Séminaires & Congrès
13, 2006, p. 127–144

AN INTRODUCTION TO THE MODULAR TOWER PROGRAM

by

Pierre Dèbes

***Abstract.* —** Modular towers have been introduced by M. Fried. They are towers of Hurwitz spaces, with levels corresponding to the characteristic quotients of the p-universal Frattini cover of a fixed finite group and with p a prime divisor of the order of the group. The tower of modular curves of levels p^n $(n > 0)$ is the original example: the finite group is then the dihedral group of order $2p$. 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 results.

***Résumé* (Une introduction au programme des tours modulaires). —** Les tours modulaires ont été introduites par M. Fried. Ce sont des tours d'espaces de Hurwitz dont les niveaux correspondent aux quotients caractéristiques du p-revêtement universel de Frattini d'un groupe fini fixé, le premier p étant un diviseur de l'ordre du groupe. La tour des courbes modulaires de niveaux p^n $(n > 0)$ est l'exemple initial : le groupe fini est dans ce cas le groupe diédral d'ordre $2p$. Il y a des conjectures diophantiennes sur les tours modulaires, qui s'inspirent de la situation des courbes modulaires : l'esprit est que les points rationnels sur un corps de nombres fixé disparaissent au-delà d'un certain niveau. Dans cet article, qui est le premier d'une série de trois sur le sujet dans ce volume, après avoir revu la construction des tours modulaires, nous revenons sur ces conjectures, en examinons l'impact et expliquons quelques résultats.

Contents

2000 *Mathematics Subject Classification.* — Primary 14G32, 14G05, 12F12, 14H10, 14H30; Secondary 11Gxx, 14Dxx.
***Key words and phrases.* —** Modular towers, Hurwitz spaces, inverse Galois theory, rational points.

Modular towers are due to M. Fried. They constitute a vertical development of the Hurwitz space theory. A modular tower is a tower of Hurwitz moduli 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, a prime divisor p of $|G|$ and r conjugacy classes of G of prime-to-p order. 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 [**Sem**] in this volume.

Persistence of rational points on high levels of a modular tower $\mathcal{H}_{G_n}(\mathbf{C}_n)$ 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. 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. A structured approach of the missing stage is given in Fried's paper [**Fri**] in this volume. A final section is devoted to the similar questions over ℓ-adic fields. We describe some recent results due to A. Cadoret, B. Deschamps, M. 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

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

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 [**Fried**], [**Ser90a**], [**Ser90b**] 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 [**FJ86**] 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 [**FJ86**, 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 [**BF02**, p.117] p.117. As a consequence, its p-Sylows are projective,

(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.

hence are free pro-p groups (by [**FJ86**, proposition 20.37]) of finite rank (by Nielsen-Schreier [**FJ86**, 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 ${}_p^n\tilde{G}$ the quotient ${}_p\tilde{G}/\ker_n$. Kernels $\ker_n$ are free pro-p groups of ${}_p\tilde{G}$ of finite rank and groups ${}_p^n\tilde{G}$ are finite (from [**FJ86**, 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 ${}_p^n\tilde{G} = \mathbb{Z}/p^{n+1}\mathbb{Z}$.

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

Proof. — Let $\phi_n : {}_p^{n+1}\tilde{G} \to {}_p^n\tilde{G}$ 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 $\mathrm{sni}_G(\mathbf{C}) \neq \varnothing$, 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 ${}_p^n\tilde{G}$ 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

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

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 $\sigma \in S_r$.

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

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

(2) By order of a conjugacy class, we mean the common order of its elements.

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, in which the Hurwitz spaces $\mathcal{H}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$ are 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 [**FK97**, appendix II p.173] or [**DF99**, §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* ([Fri95a] p.141,[BF02] proposition 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 ${}^n_p\tilde{G}$ 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 $D_{p^n} = \mathbb{Z}/p^n \rtimes \mathbb{Z}/2$ ($n > 0$ 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 π defined over k. The data $(\mathrm{Pic}^o(E), \pi)$ classically corresponds to some point on the modular curve $X_1(p^n)$ different from the cusps.

Conversely, let (E, π) be an elliptic curve given with a p^n-torsion point, both defined over k. The cover $E \to E/<\pi>$ is cyclic of degree p^n. The curve $E_o = E/<\pi>$ 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

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