz spaces. For simplicity we restrict to the G-cover situation, and so to the inner version of Hurwitz spaces; and we omit the superscript "in" generally used to distinguish this situation from the absolute mere cover situation. For each $n \geq 0$, we have a Hurwitz space

$$\mathcal{H}_n = \mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$$

and a natural morphism $\psi_n : \mathcal{H}_{n+1} \to \mathcal{H}_n$. The collection of spaces $\mathcal{H}_n$ and morphisms ψ_n $(n \geq 0)$ is called the *modular tower* associated with the triple $(G, p, \mathbf{C})$.

There is a *reduced* variant of modular towers, for which the Hurwitz spaces $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$ should be replaced by the reduced versions $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}}$. Recall the difference lies in the definition of the isomorphisms between covers: two covers $\phi_i : X_i \to \mathbb{P}^1$ $(i = 1, 2)$ are equivalent in the reduced situation if there are isomorphisms $\alpha : X_1 \to X_2$ and $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ such that $\phi_2 \circ \alpha = \beta \circ \phi_1$ while it is further required that this hold with $\beta = \mathrm{Id}$ in the original situation. So $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}}$ is the quotient of $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$ by the action of $\mathrm{PSL}_2(\mathbb{C})$. See [FrKo] appendix II p.173 or [DeFr2] §6.2 for more details.

Hurwitz spaces $\mathcal{H}^{\mathrm{in}}_{r,G}$ are *fine* moduli spaces if and only if the group G has trivial center. In general this center hypothesis does not pass to group extensions. However that is the case for modular towers.

Theorem 1.2 [Fr2; p.141],[BaFr;Prop.3.21] — *Let G be a finite group with trivial center and p be a prime dividing $|G|$ such that G is p-perfect. Then for every $n \geq 0$, the group ${}^n_pG$ has trivial center.*

1.3. The dihedral group example. Modular curves can classically be presented as quotients of Hurwitz spaces of dihedral covers of $\mathbb{P}^1$ branched at 4 points:

Namely take the dihedral group $D_{p^n}=\mathbb{Z}/p^n \times^s \mathbb{Z}/2$ ($n>0$ and $p\neq 2$ some prime), $r=4$ and all the classes C_i, $i=1,\ldots,4$, equal to the involution class C of G_n.

Suppose given a cover $f:E\to\mathbb{P}^1$ defined and Galois over some field k, of group D_{p^n}, with 4 branch points and with inertia $\mathbf{C}$. The Riemann-Hurwitz formula yields the genus g of E: $2g-2=2p^n(-2)+4p^n$, 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 of D_{p^n} are automorphisms of $\mathrm{Pic}^o(E)$ of order p^n defined over k. Thus they are translations by some p^n-torsion point p defined over k. The data $(\mathrm{Pic}^o(E),\mathrm{p})$ classically corresponds to some point on the modular curve $X_1(p^n)$ different from the cusps.

Conversely, let (E,p) be an elliptic curve given with a p^n-torsion point, both defined over k. The cover $E\to E/<\mathrm{p}>$ is cyclic of degree p^n. The curve $E_o=E/<\mathrm{p}>$ 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}, with 4 branch points and with inertia $\mathbf{C}$.

Using this, for each $n > 0$, one can construct a surjective morphism defined over $\mathbb{Q}$

$$\chi_n : \mathcal{H}_n = \mathcal{H}_{D_{p^n}}(\mathbf{C}^n) \to X_1(p^n) - \{\mathrm{cusps}\}$$

and we have a commutative diagram

$$\begin{array}{ccc} \mathcal{H}_{n+1} & \xrightarrow{\chi_{n+1}} & X_1(p^{n+1}) \\ \Big\downarrow{\scriptstyle \psi_n} & & \Big\downarrow{\scriptstyle \times p} \\ \mathcal{H}_n & \xrightarrow{\chi_n} & X_1(p^n) \end{array}$$

where the right vertical map $\times p$ is the multiplication by p. In other words, there exists a morphism from the modular tower associated with the triple $(D_p, p, \mathbf{C})$ to the modular curve tower $(X_1(p^n))_{n>0}$. Here we have ${}^n_p\tilde{D}_p = D_{p^n}$ $(n>0)$ and ${}_p\tilde{D}_p = \mathbb{Z}_p \times^s \mathbb{Z}_2 := D_{p^\infty}$.

1.4. Irreducible components and lifting invariant. This paragraph provides a generalization of the lifting invariant from the original Fried-Serre example and discusses its use for distinguishing components of Hurwitz spaces.

Let $\mathcal{T}$ be an irreducible component of $\mathcal{H}_1$, which classically corresponds to an orbit $\mathcal{O}$ of the Hurwitz monodromy group H_r on $\mathrm{ni}_G(\mathbf{C})^{\mathrm{in}}$ (the superscript "in" indicates that the set $\mathrm{ni}_G(\mathbf{C})$ is regarded modulo the componentwise action of inner automorphisms of G). Our concern here is whether a component has a lift at level n of the tower.

Proposition 1.3 [Fr2] — *For $\mathbf{g} \in \mathcal{O}$, define the subset $\nu_n(\mathbf{g}) \subset {}^n_p\tilde{G}$ by*

$$\nu_n(\mathbf{g}) = \left\{ \tilde{g}_1 \cdots \tilde{g}_r \;\middle|\; \begin{array}{l} \tilde{\mathbf{g}} = (\tilde{g}_1, \ldots, \tilde{g}_r) \text{ } \textit{is a lift of } \mathbf{g} = (g_1, \ldots, g_r) \text{ in } {}^n_p\tilde{G} \\ \tilde{g}_i \in C_i^n, \quad i = 1, \ldots, r \text{ } \textit{(up to the order)} \end{array} \right\}$$

(a) *The set $\nu_n(\mathbf{g})$ depends only on $\mathcal{O}$ and so provides an invariant $\nu_n(\mathcal{O})$.*

(b) *There exists an irreducible component of $\mathcal{H}_n$ above $\mathcal{T}$ if and only if $1 \in \nu_n(\mathcal{O})$.*

(c) *If $1 \in \nu_n(\mathcal{O})$, then each element $\mathbf{g} \in \mathcal{O}$ can be lifted in $\mathrm{ni}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$. Consequently the irreducible components of $\mathcal{H}_n$ map onto those of $\mathcal{H}_1$.*

Proof. (b) Implication $(\Rightarrow)$ is trivial. Conversely, assume $1 \in \nu_n(\mathcal{O})$. Thus there exists a r-tuple $\tilde{\mathbf{g}}$ such that $\tilde{g}_1 \cdots \tilde{g}_r = 1$ and $\tilde{g}_i \in {}^n_p\tilde{C}_i$, $i = 1, \ldots, r$ (up to the order). To conclude that $\tilde{\mathbf{g}} \in \mathrm{ni}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$ and so that the component $\mathcal{T}$ has a lift in $\mathcal{H}_n$, it remains to show that $\tilde{g}_1, \ldots, \tilde{g}_r$ generate the group ${}^n_p\tilde{G}$. This follows from the Frattini property of ${}^n_p\tilde{G} \to G$.

Let $\mathbf{g}^o, \mathbf{g} \in \mathcal{O}$ with $\mathbf{g} = (\mathbf{g}^o)Q$ for some $Q \in H_r$. Clearly if $\tilde{\mathbf{g}}^o_n$ is a lift of $\mathbf{g}^o$, then $\tilde{\mathbf{g}}_n = (\mathbf{g}^o_n)Q$ is a lift of $\mathbf{g}$ and $\tilde{g}_1 \cdots \tilde{g}_r = \tilde{g}_1^o \cdots \tilde{g}_r^o$. (a) and (c) easily follow. $\square$

A component $\mathcal{T}$ of $\mathcal{H}_1$ is said to be *obstructed* at level n if there is no irreducible component $\mathcal{T}_n$ of $\mathcal{H}_n$ that maps onto $\mathcal{T}$. An iff condition is that $1 \notin \nu_n(\mathcal{O})$. This does not happen on the modular curve tower since each level is irreducible. In general, components of a modular tower above a given component of $\mathcal{H}_1$ form a tree with finite or infinite chains.

Define then $\nu(\mathcal{O})$ to be the projective limit of the $\nu_n(\mathcal{O})$ $(n \geq 1)$. The next result says that $\nu(\mathcal{O})$ is an arithmetic invariant that can be used to distinguish two irreducible components of $\mathcal{H}_1$, and so to possibly find irreducible $\mathbb{Q}$-components.

Theorem 1.4 [Fr2] p.148 — *Assume G is of trivial center. Let $\mathcal{H}_1 = \bigcup_{i=1}^{t} \mathcal{H}_{1i}$ be the decomposition of $\mathcal{H}_1$ in geometrically irreducible components. Assume $\mathcal{H}_1$ is $\mathrm{G}_{\mathbb{Q}}$-invariant (e.g. $\{C_1, \ldots, C_r\}$ is $\mathbb{Q}$-rational[3]). Then $\mathrm{G}_{\mathbb{Q}}$ permutes the components $\mathcal{H}_{1i}$. in such a way that, for each $\tau \in \mathrm{G}_{\mathbb{Q}}$,*

$$(\nu(\mathcal{H}_{1i}^{\tau}))^{\chi(\tau)} = \nu(\mathcal{H}_{1i}),\ i = 1, \ldots, t$$

where $\chi : \mathrm{G}_{\mathbb{Q}} \to (\mathbb{Z}_p)^{\times}$ is the cyclotomic character modulo $(p^n)_{n\geq 1}$. [4]

In particular, if $\nu(\mathcal{H}_{1i})^t = \nu(\mathcal{H}_{1i})$ for all $t \in (\mathbb{Z}_p)^{\times}$ and $\nu(\mathcal{H}_{1i}) \neq \nu(\mathcal{H}_{1j})$ for $j \neq i$, then $\mathcal{H}_{1i}$ is defined over $\mathbb{Q}$. Indeed, it follows from the first condition that, for each $\tau \in \mathrm{G}_{\mathbb{Q}}$, $\mathcal{H}_{1i}$ and $\mathcal{H}_{1i}^{\tau}$ have the same invariant ν. From the second, $\mathcal{H}_{1i} = \mathcal{H}_{1i}^{\tau}$, for each $\tau \in \mathrm{G}_{\mathbb{Q}}$.

A main ingredient of the proof is the Branch Cycle Argument which we recall. Appearance of the cyclotomic character comes from the action of $\mathrm{G}_{\mathbb{Q}}$ on inertia groups.

Branch Cycle Argument 1.5 [Vo] p.34 — *Let $f : X \to \mathbb{P}^1$ be a G-cover defined over $\mathbb{Q}$ (or more generally, with field of moduli $\mathbb{Q}$). Then each $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes the branch points $t_1, \ldots, t_r$ in such a way that*

$$t_i^{\tau} = t_j \Rightarrow C_i^{\chi(\tau)} = C_j \qquad (i, j = 1, \ldots, r)$$

In particular realizing $\mathbb{Z}/n\mathbb{Z}$ regularly over $\mathbb{Q}(T)$ requires at least $\phi(n)$ branch points (where ϕ is the Euler function). A classical consequence is that $\mathbb{Z}_p$ cannot be regularly realized over $\mathbb{Q}(T)$ [Fr3] §7.

---

[3] that is, $\{C_1^m,\ldots,C_r^m\}=\{C_1,\ldots,C_r\}$ for all integers m relatively prime with $|G|$.

[4] For each $n\geq 1$, the element $\nu_n(\mathcal{O})\in {}^n_p\tilde{G}$ lies in $\ker_o/\ker_n$ which by construction is a p-group, say of order p^N. Consequently powers $\nu_n(\mathcal{O})^t$ with $t\in\mathbb{Z}/p^N\mathbb{Z}$ are well-defined.

1.5. The Hilbert property on modular towers. Suppose that on the modular tower $(\mathcal{H}_n)_{n\geq 0}$, we know a projective system $(\mathbf{p}_n)_{n\geq 0}$ of K-rational points corresponding to actual G-covers $X_n \to \mathbb{P}^1$ defined over K (that is, K is not only the field of moduli but also a field of definition). Over a hilbertian field K, one can specialize this tower of covers to get an infinite field extension of K with the same Galois structure. More specifically we have the following statement.

Proposition 1.6 — *Let K be a Hilbertian field and let $E/K(T)$ be a Galois extension of group ${}_p\tilde{G}$ and with only finitely many branch points. Then there exists an infinite subset $H \subset K$ such that for all $t \in H$ the specialization $T \to t$ provides a Galois field extension E_t/K with Galois group ${}_p\tilde{G}$.*

The proof illustrates the Frattini property. The main ideas are already in [Ser3] §10.6.

Proof. Let E_0 be the fixed field in E of the subgroup ker; the extension $E_0/K(T)$ is finite and Galois of group $G = G_0$. Let H be the subset of K consisting of all the $t \in K$ such that the specialization (or place) $T \to t$ is unramified in $E/K(T)$ and yields no trivial residue extension M_t/K, for all minimal non trivial extensions M of $K(T)$ contained in E_0. As K is hilbertian and $E/K(T)$ is branched at only finitely many points, H is infinite.

Let $F/K(T)$ be a non trivial finite extension contained in E. The field $F \cap E_0$ is the fixed field in E of the subgroup $\Gamma\,\ker$ where $\Gamma = \mathrm{Gal}(E/F)$. As ${}_p\tilde{G} \to G_0$ is Frattini, it follows from $\Gamma \neq {}_p\tilde{G}$ that $\Gamma\,\ker \neq {}_p\tilde{G}$, that is $F \cap E_0 \neq K(T)$. From above, for all $t \in H$, the specialization $T \to t$ is unramified in $(F \cap E_0)/K(T)$ and yields no trivial residue extension $(F \cap E_0)_t/K$. The same is *a fortiori* true for the residue extensions F_t/K. From standard reductions, this guarantees there is a unique residue extension F_t/K of degree $[F : K(T)]$ (*i.e.*, the place $T \to t$ is inert in the extension $[F : K(T)]$). Letting $F/K(T)$ run over all finite subextensions of E yields the result. □

2. Diophantine questions on modular towers

We are interested in the persistence of rational points on ascending levels of a modular tower. The modular curve tower shows the general pattern.

2.1. Modular curves and dihedral group realizations. Consider a projective system of points $(\mathbf{p}_n)_{n>0}$ on the modular curve tower $(X^1(p^n))_{n>0}$. Each point $\mathbf{p}_n$ corresponds to a p^n-torsion point on an elliptic curve E (the same curve for all $n>0$). Assume E is defined over some field K. The group G_K acts on the p-torsion points of $E\otimes_K \overline{K}$: this is the action of G_K on the $\mathbb{Z}_p$-Tate module V_p associated with E. Denote the map that sends $(E,\mathbf{p})\in X_1(p)$ to the canonical invariant of the elliptic curve E by $j: X_1(p)\to\mathbb{P}^1$. The above action is an action on the set of projective systems of $\overline{K}$-points $(\mathbf{p}_n)_{n>0}$ that lie above the invariant $j(E)$ of E.

There is a similar action of G_K in the general situation of modular towers:

(1) The group G_K acts on the set of projective systems of $\overline{K}$-points $(\mathbf{p}_n)_{n>0}$ that lie above any fixed $\mathbf{t}\in\mathcal{U}_r(K)$.

From Serre's open image theorem, if F is any number field, there are only finitely many F-rational p-torsion points on a given elliptic curve over F, which rewrites

(2) given a projective system of $\overline{K}$-points $(\mathbf{p}_n)_{n>0}$ above $j\in\mathbb{P}^1(K)$ and a finite extension F/K, then $\mathbf{p}_n\notin X^1(p^n)(F)$, for all but finitely many n. [5]

Furthermore, as the genus of modular curves $X^1(p^n)$ tends to ∞ with n, from Faltings' theorem, $X^1(p^n)(F)$ is finite for $n\gg 1$ (depending on p and F); and it even follows that

(3) $X^1(p^n)(F)=\emptyset$ for $n\gg 1$ (depending on p and F),

for otherwise there would be a projective system $(\mathbf{p}_n)_{n\geq 0}$ of F-rational points. In fact, from the Mazur-Merel theorem, we have the following stronger statement (where p^n can even be replaced by any integer $N>1$).

(4) $X^1(p^n)(F)=\emptyset$ for $p^n\gg 1$ (depending only on F).

The spirit of Fried's conjectures, is that similar statements hold for general modular towers (possibly with some additional assumptions). Before stating these conjectures, we give another motivation.

---

5 In particular the profinite group D_{p^∞} cannot be regularly realized over $\mathbb{Q}(T)$ with 4 branch points and only inertia groups of order 2. In fact there cannot be any regular realization at all of D_{p^∞} over $\mathbb{Q}(T)$ ([Fr3] §7).

Dihedral Group Conjecture 2.1 [DeFr1] — *Fix $r_o \geq 1$. Then only finitely many dihedral groups D_{p^n} with p an odd prime and $n \geq 1$ can be regularly realized over $\mathbb{Q}(T)$ with no more than r_o branch points.*

Proof for $r_o = 5$ [DeFr1]**.** Assume D_{p^n} is regularly realized with $r \leq 5$ branch points.

1st case: 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). So $r = 4$ and we are back with the Dihedral Group example. The starting realization then corresponds to some $\mathbb{Q}$-point on $X^1(p^n)$ which, from Mazur's theorem, can't exist if $p^n > 7$.

2nd case: One of $C_1, \dots, C_r$, say C, is not the involution class of D_{p^n}, *i.e.* is of order p^k with $k > 0$. There are at least $(p^k - p^{k-1})/2$ distinct classes C^u with u relatively prime to p. From the Branch Cycle Argument, there should be at least $(p^k - p^{k-1})/2$ branch points. So $(p-1)/2 \leq r$. Therefore $p \leq 11$.

To finish the proof, it remains to rule out the possibility that for some $p \leq 11$, infinitely many (and so all) dihedral groups D_{p^n} $(n > 0)$ be regularly realized over $\mathbb{Q}(T)$ with r branch points and with the first inertia class, say C_{n1}, of order p^{k_n} with $k_n > 0$ $(n > 0)$. If it were the case, the sequence $(k_n)_{n>0}$ would be unbounded (for otherwise, one could form an element of $D_{p^\infty} = \varprojlim_n D_{p^n}$ of finite p-power order). It follows that for n suitably large, $(p^{k_n} - p^{k_n - 1})/2 \geq r$, which again contradicts the Branch Cycle Argument. □

Remark 2.2. While D_p cannot be realized with less than 6 branch points for $p > 11$, only 3 suffice for the Monster group. Dihedral groups are significant tests in geometric inverse Galois theory. It is not even known that dihedral groups can be regularly realized with only involutions as inertia generators. The Dihedral Group conjecture would follow from conjectures of Mazur-Kamieny on the finiteness of primes that are order of rational points on an abelian variety over $\mathbb{Q}$ of given dimension (see [DeFr1]).

2.2. Main conjectures. As above we have two related conjectures: one about group realizations and another one about rational points on modular towers. The first one is inspired by the Dihedral Group conjecture [6].

[6] Note though that the number of exceptional characteristic quotients may here depend on p: for dihedral groups, conjecture 2.3 asks for less than the Dihedral Group conjecture.

Conjecture on Realizations of Characteristic Quotients 2.3 [FrKo] — *Let G be a finite group with trivial center, p be a prime dividing $|G|$ such that G is p-perfect, F be a number field and $r_o \geq 3$ be an integer. Then only finitely many characteristic quotients ${}^n_p\tilde{G}$ of ${}_p\tilde{G}$ can be regularly realized over $F(T)$ with no more than r_o branch points.*

The second conjecture is a generalization of statement (3) on modular curves.

Diophantine Conjecture on Modular Towers 2.4 — *Let G be a finite group with trivial center, p be a prime dividing $|G|$ such that G is p-perfect, $r \geq 3$ be an integer and $\mathbf{C}$ be an r-tuple of conjugacy classes of G of prime-to-p order. Then for every number field F, there are no F-rational points on levels $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}}$ of the reduced modular tower if n is suitably large.*

2.3. Reduction to modular towers. The second case of the proof of the Dihedral Group Conjecture for $r_o = 5$ uses the Branch Cycle Argument to rule out realizing dihedral groups with some of the inertia classes of order p, thus reducing the proof to inspecting rational points on the modular curve tower. This generalizes as follows.

Theorem 2.5 [FrKo] §4 — *Let G be a finite group, p be a prime divisor of $|G|$, $r_0 \geq 3$ be an integer and F be a number field. Suppose each characteristic quotient ${}^n_p\tilde{G}$ of ${}_p\tilde{G}$ can be regularly realized over $F(T)$ 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 of prime-to-p order such that the associated modular tower $(\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n))_{n\geq 0}$ has F-rational points at every level.*

As a consequence, in order to prove conjecture 2.3 on realizations of characteristic quotients for a given integer $r_0 \geq 2$, it is sufficient to prove the diophantine conjecture 2.4 on modular towers for every $r \leq r_0$.

Proof. For simplicity we take $F = \mathbb{Q}$. As for each level $n \geq 0$, there are only finitely many possible choices of tuples $\mathbf{C}_n$ with no more than r_0 entries and that any regular realization of ${}^n_p\tilde{G}$ with inertia invariant $\mathbf{C}_n$ yields a realization of ${}^{n-1}_p\tilde{G}$ with inertia invariant the tuple induced from $\mathbf{C}_n$ by the map ${}^n_p\tilde{G} \to {}^{n-1}_p\tilde{G}$ ($n > 1$), the assumption of theorem 2.5 implies that all characteristic quotients ${}^n_p\tilde{G}$ of ${}_p\tilde{G}$ can be regularly realized over $\mathbb{Q}(T)$ with inertia invariants $\mathbf{C}_n = (C_{n1}, \ldots, C_{nr})$ that are compatible all along the tower ($n > 0$); in particular, the number r of branch points is the same for all $n > 0$. We suppose given such a set of realizations.

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

(H) *There exists some integer $n_0 \geq 0$ such that for all $n \geq n_0$ there is at least one inertia group of order divisible by p in the given realization of ${}^n_p\tilde{G}$.*

We may and will assume that $C_{n_o 1}$ is of order divisible by p; then so is C_{n1} for all $n \geq n_o$. Then fix $\mathbf{g} = (g_n)_{n\geq 0} \in {}_p\tilde{G}$ such that $g_n \in C_{n1}$ for all $n \geq 0$ (such a $\mathbf{g}$ indeed exists). For each $n \geq 0$, let $\nu_n = \nu_n(\mathbf{g})$ be the number of conjugacy classes of ${}^n_p\tilde{G}$ containing powers g_n^j with j relatively prime to the order of g_n. The Branch Cycle Argument yields

$$\nu_n(\mathbf{g}) \leq r_o \text{ for all } n \geq 0 \tag{5}$$

Assume g_0 is of order αp^{k_0} for some integers $k_0 \geq 0$ and $\alpha \geq 1$ with $(p, \alpha) = 1$. Then 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 $\ker_0/\ker_n$ which is a p-group). We claim that the sequence $(k_n)_{n\geq 0}$ is unbounded. Indeed, otherwise, $\mathbf{g}^\alpha \in {}_p\tilde{G}$ would be of finite p-power order and non-trivial (p divides the order of g_{n_0}). Now such elements do not exist in the p-Sylow subgroups of ${}_p\tilde{G}$ which are free pro-p groups.

Observe next that, in order to show that (5) is impossible, one may, up to changing $\mathbf{g}$ into $\mathbf{g}^{\alpha p^{k_0}}$, assume that $\mathbf{g}$ is an element of ker of p-power order (note that $\nu_n(\mathbf{g}^{\alpha p^{k_0}}) \leq \nu_n(\mathbf{g})$ for all $n \geq 0$).

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 conjugacy classes of the prime-to-p powers of g_k. As at higher levels $n \geq k$, $g_n^{\mu_1}, \ldots, g_n^{\mu_{\nu_0}}$ remain non-conjugate, then for every level $n \geq 0$ and for every prime-to-p integer m, we have

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

As condition (6) at level n with some conjugation factor $h_{m,n}$ implies the same condition at lower levels with the same exponent μ_i and with conjugation factors those induced by $h_{m,n}$ and that both the exponents μ_i and the conjugation factors vary in finite sets, we obtain that for every prime-to-p integer m, there exist $i(m) \in \{1, \ldots, \nu_0\}$ and $\mathbf{h}_m = (h_{m,n})_{n\geq 0} \in {}_p\tilde{G}$ such that

$$\mathbf{g}^m = \mathbf{h}_m\, \mathbf{g}^{\mu_{i(m)}}\, \mathbf{h}_m^{-1} \text{ in } {}_p\tilde{G}. \tag{7}$$

Let $\kappa \geq 0$ be the smallest integer such that $\mathbf{g} \in \ker_\kappa \setminus \ker_{\kappa+1}$. From above, the order of g_n tends to ∞ with n. So if n is suitably large, there exist two prime-to-p integers m and m' such that $g_n^m \neq g_n^{m'}$ with $i(m) = i(m')$ and $h_{m,\kappa} = h_{m',\kappa}$. This yields

$$\mathbf{g}^{m'} = (\mathbf{h}_{m'}\mathbf{h}_m^{-1})\, \mathbf{g}^m\, (\mathbf{h}_{m'}\mathbf{h}_m^{-1})^{-1} \text{ with } \mathbf{h}_{m'}\mathbf{h}_m^{-1} \in \ker_\kappa \tag{8}$$

Since $\ker_\kappa$ is a free pro-p group, any collection of representatives of the non-trivial cosets of $\ker_\kappa$ modulo $\ker_{\kappa+1}$ give topological generators of $\ker_\kappa$. Complement $\mathbf{g}$ with elements $\mathbf{g}_2, \dots, \mathbf{g}_l$ so that the profinite subgroups $B =< \mathbf{g} >$ and $D =< \mathbf{g}_2, \dots, \mathbf{g}_l >$ freely generate $\ker_\kappa$. In this situation, from [HeRi], every element $\mathbf{h}' \in \ker_\kappa$ either is in B or else satisfies $\mathbf{h}'B(\mathbf{h}')^{-1} \cap B = \{1\}$. For $\mathbf{h}' = \mathbf{h}_{m'}\mathbf{h}_m^{-1}$, which, from (8) satisfies $\mathbf{h}'B(\mathbf{h}')^{-1} = B$, we get $\mathbf{h}' \in B$. But as $B =< \mathbf{g} >$ is abelian, (8) would rewrite $\mathbf{g}^{m'} = \mathbf{g}^m$ — a contradiction.

Conclude that (5) and so (H) do not hold. Therefore, in the given set of regular realizations over $\mathbb{Q}(T)$ of groups ${}^n_p\tilde{G}$ $(n \geq 0)$, there exists infinitely many levels $n \geq 0$ such that all inertia classes $C_{n1}, \dots, C_{nr}$ 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 ${}^{n+1}_p\tilde{G} \to {}^n_p\tilde{G}$ are p-groups, for each $i = 1, \dots, r$, C_{ni} has the same order as C_{0i} $(n \geq 0)$. But then, it follows from the lifting lemma 1.1 that the conjugacy classes $C_{n1}, \dots, C_{nr}$ are the unique lifts of the conjugacy classes $C_{01}, \dots, C_{0r}$ of G (respectively), *i.e.*, with the notation of §1.2, $C_{ni} = C_{0i}^n$, $i = 1, \dots, r$, $n \geq 0$. Setting $\mathbf{C} = (C_{0i}, \dots, C_{0r})$, we have obtained that there are $\mathbb{Q}$-rational points on each level of the modular tower $(\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n))_{n\geq 0}$. $\square$

Remark 2.6. As K. Kimura observed [Ki], the same conclusion still holds if the starting realizations of the groups ${}^n_p\tilde{G}$ $(n \geq 0)$ are by $\overline{\mathbb{Q}}$-G-covers with field of moduli $\mathbb{Q}$ (but not necessarily defined over $\mathbb{Q}$): this is because the Branch Cycle Argument (§1.4) holds under this more general assumption. Now if we do start with G-covers defined over $\mathbb{Q}$, the proof actually shows a little more: the $\mathbb{Q}$-rational points eventually obtained on each level of a modular tower also correspond to G-covers defined over $\mathbb{Q}$. Finally recall from theorem 1.2 that if G is p-perfect and has trivial center (as in conjectures 2.3 and 2.4), than so do all the ${}^n_p\tilde{G}$, and so, classically, at each level, the field of moduli is a field of definition [DeDo].

2.4. Reduction to a genus estimate. We retain the hypotheses and notation of the Diophantine conjecture on Modular Towers. If in addition $r = 4$, the spaces $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}}$ are 1-dimensional. Suppose we know that

(9) all geometrically irreducible components $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}}$ are of genus ≥ 2 $(n \geq 0)$. [7]

Then, from Faltings' theorem, given any number field F, there are only finitely many F-rational points on each of the curves $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}}$ $(n \geq 0)$. As noticed above, it follows there are no F-rational points at all on $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}}$ if n is suitably large unless there exists

[7] For bigger $r \geq 4$, the general conjecture is that for suitably large n, $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}}$ has only components of general type. For curves, "general type" means "of genus ≥ 2".

a projective system of F-rational points. But as the next result shows, this possibility cannot occur. Therefore the last stage of the Diophantine conjecture on Modular Towers for $r = 4$ consists in showing (9). A detailed outline of the proof of (9) is provided in Fried's paper in this volume [Fr4].

Theorem 2.7 [BaFr] theorem 6.1 — *Let G be a finite group with trivial center, p be a prime dividing $|G|$ with G p-perfect, $r \geq 3$ be an integer and $\mathbf{C}$ be an r-tuple of conjugacy classes of G of prime-to-p order. Let F be either a number field or a finite field of characteristic $\ell \not| |G|$. Then the following is true.*

(a) *There is no tower*

$$\cdots \to Y_n \to Y_{n-1} \to \cdots \to Y_0 \to \mathbb{P}^1$$

of compatible G-covers $Y_n \to \mathbb{P}^1$ defined over F with group ${}_p^n\tilde{G}$, with r branch points and with inertia canonical invariant $\mathbf{C}^n$ ($n \geq 0$). Equivalently, there is no projective system of F-rational points on the modular tower $(\mathcal{H}_{{}_p^n\tilde{G}}(\mathbf{C}^n))_{n\geq 0}$.

(b) *There is no projective system of F-points on the reduced modular tower $(\mathcal{H}_{{}_p^n\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}})_{n\geq 0}$.*

Proof. (a) Suppose first F is a number field. Assume on the contrary that there exists a tower of G-covers as in the statement. For each $n \geq 0$, the order $|{}_p^n\tilde{G}|$ has as only prime divisors those of $|G|$ and p. Furthermore the covers $Y_n \to \mathbb{P}^1$ have the same r branch points. It follows from Fulton's good reduction theorem that for each finite place v of F of suitably large residue characteristic, the tower has good reduction modulo the valuation ideal of v. Pick such a place v, denote the residue field by $\mathbb{F}$, its characteristic by ℓ and the reduced tower by

$$\ldots \overline{Y}_n \to \overline{Y}_{n-1} \to \ldots \to \overline{Y}_0 \to \mathbb{P}^1_{\mathbb{F}}$$

We are left with showing that such a tower cannot exist and have thus reduced the whole proof of (a) to the finite field situation.

Regard the $\mathbb{F}$-tower as a tower of $\overline{Y}_0$. As the inertia classes in $\mathbf{C}$ are of prime-to-p order, covers of $\overline{Y}_0$ constituting this tower are étale; and they are Galois with p-groups as Galois groups [8]. The tower thus corresponds to an epimorphism

[8] In the dihedral group example with $G{=}D_p$, one can directly conclude at this stage: indeed these Galois étale covers are then abelian (of group $\mathbb{Z}/p^n\mathbb{Z}$) and thus correspond to $\mathbb{F}$-points on $\mathrm{Jac}(\overline{Y}_1)$ of order p^n. As n is arbitrary, we obtain a contradiction.

$$\phi : \pi_1(\overline{Y}_0)^{(p)} \twoheadrightarrow \ker_0 \ \subset {}_p\tilde{G}$$

where $\pi_1(\overline{Y}_0)^{(p)}$ is the p-part of the fundamental group of $\overline{Y}_0$ (over $\mathbb{F}$).

The exact sequence

$$1 \to \pi_1(\overline{Y}_0 \otimes_F \overline{F})^{(p)} \to \pi_1(\overline{Y}_0)^{(p)} \to \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \to 1$$

admits a section s (as $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ is pro-cyclic). Denote the restriction of ϕ to the geometric fundamental group $\pi_1(\overline{Y}_0 \otimes_F \overline{F})^{(p)}$ by $\phi_{\overline{F}}$ and the map $\phi \circ s \in \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}), \ker_0)$ by φ. For each $\tau \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$, we have

$$\phi_{\overline{F}}(x^{s(\tau)}) = \varphi(\tau)\phi_{\overline{F}}(x)\varphi(\tau)^{-1} \qquad (x \in \pi_1(\overline{Y}_0 \otimes_F \overline{F})^{(p)})$$

Let $\mathbb{T}_p = \pi_1(\overline{Y}_0 \otimes_F \overline{F})^{(p)}/[\pi_1(\overline{Y}_0 \otimes_F \overline{F})^{(p)}, \pi_1(\overline{Y}_0 \otimes_F \overline{F})^{(p)}]$ be the Tate module of $\overline{Y}_0 \otimes_F \overline{F}$. The morphism $\phi_{\overline{F}}$ induces an homomorphism

$$\widetilde{\phi}_{\overline{F}} : \mathbb{T}_p \to \ker_0/[\ker_0, \ker_0]$$

which is still surjective and satisfies

$$\widetilde{\phi}_{\overline{F}}(x^{s(\tau)}) = \widetilde{\phi}_{\overline{F}}(x) \qquad (\tau \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}), x \in \mathbb{T}_p)$$

This shows that $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ has a trivial action on a quotient of the Tate module $\mathbb{T}_p$ of rank $\mathrm{rk}(\ker_0) > 0$. We obtain a contradiction as the Frobenius (in $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$) has eigenvalues of absolute value $|\mathbb{F}|^{1/2}$.

Recall finally that under our assumptions the $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$s are fine moduli spaces. This is why the result can be equivalently stated in terms of existence of projective systems of rational points on the modular tower $(\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n))_{n\geq 0}$. This ends the proof of (a).

To deduce (b), it suffices to show that every projective system of F-rational points on the reduced modular tower $(\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)^{\mathrm{rd}})_{n\geq 0}$ can be lifted to a projective system of points on the modular tower $(\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n))_{n\geq 0}$ that are rational over a finite extension of F. This last point is claimed and discussed in [BaFr]; a full proof is given in [Ki] Lemma 5.2 and, in a bigger generality, in [Ca3] corollary 2.17. $\square$

Remark 2.8. Generalizations of theorem 2.7 have been established by A. Cadoret [Ca2-3] and K. Kimura [Ki]. They notably obtain the same conclusion without assuming G has trivial center. Even more generally, A. Cadoret extends theorem 2.7 to the case ${}_p\tilde{G}$ is replaced by any extension $\widetilde{G}$ of a finite group by a free pro-p group and the modular tower $(\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n))_{n\geq 0}$ can be any tower $(\mathcal{H}_{G_n}(\mathbf{C}_n))_{n\geq 0}$ of Hurwitz spaces associated with any projective system $(G_n)_{n\geq 0}$ of finite groups such that $\widetilde{G}=\varprojlim G_n$. As a consequence, there is no regular realization of $\widetilde{G}$ over $F(T)$ for any number field F.

2.5. ℓ-adic points on Harbater-Mumford modular towers. Results and conjectures from previous sections suggest that although the characteristic quotients ${}^n_p\tilde{G}$ may look quite similar (same rank, same generating systems, etc.), regular realization over $\mathbb{Q}(T)$ of all of them with the same invariants is hopeless: one has to let the number of branch points grow. Furthermore there are purely diophantine obstructions, which one does not have a good hold on: $\mathbb{Q}$-rational points on varieties may exist or not.

What about rational points over $\mathbb{Q}_\ell$? The answer is totally different. In general it is easier to find ℓ-adic points on varieties. More particularly it is easier on Hurwitz spaces because some efficients tools — the so-called patching techniques — to construct covers over henselian fields are available.

As above fix a finite group G, a prime divisor p of $|G|$ with G p-perfect, an integer r and an r-tuple $\mathbf{C}=(C_1,\dots,C_r)$ of conjugacy classes of G of prime-to-p order such that $\mathrm{sni}_G(\mathbf{C})\neq\emptyset$. 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 2.9 — *There exist projective systems of k-rational points on the associated modular tower $(\mathcal{H}_n)_{n\geq 0}$.*

This is a special case of [DeDes]. The proof consists in constructing a tower $(K_n)_{n\geq 0}$ of regular Galois extensions of $k(T)$ that realizes the projective system $({}^n_p\tilde{G})_{n\geq 0}$. For each level n of the tower, patching methods (*e.g.* [Li], [Po]) can be used. However it should be done in such a way that the invariants of the extensions $K_n/k(T)$ (branch points, inertia invariant) be compatible all along the tower. This does not assure 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 $K_n/k(T)$

($n \geq 0$). That is what makes "passing to infinity" possible, *via* the compactness argument already used before (a projective limit of non-empty finite sets is non-empty).

In more details, Theorem 2.9 can be obtained as a special case of the general construction from [DeDes] §3.1. Our conjugacy classes C_i^n, $i = 1, \ldots, r$, $n \geq 0$ have the same (prime-to-p) order, which guarantees Hypothesis (iv) of that construction. As ζ_N is in k, Hypothesis (iii) is obviously satisfied: with the terminology from [DeDes], the cyclotomic order of the C_i^ns over k is 1. One then may choose the branch points $x_1, y_1, \ldots, x_{r/2}, y_{r/2}$ in $\mathbb{P}^1(k)$ satisfying conditions from part (2) of the construction. The other hypotheses are straightforwardly checked.

As a consequence of Theorem 2.9, the profinite group ${}_p\tilde{G}$ can be regularly realized over $k(T)$ [9]. For example, for $G = D_p$ we obtain:

Corollary 2.10 — *For each odd prime p and every prime ℓ, the profinite group D_{p^∞} can be regularly realized over $\mathbb{Q}_\ell(T)$ with 4 branch points and inertia groups of order 2.*

The varieties $\mathcal{H}_n = \mathcal{H}_{{}_p^n\tilde{G}}(\mathbf{C}_n)$ from theorem 2.9 are reducible in general. A next motivation was to obtain a similar result but with the $\mathcal{H}_n$ geometrically irreducible and defined over $\mathbb{Q}$ ($n \geq 0$). This was achieved in [DeEm].

Before stating the result, recall these definitions from [Fr2]. A tuple $\mathbf{C} = (C_1, \ldots, C_r)$ of conjugacy classes of a group G is said to be *g-complete* if it satisfies "$g_i \in C_i$, $i = 1, \ldots, r \Rightarrow < g_1, \ldots, g_r >= G$". A tuple $\mathbf{C}$ with the shape $(C_1, C_1^{-1}, \ldots, C_s, C_s^{-1})$ 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 2.11 — *In addition to the assumptions of theorem 2.9, suppose $\mathbf{C}$ is HM-g-complete and is $\mathbb{Q}$-rational (see footnote 3). Then there exists a projective system $(\mathrm{HM}_n)_{n\geq 0}$ of $\mathbb{Q}$-components of $(\mathcal{H}_{{}_p^n\tilde{G}}(\mathbf{C}_n))_{n\geq 0}$ (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 $C_1, \ldots, C_s$, then there exist projective systems of k-rational points on the tower $(\mathrm{HM}_n)_{n\geq 0}$.

The key is to take for HM_n the *Harbater-Mumford component* of $\mathcal{H}_{{}_p^n\tilde{G}}(\mathbf{C}_n)$. 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

[9] The method of construction is developed in [DeDes] in a bigger generality. Other profinite groups are considered (and regularly realized under some assumptions), notably the free profinite group $\widehat{F}_\omega$ with countably many generators.

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 [Fr2] theorem 3.21. Furthermore using Wewers' description of the boundary of Hurwitz spaces [We], 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 [DeEm]. 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 [DeDes] lie on this HM-component (under some mild assumptions).

Remark 2.12. In the dihedral group situation (§1.3), each space $\mathcal{H}_{\substack{n\\p}\tilde{G}}(\mathbf{C}_n)$ is geometrically irreducible and defined over $\mathbb{Q}$; the HM-component is the whole Hurwitz space.

Finally one would like to have an analog of theorem 2.11 with the r-dimensional varieties HM_n replaced by varieties of low dimension. Such results have been recently obtained by A. Cadoret [Ca1]. 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 2.13 [Ca1] — *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*

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

such that on the modular tower $(\mathcal{H}_{\substack{n\\p}\tilde{G}}(\mathbf{C}^n))_{n\geq 0}$, there is, above the sublocus of $\mathcal{U}_r$ 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.

A similar result holds with $\mathbb{R}$ replacing $\mathbb{Q}_\ell$ but $r-1$ becomes $r-2$ and the curves $\mathcal{C}_{\mathbf{t},n}$ surfaces $\mathcal{S}_{\mathbf{t},n}$[10], and no adjunction of root of 1 is necessary.

Denote the fields of totally real (resp. totally ℓ-adic) algebraic numbers, *i.e.* the maximal Galois extension of $\mathbb{Q}$ contained in $\mathbb{R}$ (resp. $\mathbb{Q}_l$) by $\mathbb{Q}^{\mathrm{tr}}$ (resp. $\mathbb{Q}^{\mathrm{t}\ell}$). Applying

10 Versions with curves over $\mathbb{R}$ can still be obtained but they require further assumptions on the group G [Ca1].

next the local-global principle (proved by Moret-Bailly [Mo] (see also [Po])) to the curves $\mathcal{C}_{\mathbf{t},n}$ (or the surfaces $\mathcal{S}_{\mathbf{t},n}$) one obtains that each characteristic quotient ${}^n_p\tilde{G}$ can be regularly realized over $\mathbb{Q}^{\mathrm{t}\ell}(\zeta_\mu)(T)$ with $r-1$ fixed branch points globally invariant under $\mathrm{G}_{\mathbb{Q}}$ (resp. over $\mathbb{Q}^{\mathrm{tr}}(T)$ with $r-2$ fixed branch points globally $\mathrm{G}_{\mathbb{Q}}$-invariant).

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].

References

[BaFr] P. Bailey and M. Fried, "Hurwitz monodromy, spin separation and higher levels of a Modular Tower", Proceedings of the Von Neumann Symposium on Arithmetic Fundamental Groups and Noncommutative Algebra (MSRI 1999), *Proceedings of Symposia in Pure Mathematics*,**70**, AMS, ed. by M. Fried and Y. Ihara, (2002), 70–220.

[Ca1] A. Cadoret, *Harbater-Mumford subvarieties of Hurwitz moduli spaces of covers*, Math. Annalen, (to appear).

[Ca2] A. Cadoret, *Rational points on Hurwitz towers*, preprint as of March 2005.

[Ca3] A. Cadoret, *Lifting results for rational points on Hurwitz moduli spaces*, preprint as of June 2005.

[DeDes] P. Dèbes and B. Deschamps, *Corps ψ-libres et théorie inverse de Galois infinie*, J. fur die reine und angew. Math., **574**, (2004), 197–218.

[DeDo] P. Dèbes and J.-C. Douai, *Algebraic covers: field of moduli versus field of definition*, Annales Sci. E.N.S., **30**, (1997), 303–338.

[DeFr1] P. Dèbes and M. Fried, *Nonrigid constructions in Galois theory*, Pacific J. Math., **163**, No.1, (1994), 81–122.

[DeFr2] P. Dèbes and M. Fried, *Integral specialization of families of rational functions*, Pacific J. Math., **190**, No.1, (1999), 45–85.

[DeEm] P. Dèbes and M. Emsalem, *Harbater-Mumford Components and Hurwitz Towers*, preprint, (2003).

[Fr1] M. Fried, *Alternating groups and lifting invariants*, preprint, [http://www.math.uci.edu/~mfried/].

[Fr2] M. Fried, *Introduction to modular towers*, in *Recent Developments in the Inverse Galois Problem*, Contemporary Math., **186**, (1995), 111–171.

[Fr3] M. Fried, *Topics in Galois Theory*, expanded version of review of Serre's book with same title, in *Recent Developments in the Inverse Galois Problem*, Contemporary Math., **186**, (1995), 111–171.

[Fr4] M. Fried, *Higher rank Modular Towers*, in this volume.

[FrJa] M. Fried and M. Jarden, *Field arithmetic*, Ergeb. der Math., 3. Folge, Band 11, Springer-Verlag, (1986).

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

[HeRi] W. Herfort and L. Ribes, *Torsion elements and centralizers in free products of profinite groups*, J. fur die reine und angew. Math., **358**, (1985), 155–161.

[Ki] K. Kimura, *Modular towers for finite groups that may not be centerfree*, Master Thesis (Kyoto Univ. March 2004), english translation as of 09/05.

[Li] Q. Liu, *Tout groupe fini est groupe de Galois sur $\mathbb{Q}_p(T)$*, Contemporary Mathematics, **186**, (1995), 261–265.

[Mo] L. Moret-Bailly, *Groupes de Picard et problèmes de Skolem II*, Annales Sci. E.N.S., **22**, (1989), 181–194.

[Po] F. Pop, *Embedding problems over large fields*, Annals of Math., **144**, 1–35, (1996).

[Se] D. Semmen, *Modular Towers and modular representations)*, in this volume.

[Ser1] J.-P. Serre, *Relèvements dans $\widetilde{A}_n$*, C.R.A.S. Paris, série I, **311**, (1990), 477–482.

[Ser2] J.-P. Serre, *Revêtements à ramification impaire et thêta-caractéristiques, dans $\widetilde{A}_n$*, C.R.A.S. Paris, série I, **311**, (1990), 547–552.

[Ser3] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, Friedr. Vieweg & Sohn, (1990).

[Vo] H. Völklein, *Groups as Galois groups - an introduction*, Cambridge Studies in Advanced Mathematics, **53**, Cambridge Univ. Press, (1996).

[We] S. Wewers, *Construction of Hurwitz spaces*, thesis, (1998).

Pierre.Debes@univ-lille1.fr
Univ. Lille 1, Mathématiques, 59655 Villeneuve d'Ascq Cedex, France.