Arithmetic and Moduli Spaces of Covers

Abstract. Moduli spaces of covers constitute an appropriate tool for certain arithmetic problems involving algebraic curves and rational functions. We first review the construction and the geometric properties of these spaces. Then we focus on the use of these spaces for arithmetic purposes, for example the inverse Galois problem, the Hilbert-Siegel problem, etc. Finally we consider some recents developments as the construction of modular towers.

1991 Mathematics Subject Classification. Primary 11Gxx, 14H10; Secondary 14H30, 12-xx.

1. Introduction

In a 1891 paper [Hu], A. Hurwitz explains how the set of degree d simple covers (*i.e.*, such that all fibers consist of at least $d-1$ points) of $\mathbb{P}^1$ can be endowed with a structure of complex manifold. Nowadays Hurwitz spaces refer more generally to moduli spaces of covers with specified automorphism group and with certain constraints on the ramification. The general construction and the development of these spaces are essentially due to M. Fried. W. Fulton and D. Mumford should also be cited for their works on moduli spaces of curves. This paper reviews the different stages of the theory with an emphasis on arithmetic applications. The main references are [Fr2], [DeFr1-4], [FrVö], [Fr6].

Moduli spaces of covers constitute an appropriate tool for certain diophantine problems involving algebraic curves and rational functions; more generally, for the arithmetic of covers of the line. For example, the Regular Inverse Galois Problem (over $\mathbb{Q}(T)$) amounts to finding $\mathbb{Q}$-rational points on these spaces. The general idea is to look at the constraints a given problem imposes on the intrinsic data of the covers in question, as the automorphism group and the ramification, and then to check whether there exist possible solutions on the associated moduli space, first over $\mathbb{C}$, and then over the ground field. The diophantine nature of the problem remains; but this approach somewhat classifies the equations by abstracting their structural properties.

This approach rests on the idea that group theory controls the arithmetic of covers, through their monodromy description. The Hilbert-Siegel problem illustrates this idea (§4.1): a concrete arithmetic problem — the irreducibility of polynomials

of the form $f(Y)-t$ ($f \in \mathbb{Q}[Y]$, $t \notin f(\mathbb{Q})$) — is solved by means of the classification of simple groups. More generally, the aim is to develop group-theoretic tools to investigate arithmetic properties of covers with fixed monodromy.

For applications, a major problem is to find rational points on Hurwitz spaces. There are results available over $\mathbb{Q}$ for "small" values of the parameters or over "large" fields K. These arithmetic questions require preliminary geometric investigations (§2): one should first determine the irreducible components of these spaces, their fields of definition, their geometric structure, for example whether they are (uni-)rational, etc.

The most striking achievements of the Hurwitz space theory concern the inverse Galois problem. We review this application in §3. There are others (§4): to the Hilbert-Siegel problem, the Davenport problem, the Mason-Stothers theorem, to a criterion for existence of rational points, etc. We give more details on one of them (the first one) to illustrate the method (§4.1 & §4.2).

New developments might come from modular towers (§5). These objects have been introduced by M. Fried [Fr6]. A modular tower is a tower of Hurwitz spaces that are naturally associated with a given Hurwitz space $\mathcal{H}$; each level of the tower maps onto $\mathcal{H}$ *via* a Frattini cover. The motivating example is the modular curve tower. This special case has many arithmetic implications (Serre's open image theorem, the Mazur-Merel theorem, etc.). One may ask whether such results carry over to the general case of modular towers.

Most developments discussed in this paper come from diophantine problems that have been greatly influenced by A. Schinzel. The modular approach to the Hilbert-Siegel and Davenport problems (§4) was motivated by his work on the variables separated equations $h(x) = g(y)$. Our paper [DeFr1] on rational points in families of curves (§4.4) also originates in a result of his with Lewis [LeSc].

2. Moduli spaces of covers

In this section we introduce Hurwitz spaces (§2.1), we briefly describe their construction (§2.2) and their geometric properties (§2.5); most of them come from the presentation of Hurwitz spaces as covers of the space $\mathcal{U}_r$ (§2.3). Some first examples are given in §2.4.

2.1. Presentation

The basic objects are the finite branched covers $f : X \to \mathbb{P}^1$ of the projective line $\mathbb{P}^1$, defined over the algebraic closure $\overline{K}$ of a field K of characteristic 0. More concretely a cover consists of an irreducible curve X defined over $\overline{K}$ and a non-constant rational function $f \in \overline{K}(X)$. There is a classical notion of isomorphism (the equivalence of covers). Equivalence classes have the following invariants.

Invariants.
• The monodromy group G of the cover, which is isomorphic to the Galois group of the Galois closure of the extension $\overline{K}(X)/\overline{K}(T)$ and is anti-isomorphic to the automorphism group of the Galois closure of the cover f.
• The degree $d = \deg(f)$ and the monodromy action $G \hookrightarrow S_d$ of G on an unramified fiber of the cover.
• The branch point set $\mathbf{t} = \{t_1, \ldots, t_r\} \subset \mathbb{P}^1(\mathbb{C})$. We denote by $\mathcal{U}_r$ the space parametrizing this data, *i.e.*, the variety of all sets of r distinct points from $\mathbb{P}^1$. The space $\mathcal{U}_r$ can be viewed as the projective space $\mathbb{P}^r$ with the discriminant locus removed: identify each $\mathbf{t}$ with the coefficients of the polynomial with roots $t_1, \ldots, t_r$. Also denote by $\mathcal{U}^r$ the subvariety of $(\mathbb{P}^1)^r$ of all r-tuples with no two equal coordinates. The variety $\mathcal{U}_r$ is the quotient of $\mathcal{U}^r$ by the action of S_r.
• The inertia $\mathbf{C} = \{C_1, \ldots, C_r\}$ [1], *i.e.*, the collection of conjugacy classes of branch cycles, or, equivalently, of generators of inertia groups, above the branch points.

Theorem 2.1 (Fried [Fr2])**.** *Suppose given a transitive representation $G \hookrightarrow S_d$ and an integer $r \geq 3$.*
(a) *There exists a coarse moduli space $\mathcal{H}_G$ for the category $\mathcal{C}_{r,G}$ of covers of $\mathbb{P}^1$ defined over $\mathbb{C}$, with r branch points and with monodromy group $G \subset S_d$.*
(b) *The space $\mathcal{H}_G$ is a smooth algebraic variety defined over $\mathbb{C}$ whose complex points exactly correspond to the isomorphism classes of objects of the category $\mathcal{C}_{r,G}$. We will denote by $[f]$ the point on $\mathcal{H}_G(\mathbb{C})$ corresponding to f. Furthermore the space $\mathcal{H}_G$ has the following property. If $\mathcal{P}$ is an algebraic variety that parametrizes a family $\mathcal{F}$ of covers in $\mathcal{C}_{r,G}$, then the map $\mathcal{P} \to \mathcal{H}_G$ sending each point $p \in \mathcal{P}$ to the point $[\mathcal{F}_p] \in \mathcal{H}_G$ is an algebraic morphism.*
(c) *$\mathcal{H}_G$ has a model defined over $\mathbb{Q}$. This model has the following properties. Let K be a field of characteristic 0. In every class $[f] \in \mathcal{H}_G(\overline{K})$, there exists a cover f defined over $\overline{K}$. Furthermore, the action of $G_K = G(\overline{K}/K)$ on $\mathcal{H}_G(\overline{K})$ coincides with the action on the corresponding covers. That is, $[f]^\tau = [f^\tau]$ for each $[f] \in \mathcal{H}_G(\overline{K})$ and each $\tau \in G_K$.*
(d) *For each cover f, the field $\mathbb{Q}([f])$ is called the field of moduli of f; under suitable assumptions* [DeDo1]*, it is the smallest field of definition of f.*
(e) *The application $\psi : \mathcal{H}_G \to \mathcal{U}_r$ mapping each $[f] \in \mathcal{H}_G(\mathbb{C})$ on the branch point set $\mathbf{t}$ of f is an étale morphism defined over $\mathbb{Q}$.*

[1] Some classes C_i can be repeated. Rather than a set, $\mathbf{C}$ should be regarded as a r-tuple modulo the action of S_r.

Variant: There is a similar statement for G-*covers* of $\mathbb{P}^1$ of group G (instead of covers). A G-cover is a Galois cover $f : X \to \mathbb{P}^1$ given together with an isomorphism $G(K(X)/K(T)) \simeq G$. One usually distinguishes the two situations by putting the superscript *ab* (for mere covers) or *in* (for G-covers) on $\mathcal{H}_G$. For simplicity, we will do it only when we find it necessary to the comprehension.

2.2. Construction

2.2.1. 1st approach (Fried [Fr2], Coombes-Harbater [CoHa], Fried-Völklein [FrVo], Emsalem [Em]). The different stages of the construction are the following ones.

• Set $\mathcal{H}_G(\mathbb{C}) \stackrel{\text{def}}{=} \coprod(\mathbf{t}, \varphi_{\mathbf{t}})$ where $\mathbf{t}$ runs over $\mathcal{U}_r(\mathbb{C})$ and $\varphi_{\mathbf{t}}$ over the set of all homomorphisms $\pi_1(\mathbb{P}^1 - \mathbf{t}) \to G \subset S_d$ (up to equivalence).

• Equip the set $\mathcal{H}_G(\mathbb{C})$ with a topology. To do so use the isomorphisms

$$\pi_1(\mathbb{P}^1 - \mathbf{t}) \stackrel{\chi}{\simeq} \pi_1(\mathbb{P}^1 - \mathbf{D})$$

where $\mathbf{D} = \{D_1, \ldots, D_r\}$ is a family of small disks D_i centered at t_i. Essentially, two points $(\mathbf{t}, \varphi_{\mathbf{t}})$ and $(\mathbf{t}', \varphi_{\mathbf{t}'})$ are close if $\mathbf{t}$ and $\mathbf{t}'$ are close in $\mathcal{U}_r(\mathbb{C})$ (i.e., in a small polydisk $\mathbf{D}$) and $\varphi_{\mathbf{t}}$ and $\varphi_{\mathbf{t}'}$ are equal *via* the isomorphism χ. For this topology, the projection $\psi : \mathcal{H}_G(\mathbb{C}) \to \mathcal{U}_r(\mathbb{C})$ is a topological cover.

• From the Grauert-Remmert theorem [GrRe], the cover ψ, whose base space $\mathcal{U}_r(\mathbb{C})$ is an algebraic variety, extends to a cover $\overline{\psi} : \overline{\mathcal{H}_G(\mathbb{C})} \to \mathbb{P}_r(\mathbb{C})$ of compact analytic spaces.

• This cover of compact analytic spaces comes from an algebraic morphism $\overline{\psi} : \overline{\mathcal{H}_G} \to \mathbb{P}_r$ defined over $\mathbb{C}$: this follows from the GAGA theorems [Se1].

• The morphism $\overline{\psi}$ is then shown to be defined over $\overline{\mathbb{Q}}$. This uses a general descent result for covers of a space defined over an algebraically closed field [Se2;Ch.6].

• Weil's descent [We]. Finally $\overline{\psi}$ is shown to be defined over $\mathbb{Q}$. For each $\tau \in G_{\mathbb{Q}}$, consider the application

$$\varepsilon_\tau : \left\{ \begin{array}{ccc} \mathcal{H}_G^\tau(\overline{\mathbb{Q}}) & \to & \mathcal{H}_G(\overline{\mathbb{Q}}) \\ [f]^\tau & \to & [f^\tau] \end{array} \right.$$

A first step is to show that the maps ε_τ are continuous (see below). Then it follows from $\psi\varepsilon_\tau = \psi^\tau$ that the ε_τ are analytic isomorphisms. But then, in view of the uniqueness of the algebraic structure on $\mathcal{H}_G$ (inducing the analytic structure), the ε_τ automatically are algebraic morphisms. Finally one checks the Weil cocycle condition: $\varepsilon_u \varepsilon_v^u = \varepsilon_{uv}$ $(u, v \in G_{\mathbb{Q}})$. Weil's descent criterion gives then both parts of conclusion (c) of Th.2.1.

Continuity of ε_τ. One may work over a cover $\widetilde{\mathcal{H}}$ of $\mathcal{H}_G$ (instead of $\mathcal{H}_G$ itself): the continuity of ε_τ follows from that of $\widetilde{\varepsilon}_\tau : \widetilde{\mathcal{H}}^\tau \to \widetilde{\mathcal{H}}$. There are several possible covers $\widetilde{\mathcal{H}}$ of $\mathcal{H}_G$:
- (Fried-Völklein): $\widetilde{\mathcal{H}} = \mathcal{H}_{\widetilde{G}}$ where $\widetilde{G}$ is an extension of G with trivial centralizer in $S_{\tilde{d}}$ (or with trivial center in the "G-cover" situation). The covers correspond-

ing to points on $\widetilde{\mathcal{H}}$ have no (non-trivial) automorphisms. This method requires a preliminary group-theoretic lemma asserting that every group G has an extension $\widetilde{G}$ satisfying the desired properties.
- (Emsalem): $\widetilde{\mathcal{H}}$ is the moduli space of covers $f \in \mathcal{H}_G$ given with a point above a base point t_o. These pointed covers have no automorphisms.

In both cases, absence of non-trivial automorphisms implies there exists a *family* $\widetilde{\mathcal{F}}$ of covers above $\widetilde{\mathcal{H}}$ (see §2.5.3). The continuity of $\widetilde{\varepsilon}_\tau$ follows. Here is why.

Assume that $([f_n]^\tau)_n$ converges to $[f]^\tau$ in $\widetilde{\mathcal{H}}^\tau$ (when $n \to +\infty$). There exists a family above $\widetilde{\mathcal{H}}^\tau$, namely the family $\widetilde{\mathcal{F}}^\tau$. The following can be deduced: *the* representative of $([f_n]^\tau)_n$ in the family $\widetilde{\mathcal{F}}^\tau$ converges to *the* representative of $[f]^\tau$ in the family $\widetilde{\mathcal{F}}^\tau$ (when $n \to +\infty$). Say that f_n $(n > 0)$ et f are *the* covers of the family $\widetilde{\mathcal{F}}$ that represent the points $[f_n]$ $(n > 0)$ and $[f]$. Then f_n^τ $(n > 0)$ and f^τ are *the* covers of the family $\widetilde{\mathcal{F}}^\tau$ that represent $([f_n]^\tau)$ $(n > 0)$ and $[f]^\tau$. Conclude: f_n^τ converges to f^τ; *a fortiori*, $[f_n^\tau]$ converges to $[f^\tau]$ on $\widetilde{\mathcal{H}}$.

2.2.2. 2nd approach (Bertin [Be]). J. Bertin uses purely algebraic techniques introduced by Mumford and Gieseker in the context of the construction of the moduli space of curves $\mathcal{M}_g$. He uses them to construct the moduli space $H_{g,G}$ of smooth curves of genus $g \geq 2$ given with an action of some group G. The space $\mathcal{M}_g$ is obtained from the Hilbert scheme of curves of genus g and of degree $m(2g-2)$ in $\mathbb{P}_n$ $(n = card(G)))$. Here one is only interested in curves that are left invariant by the action of G. The space $H_{g,G}$ is the subvariety of $\mathcal{M}_g$ fixed by the action of G (extended to the Hilbert scheme). This construction has the advantage of being appropriate in all characteristics. This approach also yields a compactification $\overline{H}_{g,G}$ of $H_{g,G}$; it provides an interesting description of points on the boundary of $\overline{H}_{g,G}$ as stable curves of genus g equipped with a *stable* action of G (see [Be] for precise definitions). This shed light on the process of coalescing branch points.

There is another difference with the preceding construction. If the objects corresponding to points on $H_{g,G}$ can be viewed as covers $X \to X/G$, the base is not fixed as it is for covers parametrized by points on $\mathcal{H}_G$. This makes the space $\mathcal{H}_G$ maybe more appropriate for diophantine considerations since that choice of the base corresponds to some choice of coordinate and so of an equation for the top curve. In Bertin's construction, the base is fixed only up to isomorphism. In fact the scheme $H_{g,G}$ is a quotient of the space $\mathcal{H}_G$ (for $g = 0$, the quotient by $\mathrm{PGL}(2,\mathbb{C}) = \mathrm{Aut}(\mathbb{P}^1)$). Consequently, interpretation of fields of definition of points on $H_{g,G}$ is somewhat different. For example, k-rational points on $H_{0,G}$ correspond, not to covers of $\mathbb{P}^1$ defined over k as k-points on $\mathcal{H}_G$ do, but to covers of a k-curve of genus 0 (which might be a conic without k-points).

For questions relating to the construction, the compactification and the reduction of moduli spaces of curves or covers, see also the papers [Fu], [DelMu], [HarMu] and the more recent [Ek], [Mo] and [Wew].

2.3. The cover $\mathcal{H}_G \to \mathcal{U}_r$

For $\mathbf{t} \in \mathcal{U}_r(\mathbb{C})$, there is a one-one correspondence between the fiber $\psi^{-1}(\mathbf{t})$ and

• the set of equivalence classes of covers with monodromy $G \subset S_d$ and fixed branch point set, or, equivalently,

• the set of surjective homomorphisms $\pi_1(\mathbb{P}^1 - \mathbf{t}) \to G$, up to equivalence in S_d, from the fundamental group $\pi_1(\mathbb{P}^1 - \mathbf{t})$ (which is isomorphic to the free group $F(x_1, \ldots, x_r)/x_1 \cdots x_r$) onto G, or, equivalently,

• the set $\mathrm{ni}_G^{\mathrm{ab}} = \left\{ (g_1, \ldots, g_r) \in G^r \mid \begin{array}{c} g_1 \cdots g_r = 1 \\ < g_1, \ldots, g_r > = G \end{array} \right\} / \mathrm{Nor}_{S_d}(G)$

The fundamental group of $\mathcal{U}_r(\mathbb{C})$ is a braid group, namely the Hurwitz braid group H_r. It has a presentation with generators and relations. More specifically, the Artin braid group B_r is the group on $r-1$ generators $Q_1, \ldots, Q_{r-1}$ with the relations

$$\begin{cases} Q_i Q_j = Q_j Q_i \text{ pour } |i-j| > 1 \\ Q_{i+1} Q_i Q_{i+1} = Q_i Q_{i+1} Q_i \text{ pour } 1 \le i \le r-2 \end{cases}$$

With the additional relation

$$Q_1 \cdots Q_{r-1} Q_{r-1} \cdots Q_1 = 1$$

one obtains the Hurwitz braid group. For a certain (standard) choice of an isomorphism $\pi_1(\mathbb{P}^1 - \mathbf{t}) \simeq F(x_1, \ldots, x_r)/x_1 \cdots x_r$, the monodromy action associated with the cover $\mathcal{H}_G \to \mathcal{U}_r$ is the action of H_r sur $\mathrm{ni}_G^{\mathrm{ab}}$ given by the following formula (which is already in [Hu]; see also [Fr2] and [FrVo]): for $\mathbf{g} = (g_1, \ldots, g_r) \in \mathrm{ni}_G^{\mathrm{ab}}$,

$$(\mathbf{g})Q_i = (g_1, \ldots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_i, g_{i+2}, \ldots, g_r), \quad i = 1, \ldots, r-1$$

Proposition 2.2. *Connected (and so irreducible*[2]*) components of $\mathcal{H}_G$ correspond to orbits of this action of H_r on $\mathrm{ni}_G^{\mathrm{ab}}$.*

Locally on $\mathcal{H}_G(\mathbb{C})$, inertia $\mathbf{C} = \{C_1, \ldots, C_r\}$ is constant (*e.g.* [DeFr1;Lemma 1.5]); thus inertia is constant on each connected component of $\mathcal{H}_G(\mathbb{C})$. Given $\mathbf{C}$, the subset of $\mathcal{H}_G(\mathbb{C})$ consisting of all points corresponding to covers with inertia $\mathbf{C}$ is denoted by $\mathcal{H}_G(\mathbf{C})(\mathbb{C})$; it is a disjoint union of connected components of $\mathcal{H}_G(\mathbb{C})$, which is connected (and irreducible) if and only if H_r acts transitively on the set

$$\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}} = \left\{ (g_1, \ldots, g_r) \in G^r \mid \begin{array}{c} g_1 \cdots g_r = 1 \\ < g_1, \ldots, g_r > = G \\ g_i \in C_i \text{ (up to the order)} \end{array} \right\} / \mathrm{Nor}_{S_d}(G)$$ [3]

[2] because the cover $\psi : \mathcal{H}_G \to \mathcal{U}_r$ is étale.

[3] Stricto sensu it is not the normalizer $Nor_{S_d}(G)$ that acts but the subgroup of elements that globally fix the set $\{C_1, \ldots, C_r\}$.

Without the indication "up to the order", the formula defines a subset of $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ denoted by $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$.

2.4. First examples

2.4.1. A family of degree 5 *polynomials* [DeFr1]. Take $G = S_5$ (embedded in itself), $r = 4$; $C_2 = C_3$ is the conjugacy class of 2-cycles, C_1 is the class of products of two disjoint 2-cycles and C_4 the class of 5-cycles. A first calculation provides the list of elements $(g_1, \ldots, g_4)$ from $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. Those for which $g_i \in C_i$, $i = 1, \ldots, 4$ and $g_4 = (54321)$ are the following ones (only g_1, g_2, g_3 are given):

(a) $((23)(45), (12), (14))$ (b) $((23)(45), (14), (24))$
(c) $((23)(45), (24), (12))$ (d) $((25)(34), (12), (35))$
(e) $((25)(34), (35), (12))$.

Points on the Hurwitz space $\mathcal{H}_G(\mathbf{C})$ correspond to covers $f : X \to \mathbb{P}^1$ of genus $g = 0$ ($2(5+g-1) = 2+1+1+4 = 8$). If the branch point with inertia generators in C_4 is required to be ∞, the cover $\mathbb{P}^1 \to \mathbb{P}^1$ is a polynomial cover.

It is easily checked that Q_1^2 et Q_2^2 act on the above list as follows:

$$\begin{cases} Q_1^2 : (a\ e\ c)(b\ d) \\ Q_2^2 : (a\ c\ b)(d\ e) \end{cases}$$

Thus the action H_r on $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ is transitive. The space $\mathcal{H}_G(\mathbf{C})$ is irreducible.

2.4.2. Irreducibility of $\mathcal{M}_g$. Given an integer $g \geq 0$, take $G = S_d$ where $d \geq g+1$, $r = 2g + 2d - 2$, $C_i = C$ is the class of 2-cycles, $i = 1, \ldots, r$. Every curve of genus g can be presented as a simple cover of $\mathbb{P}^1$, *i.e.*, with all inertia generators in C. This provides a surjective map $\mathcal{H}_G(\mathbf{C}) \to \mathcal{M}_g$. Some calculations due to Luröth et Clebsch [Cl] show that the action of H_r on $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ is transitive. The space $\mathcal{H}_G(\mathbf{C})$ is irreducible; so is its image $\mathcal{M}_g$. Historically, the Hurwitz space $\mathcal{H}_G(\mathbf{C})$ considered by Hurwitz is the first moduli space of covers that appears in the literature [Hu]. The above argument showing irreducibility of $\mathcal{M}_g$ in characteristic 0 is given in a paper of Severi [Sev]. The positive characteristic case is due to Fulton [Fu] and Deligne-Mumford [DelMu].

2.4.3. Irreducibility of modular curves (Fried). Modular curves can be presented as quotients of Hurwitz spaces of Galois covers of $\mathbb{P}^1$ with dihedral group as Galois group and with 4 branch points (see §3.1.4). As above, irreducibility of these Hurwitz spaces and hence of modular curves follows from transitivity of the associated action of H_4.

2.5. Geometric preliminaries

The use of Hurwitz spaces for arithmetic purposes depends on the knowledge of rational points on these spaces. In order to find K-rational points, a first step is to find irreducible components defined over K. The following criteria are available.

2.5.1. Irreducibility criteria.

• *General criterion.* The space $\mathcal{H}_G(\mathbf{C})$ is irreducible if and only if H_r acts transitively on $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. Furthermore, $\mathcal{H}_G$ is defined over $\mathbb{Q}$. Therefore $G_{\mathbb{Q}}$ permutes the spaces $\mathcal{H}_G(\mathbf{C})$. More specifically, we have, for each $\tau \in G_{\mathbb{Q}}$,

$$\mathcal{H}_G(\mathbf{C})^{\tau} = \mathcal{H}_G(\mathbf{C}^{\chi(\tau)})$$

where $\chi : G_{\mathbb{Q}} \to \mathbb{Z}/n\mathbb{Z}$ ($n = card(G)$) is the cyclotomic character. The field of definition of $\mathcal{H}_G(\mathbf{C})$ is a cyclotomic field, which can be explicitly determined, and which is equal to $\mathbb{Q}$ under some additional fairly simple assumptions, *e.g.* , if the classes $C_1, \ldots, C_r$ are rational (*i.e.*, invariant under raising them to any power relatively prime to the orders of their elements).

Observations: this criterion leads to complicated calculations, which can be performed in practice only for small values of r.

• *The Conway-Parker criterion* [FrVo;appendix]. Assume the group G has trivial center and that the Schur multiplier group is generated by commutators. If every class $C \neq \{1\}$ of G is repeated suitably often in $\mathbf{C}$, H_r acts transitively on $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. Consequently, $\mathcal{H}_G(\mathbf{C})$ is irreducible and defined over $\mathbb{Q}$.

Observations: this criterion can be used only for big values of r; furthermore, there is no known effective bound for r.

• *Harbater-Mumford inertia* (Fried) [Fr6]. An element $\mathbf{g} \in \mathrm{ni}_G(\mathbf{C})$ is said to be a HM representative if it is of the form $\mathbf{g} = (g_1, g_1^{-1}, \ldots, g_s, g_s^{-1})$. Fried showed that, under some technical hypotheses (including $Z(G) = \{1\}$), the HM representatives $\mathbf{g} \in \mathrm{ni}_G(\mathbf{C})$ are in the same orbit of H_r and that the corresponding irreducible component is defined over $\mathbb{Q}$.

2.5.2. (Uni-)rationality criteria. Recall a K-variety V is said to be *rational* if its function field $K(V)$ is a pure transcendental extension of K, or, equivalently, if V is birational over K to an open subset of a projective space $\mathbb{P}^r$; V is said to be *unirational* if $K(V)$ is contained in a pure transcendental extension of K. Some rationality criteria for the space $\mathcal{H}'_G(\mathbf{C})$ are available: the ' indicates that the branch points have been adjoined; more precisely, $\mathcal{H}'_G(\mathbf{C})$ is a connected component of the fiber product of $\mathcal{H}_G(\mathbf{C})$ with $\mathcal{U}^r$ (defined in §2.1) above $\mathcal{U}_r$. The function field of $\mathcal{H}'_G(\mathbf{C})$ is the function field of $\mathcal{H}_G(\mathbf{C})$ with the indeterminates $t_1, \ldots, t_r$ adjoined.

• *Rigidity* (Belyi, Fried, Matzat, Shih, Thompson; see [Se2]). The cardinality of the set $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$ [resp. $\mathrm{sni}_G(\mathbf{C})^{\mathrm{in}}$] can be explicitly computed, by hand or with a computer for small r; there also exists a formula involving characters of G. Rigidity is a set of hypotheses that guarantee that this cardinality is 1. In that case the

cover $\psi' : \mathcal{H}'_G(\mathbf{C})^{\mathrm{ab}} \to \mathcal{U}^r$ [resp. $\psi' : \mathcal{H}'_G(\mathbf{C})^{\mathrm{in}} \to \mathcal{U}^r$] is an isomorphism; the field of definition of a cover [resp. a G-cover] with inertia $\mathbf{C}$ is that of its branch points.

• *Another rationality criterion* [FrBi],[Fr4], [Fr5]. Assume $\mathcal{H}' = \mathcal{H}'_G(\mathbf{C})$ is irreducible. The cover $\mathcal{H}' \to \mathcal{U}^r$ can be viewed as a family $\mathcal{H}'_{t_2,\dots,t_r}$ of covers of $\mathbb{P}^1$ parametrized by the variables $t_2, \dots, t_r$. Ramification of these covers is known: the branch points are $t_2, \dots, t_r$ and the associated branch cycles are given by explicit formulas in an appropriate braid group. The Riemann-Hurwitz formula then yields the genus of the curve $\mathcal{H}'_{t_2,\dots,t_r}$. In some situations, inspection of ramification indices provides a rational point above some branch point. When that is the case and when the genus is 0, the variety $\mathcal{H}'$ is a rational variety.

• *Unirationality criteria* (Fried [DeFr4]). Fried established a unirationality criterion for the space $\mathcal{H}' = \mathcal{H}'_G(\mathbf{C})$. He also conjectures that, under certain assumptions on G and for suitably large r, the space $\mathcal{H}'_G(\mathbf{C})$ is unirational.

2.5.3. Existence of Hurwitz families. Hurwitz spaces have been defined as coarse moduli spaces. A natural question arises: is there a family above a given Hurwitz space $\mathcal{H}$, *i.e.*, a cover $\mathcal{T} \to \mathcal{H} \times \mathbb{P}^1$ such that, for each $[f] \in \mathcal{H}$, the fiber cover $\mathcal{T}_{[f]} \to [f] \times \mathbb{P}^1$ above $\{[f]\}$ is a cover equivalent to f? And when there exists a family, is it a universal family?

In his paper [Fr2], Fried shows the answer to both questions is positive when the covers parametrized by $\mathcal{H}$ have no non-trivial automorphism, or, equivalently, if $\mathrm{Cen}_{S_d}(G) = \{1\}$; $\mathcal{H}$ is then a *fine* moduli space. The main point is that Hurwitz families exist at least locally; absence of automorphisms then makes it possible to patch and glue these local families to provide a family above the whole space $\mathcal{H}$. This result, which he originally proved in the case of mere covers extends to the case of G-covers ([CoHa], [FrVo]); in that case absence of automorphisms corresponds to the condition $Z(G) = \{1\}$. Hurwitz spaces are also fine moduli spaces in the situation of *pointed* covers ([CoHa], [Em]); again the point is that pointed covers have no automorphism.

The case the objects do have non-trivial automorphisms is subtler. There is an obstruction to existence of a family above $\mathcal{H}$, which is of cohomological nature. In the situation of G-covers, the obstruction can be measured by a characteristic class in $H^2(\pi_1(\mathcal{H}), Z(G))$. The situation of mere covers leads to a non-abelian cohomological problem: the obstruction "lies" in the group $H^2(\pi_1(\mathcal{H}), \mathrm{Cen}_{S_d}(G))$. Proceeding as in [DeDo1], it is possible to reduce it in $H^2(\pi_1(\mathcal{H}), Z(G))$. From a theoretic viewpoint, the most appropriate tool is the notion of *gerbe*, introduced by Grothendieck and Giraud (see [DeDoEm]).

3. The inverse Galois problem

We review the applications of the Hurwitz space theory to the inverse Galois problem. We are actually interested in the *regular* form of the inverse Galois problem.

Problem. *Given a field K, is each finite group G the Galois group of some extension $E/K(T)$, regular over K* [4]*? or, equivalently, the automorphism group of a cover $f : X \to \mathbb{P}^1$, defined over K as G-cover?*

The original problem is stated over $\mathbb{Q}$ instead of $K(T)$. This form follows from the regular form over $\mathbb{Q}(T)$ thanks to Hilbert's irreducibility theorem. Given a finite group G, realizing G over $\mathbb{Q}(T)$ regularly amounts to finding $\mathbb{Q}$-rational points on a Hurwitz space $\mathcal{H}_G^{\rm in}$ (of G-covers). In the remainder of this section, we distinguish two kinds of results depending on whether one works with a fixed group (§3.1) or with a fixed field (§3.2). We refer to [De1] and [DeDes] for more details and a more complete bibliography.

3.1. The problem with G fixed over $\mathbb{Q}$ or over $\mathbb{Q}^{\rm ab}$

Remark 3.1. Working over $\mathbb{Q}^{\rm ab}$ is easier for two reasons:
- in general a K-rational point on a Hurwitz space actually corresponds to a cover with *field of moduli* equal to K (but not necessarily defined over K). But over $\mathbb{Q}^{\rm ab}$, the field of moduli is a field of definition (because $\mathbb{Q}^{\rm ab}$ is of cohomological dimension ≤ 1).
- that Hurwitz spaces $\mathcal{H}_G(\mathbf{C})$ are defined over $\mathbb{Q}$ requires some *rationality* properties of the classes C_i (§2.5.1). These additional hypotheses are not necessary over $\mathbb{Q}^{\rm ab}$: Hurwitz spaces $\mathcal{H}_G(\mathbf{C})$ are always defined over $\mathbb{Q}^{\rm ab}$.

3.1.1. The rigid case (Thompson, et al.). This is the simplest case (voir §2.5.2): $\mathcal{H}'_G(\mathbf{C})^{\rm in}$ is isomorphic to $\mathcal{U}^r$ over $\mathbb{Q}$ (*via* ψ'). The rigidity assumptions, which imply that the covers in question are determined by their branch points, are rather strong. Some groups however do satisfy them, for example, the symmetric group S_d, the Monster group [Th], etc. Strictly speaking, Hurwitz spaces are not necessary in the rigid context, but this case certainly initiated and promoted the modular method.

3.1.2. Other rationality situations (Matzat). Using the second rationality criterion above (§2.5.2), Matzat managed to realize (regularly) over $\mathbb{Q}(T)$ quite a few simple groups, in particular sporadic groups (only M_{23} has not yet been realized). The method has been developed by the Heidelberg school (Matzat, Malle, et al.); there are now many variants of the original criterion, many other groups have been realized (see [MaMa]). This approach is a big success of the Hurwitz space theory. However it is most likely not sufficient to handle the whole problem. This method considers groups one at a time and requires fairly complicated calculations. Furthermore the genus of $\mathcal{H}'_{t_2,\ldots,t_r}$ (see §2.5.2), which has to be 0 in the method, is not bounded in general [DeFr3;§4].

[4] c'est-à-dire, G=$G(E/K(T))$=$G(E\overline{K}/\overline{K}(T))$

3.1.3. An idea of Völklein-Strambach [StrVo]. The preceding method consists in finding a rational component $\mathcal{H}_G(\mathbf{C})$ that is defined over $\mathbb{Q}$; one uses the presentation of $\mathcal{H}_G(\mathbf{C})$ as a cover of $\mathcal{U}_r$. Völklein and Strambach fix a closed subvariety $\mathcal{P}$ of $\mathcal{U}_r$ and investigate whether a rational variety defined over $\mathbb{Q}$ can be found above $\mathcal{P}$. The variety $\mathcal{P}$ they fix is the variety of sets of r points that are symmetric with respect to the origin. The fundamental group of this variety can be explicitly described: they call it the symplectic braid group. The preceding method can be performed in the same manner; they obtain similar rationality criteria. For example they could realize regularly over $\mathbb{Q}(T)$ some groups $\mathrm{Sp}_n(4^s)$.

3.1.4. Dihedral groups and modular curves [Fr3] [DeFr3]. Deciding whether a Hurwitz space has rational points is a difficult problem. In the following example [DeFr3], it is indeed equivalent to finding rational points on modular curves.

Take $G = D_p = \mathbb{Z}/p \times^s \mathbb{Z}/2$, $r = 4$ and all the classes C_i, $i = 1, \ldots, 4$ equal to the class C of involutions of G. It is shown that there exists a surjective morphism defined over $\mathbb{Q}$

$$\chi : \mathcal{H} = \mathcal{H}_G^{\mathrm{in}}(\mathbf{C}) \to X_1(p) - \{\text{cusps}\}$$

Consequently, from Mazur's theorem, if $p > 7$, then $\mathcal{H}(\mathbb{Q}) = \emptyset$ and so the dihedral group D_p cannot be regularly realized over $\mathbb{Q}(T)$ with these constraints on ramification. In fact, some additional observations show the dihedral group cannot be realized with less than 6 branch points (while 3 suffice for the Monster group). We conjecture that for fixed r_o, only finitely many dihedral groups can be realized over $\mathbb{Q}(T)$ with less than r_o branch points. This would follow from conjectures of Mazur-Kamieny [MaKa] on the finiteness of primes that are order of rational points on an abelian variety over $\mathbb{Q}$ of given dimension.

Indications on the construction of χ. Suppose given a cover $f : E \to \mathbb{P}^1$ defined and Galois over $\mathbb{Q}$, of group D_p, with 4 branch points and with inertia $\mathbf{C}$. The Riemann-Hurwitz formula yields the genus g of E: $2g - 2 = 2p(-2) + 4p$, that is $g = 1$. One may assume E has a $\mathbb{Q}$-rational point (otherwise replace E by $Pic^o(E)$) and so is an elliptic curve over $\mathbb{Q}$. Elements of order p of D_p are automorphisms of E of order p defined over $\mathbb{Q}$. Thus they are translations by some p-torsion point p defined over $\mathbb{Q}$. The data (E, p) classically corresponds to a point on the modular curve $X_1(p)$ different from the cusps.

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

3.2. The problem with fixed K and for all G

Instead of trying to realize (regularly) a given group over the smallest possible field, one can fix a field K and try to realize as many groups as possible over K.

3.2.1. Reduction of the problem [FrVo]. Fried and Völklein proved that to each finite group G can be attached an infinite collection of Hurwitz spaces $\mathcal{H}_G^{\rm in}(\mathbf{C})$, irreducible and defined over $\mathbb{Q}$ and such that finding one K-rational on one of these spaces suffices to conclude G is a Galois group over $K(T)$ (regularly).

The main point is that these spaces $\mathcal{H}_G^{\rm in}(\mathbf{C})$ are irreducible. Fried and Völklein use the Conway-Parker criterion (§2.5.1). More precisely, they first replace G by an extension $\widetilde{G}$ of G satisfying the hypotheses of the Conway-Parker criterion ($Z(G) = \{1\}$, etc.); this requires a preliminary group-theoretic lemma (showing such an extension always exists). Then they consider a tuple $\widetilde{\mathbf{C}}$ where each non-trivial conjugacy class of $\widetilde{G}$ is repeated as many times as required by the Conway-Parker criterion. The space $\mathcal{H}_{\widetilde{G}}^{\rm in}(\widetilde{\mathbf{C}})$ is then irreducible, defined over $\mathbb{Q}$ and every K-rational point provides a regular realization over K of $\widetilde{G}$ and so also of G.

Observations. Conway and Parker do not give an effective bound for the number of times every conjugacy class should be repeated. There is now an alternative to using the Conway-Parker criterion, which is effective. It is the Harbater-Mumford inertia irreducibility criterion (see §2.5.1).

3.2.2. The results. This approach led to the proof of the Regular Inverse Galois Problem over the following fields K:

• K Pseudo Algebraically Closed of characteristic 0 (Fried-Völklein [FrVo]). Ultraproducts of finite fields are typical PAC fields. The Fried-Völklein result has this consequence: each group G can be regularly realized over $\mathbb{F}_p(T)$, for all but finitely many p.

• $K = \mathbb{Q}^{tr} = \{$totally real algebraic numbers$\}$ (Dèbes-Fried [DeFr3]),

• $K = \mathbb{Q}^{tp} = \{$totally p-adic algebraic numbers$\}$ (Dèbes [De2])

These two results use a theorem of Pop [Po;appendix] that asserts that a smooth variety defined over $\mathbb{Q}$ has totally p-adic points provided it has p-adic points (including $p = \infty$). Real points on Hurwitz spaces can explicitly determined because the action of complex conjugation on covers of $\mathbb{P}^1$ is perfectly known ([Hu], [KrNe], [DeFr2]). In order to construct Hurwitz spaces with p-adic points (*i.e.*, covers defined over $\mathbb{Q}_p$), one uses patching and glueing techniques for formal (or rigid) analytic spaces due to Harbater [Ha].

• B. Deschamps [Des] refined the preceding construction and showed that the Hurwitz space $\mathcal{H}_G^{\rm in}(\mathbf{C})$ containing p-adic points could be taken independent of p. More precisely he showed that to each finite group G can be attached an infinite collection of Hurwitz spaces $\mathcal{H}_G^{\rm in}(\mathbf{C})$, irreducible, defined over $\mathbb{Q}$ and with p-adic points for all primes p, including $p = \infty$.

• The above results have been generalized by Pop [Po]. The regular inverse Galois problem over $K(T)$) is known to be true for every *ample* field K. A field K is said

to be ample if every smooth curve defined over K has infinitely many K-rational points provided there is at least one. PAC fields, complete valued fields, the fields $\mathbb{Q}^{tp}$, etc. are ample.

4. Further arithmetic applications

This section gives four applications. We will develop the first one, which is concerned with the so-called Hilbert-Siegel problem (§4.1 and §4.2). Other applications to the Davenport problem and to the Mason-Stothers theorem (§4.3) will be mentioned. The section ends with a monodromy criterion for existence of rational points on covers (§4.4).

4.1. The Hilbert-Siegel problem [Fr5]

Fried named so the following problem (referring to an observation of Siegel [Si]). The problem is to determine all polynomials $h(Y) \in \mathbb{Q}[Y]$ such that $h(Y) - t$ is reducible in $\mathbb{Q}[Y]$ for infinitely many $t \in \mathbb{Z}-h(\mathbb{Q})$. The polynomial h will be assumed to be indecomposable (in the opposite case $h(Y) = h_1(h_2(Y))$ and $h(Y)-t$ is reducible for all $t = h_1(z)$, $z \in \mathbb{Q}$).

Theorem 4.1 (Fried)**.** *The only indecomposable polynomials $h(Y) \in \mathbb{Q}[Y]$ for which $h(Y) - t$ is reducible in $\mathbb{Q}[Y]$ for infinitely $t \in \mathbb{Z}-h(\mathbb{Q})$ are of degree 5.*

Sketch of proof. Consider a non-trivial factorization $h(Y) - T = Q(Y)R(Y)$ in $\overline{\mathbb{Q}(T)}$. Let $F \subset \overline{\mathbb{Q}(T)}$ be the field generated by the coefficients of Q and R. The field F is a proper extension of $\overline{\mathbb{Q}}(T)$ which corresponds to a cover $f : C \to \mathbb{P}^1$. Those $t \in \mathbb{Q}$ for which $h(Y) - t$ is reducible in $\mathbb{Q}[Y]$ correspond (except possibly finitely many of them) to $\mathbb{Q}$-rational specializations of fields F associated with all possible non-trivial factorizations $h(Y) - T$ in $\overline{\mathbb{Q}(T)}$ [5], or, equivalently, to values $f(\mathrm{m})$ assumed by f at some $\mathbb{Q}$-rational point m on the corresponding curves C.

Suppose $h(Y) - t$ is reducible in $\mathbb{Q}[Y]$ for infinitely many $t \in \mathbb{Z}-h(\mathbb{Q})$. From Siegel's theorem on finiteness of integral points on algebraic curves, there is at least one of the curves C (apart from the curve $h(y) = t$) that is $\mathbb{Q}$-birational to $\mathbb{P}^1$ and such that the function g has either a $\mathbb{Q}$-rational pole or two real quadratic poles. In other words, there exist non-constant rational functions $g_1(Z), \ldots, g_s(Z) \in \mathbb{Q}(Z)$ with $s \geq 1$ such that:

- $h(Y) - g_i(Z)$ reducible in $\overline{\mathbb{Q}}(Z)[Y]$, $i = 1, \ldots, s$,
- The denominator of each $g_i(Z)$ is of the form $(Z-a)^\ell$ with $a \in \mathbb{Q}$ or $(z^2+pZ+q)^\mu$ with $p^2 - 4q > 0$,

[5] Note that F must be a regular extension of $\mathbb{Q}$ to have such specializations

• $g_i(Z)$ cannot be obtained from $h(Z)$ by any substitution $(z \leftrightarrow (az+b)/(cz+d))$, $i = 1, \ldots, s$.

• For all but finitely many $t \in \mathbb{Z}-h(\mathbb{Q})$, $h(Y) - t$ is reducible in $\mathbb{Q}[Y]$ if and only if there exists $i \in \{1, \ldots, s\}$ such that $t = g_i(z)$ with $z \in \mathbb{P}^1(\mathbb{Q})$.

Fix an index i and set $g_i = g$. The first condition means that the fibered product of the two covers of $\mathbb{P}^1$ induced by $h(Y)$ and $g(Y)$ is reducible. The next step of Fried's proof is to show that the Galois closures over $\overline{\mathbb{Q}}(T)$ of the polynomials $h(Y) - T$ and $g(Y) - T$ are necessarily equal [Fr1]. Let G denote the Galois group of this extension. The two covers correspond to two transitive representations $T_h : G \to S_n$ and $T_g : G \to S_m$. The two covers are of genus 0; this provides, *via* the Riemann-Hurwitz formula, a first condition on T_h and T_g. The four points above translate as follows. Let $T_g(1)$ [resp. $T_h(1)$] be the stabilizer of 1 in the representation T_g [resp. T_h].

• The restriction of T_g to $T_h(1)$ is not transitive,

• There exists $\sigma \in G$ such that $T_h(\sigma)$ is a n-cycle and $T_g(\sigma)$ is, either a m-cycle, or the product of two μ-cycles,

• $T_h(1)$ contains no conjugate of $T_g(1)$.

Finally, the hypothesis "$h(Y)$ indecomposable" is classically equivalent to

• The representation $T_h : G \to S_n$ is primitive.

The rest of the proof is group-theoretic. Using the classification of simple groups, one can show that such representations only exist for $n = 5$, $m = 10$ and $G = S_5$ or $G = A_5$. □

Remark 4.2. This approach was recently developed by P. Mueller [Mu]. Let $f(T, Y) \in \mathbb{Q}[T, Y]$ be absolutely irreducible. Assume that, for infinitely many $t \in \mathbb{Z}$, $f(t, Y)$ is reducible but has no linear factor. Does it follow that $\deg_Y(f) = 5$? Mueller showed the answer is "Yes" if the Galois group of $f(T, Y)$ over $\overline{\mathbb{Q}}(T)$ is the symmetric group or if $\deg_Y(f)$ is prime.

4.2. An exceptional case with $\deg(h) = 5$ ([DeFr1], [DeFr4])

Fried's proof leads to a precise description of the exceptional cases of degree 5. We will study the following one. The covers h and g have group S_5 and $r = 4$ branch points. The branch cycles have the following shape (in S_5):

• for h: (2)(2) ; (2) ; (2) ; (5)

Denote by $\mathbf{C}$ the set of corresponding conjugacy classes of S_5. The situation is that of §2.4.1. The representation $T_h : S_5 \to S_5$ is the standard action of S_5 on $\{1, \ldots, 5\}$. The representation $T_g : S_5 \to S_{10}$ is given by the action of S_5 on the 10 pairs $\{i, j\}$ of distinct elements from $\{1, \ldots, 5\}$. (This exceptional case corresponds to the situation where one starts with a decomposition $h(Y) - T = Q(Y)R(Y)$ in

$\overline{\mathbb{Q}(T)}$ with a degree 2 factor). One obtains the following branch cycle shape (in S_{10}):

• for g: (2)(2)(2)(2) ; (2)(2)(2) ; (2)(2)(2) ; (5)(5)

We are concerned with the following question: does there exist a polynomial $h(Y) \in \mathbb{Q}[Y]$ such that hypotheses of this case hold and which is indeed exceptional, *i.e.*, for which $h(Y)-t$ is reducible in $\mathbb{Q}[Y]$ for infinitely many $t \in \mathbb{Z}-h(\mathbb{Q})$? Consider the Hurwitz space $\mathcal{H} = \mathcal{H}_{S_5}(\mathbf{C})$ [6]. From §2.4.1 $\mathcal{H}$ is irreducible. Furthermore as $\mathrm{Cen}_{S_5}(S_5) = \{1\}$ and $\mathrm{Cen}_{S_{10}}(S_5) = \{1\}$, $\mathcal{H}$ is a fine moduli space (§2.5.3): there exists above $\mathcal{H}$ a universal Hurwitz family $\mathcal{F}_5$ [resp. $\mathcal{F}_{10}$] of covers of degree 5 [resp. of degree 10] with the above invariants. The question rephrases as follows:

Question 4.3. *Does there exist a point $[h] \in \mathcal{H}(\mathbb{Q})$ such that*

(*) *the corresponding cover $h : \mathbb{P}^1 \to \mathbb{P}^1$ in the family $\mathcal{F}_5$ is a polynomial cover and the corresponding cover $\gamma_{[h]} : Y_{[h]} \to \mathbb{P}^1$ in the family $\mathcal{F}_{10}$ has the following properties: $\gamma_{[h]}(Y_{[h]}(\mathbb{Q})) \cap \mathbb{Z}$ is infinite and $\gamma_{[h]}(Y_{[h]}(\mathbb{Q})) \cap h(\mathbb{Q}) \cap \mathbb{Z}$ is finite?*

The cover $\gamma_{[h]}$ can be described more concretely: in terms of function fields, the cover $h : \mathbb{P}^1 \to \mathbb{P}^1$ corresponds to the extension $\overline{\mathbb{Q}}(y_1)/\overline{\mathbb{Q}}(T)$, where y_1 is one of the 5 roots in $\overline{\mathbb{Q}(T)}$ of $h(Y) - T$. The cover $\gamma_{[h]} : Y_{[h]} \to \mathbb{P}^1$ then corresponds to the extension $\overline{\mathbb{Q}}(y_1 + y_2, y_1 y_2)/\overline{\mathbb{Q}}(T)$.

Theorem 4.4 (Dèbes-Fried [DeFr4])**.** *The set of points $[h] \in \mathcal{H}(\mathbb{Q})$ such that (*) holds is Zariski-dense. Consequently, there exists indecomposable polynomials $h(Y) \in \mathbb{Q}[Y]$ such that $h(Y) - t$ is reducible in $\mathbb{Q}[Y]$ for infinitely many $t \in \mathbb{Z}-h(\mathbb{Q})$.*

Sketch of proof. The main steps of the proof are the following.

• $\mathcal{F}_{10}$ is a family of genus 0 covers. Furthermore, the set of points on $\mathcal{H}(\mathbb{C})$ for which the corresponding cover in the family $\mathcal{F}_{10}$ has the three following properties is Zariski-dense:

- the cover is defined over $\mathbb{R}$,
- ∞ is the branch cycle with inertia in C_4,
- both points in the fiber above ∞ are real.

This first point is a necessary condition for the conclusion of Th.4.4 to be true. For testing the conditions above, which are over the reals, pure group-theoretic criteria involving the set $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ are available. We refer to [DeFr4] for more details.

• $\mathcal{H}$ is unirational: Let $\mathcal{M} = (\mathbb{A}^1)^2 \times (\mathbb{A}^1-\{0\})^2$. For all $\mathbf{x} = (\beta, s, t, \alpha) \in \mathcal{M}$, the polynomial

[6] A priori, since S_5 is embedded, in itself on one hand, and in S_{10} on the other hand, the two situations should be distinguished. But it can be checked that the cardinality of $ni_G(\mathbf{C})^{\mathrm{ab}}$ is the same in both situations; therefore the corresponding Hurwitz spaces are isomorphic.

$$h_{\mathbf{x}}(y)=\alpha(\frac{y^5}{5}-s\frac{y^4}{4}+2ty^3-5st\frac{y^2}{2}+5t^2y)+\beta$$

induces a cover of the family $\mathcal{F}_5$ (up to equivalence). Conversely, each point $[h]\in\mathcal{H}$ that corresponds to a polynomial cover represents the equivalence class of a cover induced by some polynomial as above. Whence a map $\mathcal{M}\twoheadrightarrow\mathcal{H}$.

• $\mathcal{H}$ is defined over $\mathbb{Q}$ because the conjugacy classes in $\mathbf{C}$ are rational (§2.5.1).

• Calculation of the cover $\gamma_{[h_{\mathbf{x}}]}$ (denoted more simply by $\gamma_{\mathbf{x}}$). The degree 2 divisor consisting of the two points above ∞ (corresponding to the two 5-cycles from the 4th branch cycle) is rational over $\mathbb{Q}(\mathbf{x})$. A basis of the associated linear system provides an embedding of $Y_{[h_{\mathbf{x}}]}=Y_{\mathbf{x}}$ into $\mathbb{P}^2$. The image of this embedding is the conic $C_{\mathbf{x}}$:

$$U^2+V^2-3UV-5s\frac{U}{4}+5s\frac{V}{2}-5t=0$$

The map $\gamma_{\mathbf{x}}$ of the cover is obtained by writing out T in terms of U and V

$$T=\frac{\alpha}{2}\left[\left(\frac{U^5}{5}-U^4V+U^3V^2\right)-\frac{s}{4}(U^4-4U^3V+2U^2V^2)+\right.$$
$$\left.t(-3U^3+4U^2V)+\frac{5}{2}stU^2+\frac{25}{2}st^2\right]\ +\ \beta.$$

• Let $\mathcal{O}\subset\mathcal{M}(\mathbb{Q})$ be the set of points of the form $(\beta,c+d,cd,\alpha)$ with $c,d\in\mathbb{Q}$. The set $\mathcal{O}$ is Zariski-dense and for each $\mathbf{x}=(\beta,c+d,cd,\alpha)\in\mathcal{O}$, the conic $C_{\mathbf{x}}$ has a $\mathbb{Q}$-rational point, namely the point $(2c,\frac{c-5d}{2})$ (Cf. [DeFr1;Lemma 3.18]).

• Use Euler's parametrization to identify the conic $C_{\mathbf{x}}$ to $\mathbb{P}^1$ (for $\mathbf{x}\in\mathcal{O}$). More specifically we obtain

$$\begin{cases}U(w)=\dfrac{8cw^2+(-14c+10d)w+3c-25d}{4(w^2-3w+1)},\\ V(w)=\dfrac{12cw^2+(-11c+5d)w+2(c-5d)}{4(w^2-3w+1)}\quad\text{where } w=\dfrac{V-\frac{c-5d}{2}}{U-2c}\end{cases}$$

Substituting U and V back in the above formula for T yields a rational fraction $g_{\mathbf{x}}(w)$ of degree 10 and with denominator a power of a trinomial.

• It remains to study the values of this rational fraction; more specifically, we need to check that

- $g_{\mathbf{x}}(\mathbb{Q})\cap\mathbb{Z}$ is infinite for all $\mathbf{x}$ in a Zariski-dense subset of $\mathcal{O}$: this is done thanks to the explicit form of $g_{\mathbf{x}}$.

- $g_{\mathbf{x}}(\mathbb{Q})\cap h_{\mathbf{x}}(\mathbb{Q})\cap\mathbb{Z}$ is finite: this amounts to showing that the fiber product $\mathbb{P}^1\times_{\mathbb{P}^1}Y_{\mathbf{x}}$ of the covers $h_{\mathbf{x}}$ and $\gamma_{\mathbf{x}}$ has only finitely $\mathbb{Q}$-rational points lying above integers $z\in\mathbb{Z}$. This follows from Siegel's theorem if all irreducible components of this fiber product are of genus >0. A calculation using the Riemann-Hurwitz formula combined with Abhyankar's lemma [DeFr4] shows there are only two components: one is of genus 1 and the other of genus 2. $\square$

Remark 4.5 (Siegel families)**.** Section §4.2 can be regarded as a special case of a general problem, which is a converse to Siegel's theorem. Given an algebraic curve C, a rational function $f : C \to \mathbb{P}^1$, both defined over $\mathbb{Q}$ and a fractional ideal $\mathcal{A}$ of $\mathbb{Q}$, Siegel's theorem gives a necessary condition for $C(\mathbb{Q}) \cap f^{-1}(\mathcal{A})$ to be infinite: C is of genus 0 and f has either a unique rational pole or two conjugate quadratic real points. We consider the following converse. Let $\mathcal{P}$ be the parameter space of a smooth family $\Phi : \mathcal{P} \times \mathbb{P}^1 \to \mathcal{P} \times \mathbb{P}^1$, defined over $\mathbb{Q}$, of rational functions (of degree n). Assume that for all $\mathbf{p}$ in a Zariski-dense subset of $\mathcal{P}(\mathbb{Q})$, the function $\Phi_{\mathbf{p}}$ has two conjugate quadratic real points. The family Φ is then called a *Siegel family*. The question is whether Siegel's condition — $\Phi_{\mathbf{p}}(\mathbb{Q}) \cap \mathcal{A}$ infinite — holds for all $\mathbf{p}$ in a Zariski-dense subset of $\mathcal{P}(\mathbb{Q})$. We showed above that the family of degree 10 rational functions parametrized by the pull-back of $\mathcal{O}$ along the map $(\beta, c, d, \alpha) \to (\beta, c + d, cd, \alpha)$ satisfies this converse to Siegel's theorem.

4.3. Davenport, Mason, et al.

4.3.1. The Davenport problem. The Hilbert-Siegel problem is a special case of the general problem of classifying pairs of covers of $\mathbb{P}^1$ such that the fiber product is reducible. The approach was to consider the Galois closure of these covers and to interpret the problem in terms of bi-representations of the associated Galois group. The specific constraints given by Siegel's theorem were strong enough to conclude. The same approach can be used to tackle the following problem, stated by Davenport, which is to classify the polynomials $h(y), g(y) \in \mathbb{Z}[Y]$ that assume the same values modulo p, for all but finitely many p. The following result was proved by Fried [Fr5]; significant contributions are due to Schinzel (in the context of his work on the variables separated equations $h(x) = g(y)$ [DaLeSc], [Sc]) and to Feit (for the group-theoretic part [Fe1-3]).

Theorem 4.6. *Let K be a number field and O_K be its ring of integers. Let $h(Y), g(Y) \in O_K[Y]$ such that h is indecomposable and "linearly independent" from g (i.e., $h(y) \neq g(ay + b)$, $a, b \in \mathbb{C}$). Assume that, for all but finitely many primes p of O_K, the value sets $h(O_K/p)$ and $g(O_K/p)$ of h and g over O_K/p coincide. Then we have*

$$\begin{cases} \deg(h) = \deg(g) = n \in \{7, 11, 13, 15, 21, 31\} \\ [\mathbb{Q}(\zeta_n) \cap K : \mathbb{Q}] > 1 \end{cases}$$

In particular, if $K = \mathbb{Q}$, no polynomials $h(Y)$, $g(Y)$ satisfy such hypotheses.

Each of the degrees n above is actually exceptional over $\mathbb{Q}(\zeta_n)$: there are pairs $h(Y), g(Y) \in O_{\mathbb{Q}(\zeta_n)}[Y]$ satisfying the hypotheses of the theorem and such that $\deg(h) = n$; exceptional pairs (h, g) have recently been classified by P. Cassou-Noguès and J-M. Couveignes [CaCou]. On the other hand, for $K = \mathbb{Q}$, no example is known even with h decomposable.

4.3.2. On the Mason-Stothers theorem [Za1]. Hurwitz spaces also appear in a work of U. Zannier. He is interested in the cases of equality in the Mason-Stothers theorem [7] (polynomial analog of the *abc* conjecture — if $a, b, c \in \mathbb{C}[Y]$ are three relatively prime polynomials such that $a-b=c$, then the number of distinct roots in $\mathbb{C}$ of *abc* is bigger than the maximum of the degrees of a, b and c —). Zannier associates to such a triple (a, b, c) the cover $f : \mathbb{P}^1 \to \mathbb{P}^1$ induced by the rational function a/b. Equality in the Mason-Stothers theorem translates in terms of ramification of the cover: the branch points are 0, 1 and ∞ and there are additional conditions on the ramification indices. He can in fact restates the whole problem only in terms of existence of subgroups de S_n generated by elements $\sigma_1, \ldots, \sigma_{r-1}$ satisfying certain conditions. Then he gives a combinatoric construction of such subgroups.

Hurwitz spaces explicitly appear when it comes to rationality questions. It is Riemann's existence theorem that makes it possible to associate to the constructed subgroups of S_n a cover $f : X \to \mathbb{P}^1$ (of genus 0), and so a rational function a/b. But polynomials a and b have *a priori* coefficients in $\mathbb{C}$. Existence of polynomials with coefficients in $\mathbb{Q}$ is equivalent to showing the cover f can be defined over $\mathbb{Q}$, and so to finding $\mathbb{Q}$-rational points on Hurwitz spaces. Zannier explains that this is possible under certain additional assumptions that guarantee the cover f is unique: that is the "rigid" case. He suggests that more generally results on the arithmetic of Hurwitz spaces could be used. The value of finding polynomials with coefficients in $\mathbb{Q}$ is that one can expect to deduce, by specialization, examples close to cases of equality in the numerical *abc* conjecture.

4.4. A criterion for existence of rational points [DeFr1]

Our final application is a criterion that uses the very modular structure of Hurwitz spaces — precisely the monodromy of the cover $\mathcal{H}_G(\mathbf{C}) \to \mathcal{U}_r$ — to detect rational points on covers parametrized by points of $\mathcal{H}_G(\mathbf{C})$.

Let $f : X \to \mathbb{P}^1$ be a cover defined over a field K. *Via* the choice of an isomorphism $\pi_1(\mathbb{P}^1-\mathbf{t}) \simeq F(x_1, \ldots, x_r)/x_1 \cdots x_r$, f can be viewed (up to isomorphism) as the data consisting of the branch point set $\mathbf{t} = \{t_1, \ldots, t_r\}$ and a r-tuple $\mathbf{g} = (g_1, \ldots, g_r) \in \mathrm{ni}_G(\mathbf{C})$, where G is the group of the cover f and $\mathbf{C}$ its inertia. For $i = 1, \ldots, r$, write g_i as a product of disjoint cycles in S_d: $g_i = \beta_{i1} \cdots \beta_{i\ell_i}$. Classically, for $i = 1, \ldots, r$, points in the fiber $f^{-1}(t_i)$ correspond to cycles β_{ij} of the decomposition of g_i, the length of each cycle corresponding to the ramification index. Also it is known (*e.g.* [Fr2;p.62]) that the action of G_K on the branch points has the following property. For $\tau \in G_K$ and $i = 1, \ldots, r$, if $t_i^\tau = t_j$, then there exists $\gamma \in S_d$ and an integer a relatively prime to the order of elements from C_i such that $C_j = \gamma C_i^a \gamma^{-1}$. It follows that, for each $i \in \{1, \ldots, r\}$, the divisor $\sum_j (t_j)$,

[7] Zannier [Za2] points out that this result, which is usually credited to Mason, actually appeared in an older paper of Stothers [St].

where j runs over the set I of indices such that $C_j = \gamma C_i^a \gamma^{-1}$ for some γ and a as above, is a K-rational divisor of $\mathbb{P}^1$.

Fix an index $i \in \{1, \ldots, r\}$ and the length λ of some cycle g_{ik}. Denote the set of cycles of length λ appearing in the decomposition of some g_{jk} ($j \in I$) by $g(i, \lambda)$ and the set of points of X corresponding to cycles in $g(i, \lambda)$ by $P_f(i, \lambda)$. Consider the subgroup

$$H_{\mathbf{g}} = \{Q \in H(r) | \exists \gamma \in S_d, Q(\mathbf{g}) = (\gamma g_1 \gamma^{-1}, \ldots, \gamma g_r \gamma^{-1})\}$$

Assume the group G of the cover has trivial centralizer $\mathrm{Cen}_{S_d}(G)$ in S_d. Then the element γ attached to each element $Q \in H_{\mathbf{g}}$ is unique. Action of Q composed with conjugation by γ^{-1} fixes the r-tuple $\mathbf{g}$ and so permutes the cycles in $g(i, \lambda)$; thus we get an action of $H_{\mathbf{g}}$ on $g(i, \lambda)$.

In addition to $\mathrm{Cen}_{S_d}(G) = \{1\}$, assume that $H(r)$ acts transitively on $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$. Then the action of $H_{\mathbf{g}}$ on $g(i, \lambda)$ does not depend (up to equivalence) on the r-tuple $\mathbf{g} \in \mathrm{sni}_G(\mathbf{C})$ (see [DeFr1;Remark 3.13]). Set $\mathcal{H} = \mathcal{H}_G(\mathbf{C})$. The transitivity condition above gives that the Hurwitz space $\mathcal{H}$ is irreducible. From the hypothesis $\mathrm{Cen}_{S_d}(G) = \{1\}$, the covers parametrized by $\mathcal{H}$ have no automorphisms; consequently, there exists a universal Hurwitz family $\mathcal{F}$ above $\mathcal{H}$. Denote by $f_{\mathrm{gen}} : X_{\mathrm{gen}} \to \mathbb{P}^1$ the generic cover of the family $\mathcal{F}$ and let $F = \overline{\mathbb{Q}}(\mathcal{H})$ be the function field of $\mathcal{H}$, which is a field of definition of f_{gen}.

Theorem 4.7 (Dèbes-Fried) [DeFr1;Th.3.14]**.** *Orbits of $H_{\mathbf{g}}$ on $g(i, \lambda)$ exactly correspond to orbits of G_F on $P_{f_{\mathrm{gen}}}(\mathbf{g}, \lambda)$.*

This is a statement on the generic cover of $\mathcal{F}$. A nice property of Hurwitz families is that this kind of statement, once established on the generic cover, automatically carries over to all covers of the family. Here is a practical application of Th.4.7. Assume the group $H_{\mathbf{g}}$ has a unique [8] orbit of given length ℓ. It follows from Th.4.7 that for each cover $f : X \to \mathbb{P}^1$ of the Hurwitz family $\mathcal{F}$, there exists a divisor of X of length ℓ that is rational over the field of definition of f.

When X is of genus 0 or 1, Th.4.7 provides a practical criterion for existence of rational points on X: combine the preceding statement with the following fact [DeFr1; Cor3.15 et Cor.3.17]. In order to find a rational point on a genus 0 curve, it suffices to find an odd degree rational divisor; on a genus 1 curve, it suffices to find rational divisors with relatively prime degrees. More generally, this leads to the notion of rational points produced by ramification [DeFr1;§3.2]: these are rational points that, as divisors, are in the group generated by the rational divisors with support in the set of ramified points on X and the divisors of rational functions. Natural questions arise [DeFr1;§3 & §4]: for example, for $g = 0$ or $g = 1$, to what extent generic existence of rational points on X is equivalent to generic existence of rational points produced by ramification (in which case Th.4.7 would be a decisive

[8] Let k the minimal field of definition of $\mathcal{H}$. Uniqueness assures here that the orbit in question will be, not only an orbit the Galois group $G_{\overline{\mathbb{Q}}(\mathcal{H})}$ but also of the Galois group $G_{k(\mathcal{H})}$.

criterion as to existence of rational points on the generic cover of the family)? Concerning rational points produced by ramification, one can also ask whether their generic existence is equivalent to their existence on every curve X of the family? Thanks to Hilbert's irreducibility theorem, it is actually shown that this second question has a positive answer for $g = 0$ or $g = 1$ [DeFr1;Th.3.11]. This second question naturally relates to the similar one for which arbitrary rational points are considered (and not only those produced by ramification). From a paper of Lewis and Schinzel [LeSc] (which motivated [DeFr1]), the result still holds for families of curves of genus 0; one suspects however that the result is false for $g \geq 1$.

5. Modular towers

Modular towers constitute a recent development of the Hurwitz space theory. This section presents their construction (§5.1). The motivating example is the tower of modular curves (§5.2). This example naturally leads to arithmetic questions on general modular towers (§5.3). Modular towers are due to Fried; this section is a brief exposition of his paper [Fr6].

5.1. Construction

Suppose given a finite group $G \subset S_d$, a prime divisor p of $|G|$, an integer $r > 0$ and a collection $\mathbf{C} = \{C_1, \ldots, C_r\}$ of conjugacy classes of G whose elements are of order relatively prime to p.

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 $(\alpha_1, \ldots, \alpha_r > 0)$. The fiber product of two Frattini covers is a Frattini cover. 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. 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 $\ker(\psi)$ a p-group. This object is called the universal p-Frattini cover of G and is denoted by ${}_p\tilde{G}$. 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 quotients 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 denote by ${}^n_p\tilde{G}$ the quotient ${}_p\tilde{G}/\ker_n$ $(n \geq 0)$. For example, for $G = \mathbb{Z}/p\mathbb{Z}$, we have $\ker_n = p^{n+1}\mathbb{Z}_p$ and ${}^n_p\tilde{G} = \mathbb{Z}/p^{n+1}\mathbb{Z}$.

Lemma 5.1. *If C is a conjugacy class of elements of ${}^n_p\tilde{G}$ of order ρ prime to p, then there exists a unique conjugacy class ${}^{n+1}_p\tilde{G}$ that lifts C and whose elements are of order ρ.*

Proof. Let $\phi : {}^{n+1}_p\tilde{G} \to {}^n_p\tilde{G}$ be the natural surjection. Let $g \in C$ and $H = \phi^{-1}(< g >)$. 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. □

Thanks to this lemma, one can define, for each integer $n \geq 0$, a 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 a lifting of C_i^n of the same order, $i = 1, \ldots, r$ (by order we mean here the order of elements in the class). This definition naturally provides, for each $n \geq 0$, a map

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

In the mere cover case, we also need to define, in a compatible way, a representation T_n of ${}^n_p\tilde{G}$ in a symmetric group $(n \geq 0)$. Denote the stabilizer of 1 in the representation $G \subset S_d$ by $G(1)$ and select the prime p not dividing the order of $G(1)$. Using the Schur-Zassenhaus lemma as above, we obtain that there exists a copy of $G(1)$ in the preimage of $G(1)$ by the morphism ${}^n_p\tilde{G} \to G$, which is unique up to conjugation $(n \geq 0)$. Define T_n to be the left multiplication on the left cosets in ${}^n_p\tilde{G}$ modulo this copy of $G(1)$ $(n \geq 0)$.

For each $n \geq 0$, we can now associate a Hurwitz space

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

For each $n \geq 0$, there is 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 $(G \subset S_d, p, \mathbf{C})$.

5.2. The dihedral group case

As in §3.1.4, take $G = D_p = \mathbb{Z}/p \times^s \mathbb{Z}/2$, $r = 4$ and all classes $C_1, \ldots, C_4$ equal to the class C of involutions of G. We have ${}_p\tilde{D}_p = \mathbb{Z}_p \times^s \mathbb{Z}_2 := D_{p^\infty}$ and for each $n \geq 0$, ${}^n_p\tilde{D}_p = D_{p^n}$. From §3.1.4 there exists a surjective morphism defined over $\mathbb{Q}$:

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

Furthermore, for each $n > 0$, we have a commutative diagram

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

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 $(G \subset S_d, p, \mathbf{C})$ to the modular curve tower $(X_1(p^n))_{n>0}$.

5.3. Arithmetic questions on modular towers

As before, we are interested in fields of definition of irreducible components and possible existence of rational points on these components. The modular curve example will serve us as a guide to investigate these questions.

5.3.1. Irreducible components. Let $\mathcal{T}$ be an irreducible component of $\mathcal{H}_1$ (corresponding to an orbit $\mathcal{O}$ of H_r on $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ (or $\mathrm{ni}_G(\mathbf{C})^{\mathrm{in}}$ in the G-cover case as in §5.2)). Our first concern is whether a component has a lift at level n of the tower.

Proposition 5.2 [Fr6]**.** *For $\mathbf{g} \in \mathcal{O}$, define the subset $\nu_n(\mathbf{g}) \subset {}_p^n\tilde{G}$ by*

$$\nu_n(\mathbf{g}) = \left\{ \tilde{g}_1 \cdots \tilde{g}_r \;\middle|\; \begin{array}{l} \tilde{g}_i \in {}_p^n\tilde{C}_i, i = 1, \ldots, r \text{ (up to the order)} \\ \text{and } \tilde{\mathbf{g}} \text{ lifts } \mathbf{g} \end{array} \right\}$$

(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 $\mathrm{ni}_{{}_p^n\tilde{G}}(\mathbf{C}^n)$. 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 $\tilde{g}_i \in {}_p^n\tilde{C}_i$, $i = 1, \ldots, r$ (up to the order). To conclude that $\tilde{\mathbf{g}} \in \mathrm{ni}_{{}_p^n\tilde{G}}(\mathbf{C}^n)$ 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 ${}_p^n\tilde{G}$. This follows from the Frattini property of the cover ${}_p^n\tilde{G} \to G$.

Let $\mathbf{g}^o, \mathbf{g} \in \mathcal{O}$; $\mathbf{g} = (\mathbf{g}^o)Q$ for some $Q \in H_r$. Clearly if $\tilde{\mathbf{g}}_n^o$ is a lift of $\mathbf{g}^o$, then $\tilde{\mathbf{g}}_n = (\mathbf{g}_n^o)Q$ 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. □

Remark 5.3. The proof of (b) shows a common use of the Frattini property. Frattini covers have this other property: they cannot be split (unless they are isomorphims). Somehow being split and being Frattini are opposite to one another. Also recall this useful fact: the universal Frattini cover is a projective cover [FrJa].

A component $\mathcal{T}$ of $\mathcal{H}_1$ is said to be *obstructed* at nth level 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 of the tower 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 basically 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 components defined over $\mathbb{Q}$.

Theorem 5.4 [Fr6;Th.3.16]**.** *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 irreducible components. Assume $\mathcal{H}_1$ is defined over $\mathbb{Q}$ (e.g. $C_1, \ldots, C_r$ are rational). Then $G_{\mathbb{Q}}$ permutes the components $\mathcal{H}_{1i}$. More precisely, for each $\tau \in G_{\mathbb{Q}}$, we have*

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

where $\chi : G_{\mathbb{Q}} \to (\mathbb{Z}_p)^{\times}$ is the cyclotomic character modulo $(p^n)_{n\geq 1}$. [9]

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 $\tau \in G_{\mathbb{Q}}$, $\mathcal{H}_{1i}$ and $\mathcal{H}_{1i}^{\tau}$ have the same invariant ν. From the second condition, $\mathcal{H}_{1i} = \mathcal{H}_{1i}^{\tau}$, for each $\tau \in G_{\mathbb{Q}}$.

5.3.2. Projective system of rational points. Consider a projective system of rational points $(\mathbf{p}_n)_{n>0}$ on the modular curve tower. Each point $\mathbf{p}_n$ corresponds to a p^n-torsion point on an elliptic curve E (the same curve for all n). Assume E is defined over a field K. The group G_K acts on the p-torsion points of E: this is the action of G_K on the Tate $\mathbb{Z}_p$-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 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:

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

In the case of modular curves, a celebrated theorem of Serre yields that, if K is a number field,

[9] For each $n\geq 1$, the element $\nu_n(\mathcal{O}) \in \frac{n}{p}\tilde{G}$ 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.

(**) given a projective systems of points $(\mathbf{p}_n)_{n>0}$ above $j \in \mathbb{P}^1(K)$ and a finite extension F/K, $\mathbf{p}_n \notin \mathcal{H}_n(F)$, for all but finitely many n.

Indeed, there are only finitely many F-rational p-torsion points on a given elliptic curve over K. One may think that such a statement (with $\mathbf{t} \in \mathcal{U}_r(K)$ replacing $j \in \mathbb{P}^1(K)$ and possibly with some additional assumptions) carries over to the general situation of modular towers. In particular, it seems natural to fix a projective system $(\mathcal{T}_n)_{n>0}$ of irreducible components defined over K such that for each $n > 0$, $\mathbf{p}_n \in \mathcal{T}_n(K)$.

References

[Be] J. Bertin, Compactification des schémas de Hurwitz, C. R. Acad. Sci. Paris, 322, Série I, 1063–1066, (1996) [+ preprint, même titre, 49 pages, (1996)].

[CaCou] P. Cassou-Noguès and J-M. Couveignes, Factorisation explicite de $g(y)-h(z)$, preprint, (1997).

[Cl] A. Clebsch, Zur Theorie der Riemann' schen Fläche, Math. Ann., 6, (1872), 216–230.

[CoHa] K. Coombes and D. Harbater, Hurwitz families and arithmetic Galois groups, Duke Math. J., 52, (1985), 821–839.

[DaLeSc] H. Davenport and D.J. Lewis and A. Schinzel, Equations of the form $f(x) = g(y)$, Quart. J. Math. Oxford, 12, (1961), 304–312.

[De1] P. Dèbes, Groupes de Galois sur K(T), Sém. Th. Nombres de Bordeaux, 2, (1990), 229–243.

[De2] P. Dèbes, Covers of $\mathbb{P}^1$ over the p-adics, in Recent Developments in the Inverse Galois Problem, Contemporary Math., 186, (1995), 217–238.

[DeDes] P. Dèbes and B. Deschamps, The Inverse Galois problem over large fields, in Geometric Galois Action, London Math. Soc. Lecture Note Series, Cambridge University Press, (1997), 119–138.

[DeDo1] P. Dèbes and J-C. Douai, Algebraic covers: field of moduli versus field of definition, Annales Sci. E.N.S., 4ème série, 30, (1997), 303–338.

[DeDo2] — Gerbes and covers, Comm. Algebra, (to appear).

[DeDoEm] P. Dèbes, J-C. Douai et M. Emsalem, Familles de Hurwitz et cohomologie non abélienne, preprint, (1998).

[DeFr1] P. Dèbes and M. Fried, Arithmetic variation of fibers in algebraic families of curves. Part 1: Criteria for existence of rational points, J. fur die reine und angew. Math., 409, (1990), 106–137.

[DeFr2] — Rigidity and real residue class fields, Acta Arith. 56, 4, (1990), 13–45.

[DeFr3] — Non rigid situations in constructive Galois Theory, Pacific J. Math., 163 #1, (1994), 81–122.

[DeFr4] — Integral specialization of families of rational functions, Pacific J. Math., (to appear).

[DelMu] Deligne, P., Mumford, D., The irreducibility of the space of curves of given genus. Publ. Math. de l'I.H.E.S. 36 (1969), 75–109.

[Des] B. Deschamps, Existence de points p-adiques pour tout p sur un espace de Hurwitz, Contemporary Mathematics, 186, (1995), 239–247.

[Ek] Ekedahl,T., Boundary behaviour of Hurwitz schemes. In: The moduli space of curves (ed. par R. Dijkgraaf, C. Faber et G. van der Geers; Progress in Math. 129), 173–198, Birkhäuser 1995.

[Em] M. Emsalem, Familles de revêtements de la droite projective, Bull. Soc. Math. France 123, (1995), 47–85.

[Fe1] W. Feit, Automorphisms of Symmetric Balanced Incomplete Block Designs, Math. Z., 118, (1970), 40–49.

[Fe2] — On Symmetric Balanced Incomplete Block Designs with Doubly Transitive Automorphism Groups, Journal of Combinatorial Theory (A), 14, (1973), 221–247.

[Fe3] — Some consequences of the classification of finite simple groups, Proceedings of Symposia in Pure Math., 37, (1980), 175–181.

[Fr1] M. Fried, The fields of definition of function fields and a problem in the reducibility of polynomials in two variables, Illinois J. Math., 17/1, (1973), 128–146.

[Fr2] — Fields of definition of function fields and Hurwitz families, Groups as Galois groups, Comm. Alg., 1 (1977), 17–82.

[Fr3] — Exposition of an arithmetic-group theoretic connection via Riemann's existence theorem, Proc. Symposia Pure Math., 37 (1980), 571–602.

[Fr4] — On reduction of the inverse Galois group problem to simple groups, Proc. Rutgers Group Theory Year, (1983/84), Gorenstein, Lyons, O'Nan, Sims, Aschbacher and Feit ed., Cambridge Univ. Press, (1984), 289–301.

[Fr5] — Rigidity and applications of the classification of simple groups to monodromy, preprint, (1987).

[Fr6] —, Introduction to modular towers, in Recent Developments in the Inverse Galois Problem, Contemporary Math. 186, (1995), 111–171.

[FrBi] M. Fried and R. Biggers, Moduli spaces of covers and the Hurwitz monodromy group, J. fur die reine und angew. Math., 335, (1982), 87–121.

[FrJa] M. Fried and M. Jarden, Field Arithmetic, Springer-Verlag, (1986).

[FrVö] M. Fried and H. Völklein, The inverse Galois problem and rational points on moduli spaces, Math. Annalen, 290 (1991), 771–800.

[Fu] W. Fulton, Hurwitz schemes and irreducibility of moduli of algebraic curves, Ann. Math., series 2, 90, (1969), 543–573.

[GrRe] H. Grauert and R. Remmert, 3 notes in C.R.A.S. Paris, 245, Série I, 819–822 / 822–825 / 918–921, (1957).

[Ha] D. Harbater, Galois covering of the arithmetic line, Proc. of the NY Number Thy. Conf., LNM, 1240, Springer, (1985).

[HarMu] Harris,J., Mumford, D., On the Kodaira dimension of the moduli space of curves. Invent. Math. 67 (1982), 23–86.

[Hu] A. Hurwitz, Über Riemann'sche Flächen mit gegebenen Veizweigungspunkten, Math. Ann., 39, (1891), 1–61, [= Mathematische Werke, I, 321–383].

[KrNe] A. Krull and J. Neukirch, Die Struktur der absoluten Galois gruppe über dem Körper $\mathbb{R}(T)$, Math. Ann., 193 (1971), 197–209.

[LeSc] D.J. Lewis and A. Schinzel, Quadratic diophantine equations with parameters, Acta Arith. 37, (1980), 133–141.

[MaKa] B. Mazur and S. Kamienny, Rational torsion of prime order in elliptic curves over number fields, preprint 6/92.

[MaMa] B. H. Matzat and G. Malle, Inverse Galois theory, preprint, University of Heidelberg, (1996).

[Me] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Inv. Math., (1996), 437–449.

[Mo] Mochizuki, S., The geometry of the compactification of the Hurwitz scheme. Publ. of the R.I.M.S (Kyoto University) 31 (1995), 355–441.

[Mu] P. Müller, Hilbert's irreducibility theorem for polynomials of prime degree and for generic polynomials, preprint, (1996).

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

[Sc] A. Schinzel, Reducibility of polynomials of the form $f(x)-g(y)$, Colloquium Math., 18, (1967), 213–218.

[Se1] J-P. Serre, Géométrie algébrique et géométrie analytique, Ann. Inst. Fourier, 6, (1956), 1–42, [= C.P. no32].

[Se2] —, Topics in Galois Theory, Jones and Bartlett Publ., Boston, (1992).

[Sev] F. Severi, Vorlesungen über algebraische Geometrie, (translated by E. Löffler), Teubeuer, Leibzig, (1921).

[Si] C. L. Siegel, Über einige anwendungen diophantischer approximationen, Abh. Preuss Akad. Wiss., Phys.-Math. Kl., 1, (1929), 14–67.

[St] W. W. Stothers, Polynomial identitites and Hauptmoduln, Quart. J. Math., (2) 32, (1981), 349–370.

[StrVo] K. Strambach and H. Völklein, The symplectic braid group and Galois realizations in Geometric Galois Action, London Math. Soc. Lecture Note Series, Cambridge University Press, (1997).

[Th] J. G. Thompson, Some finite groups which occur as $Gal(L/K)$ where $K \leq \mathbb{Q}(\mu_n)$, J. Algebra 89, (1984), 437–499.

[We] A. Weil, The field of definition of a variety, Oeuvres complètes (Collected papers) II , Springer-Verlag, 291–306.

[Wew] Wewers, S., Construction of Hurwitz spaces. Thesis, Inst. Exp. Math., Essen, 1998.

[Za1] U. Zannier, On Davenport's bound for the degree of f^3-g^2 and Riemann's existence theorem, Acta Arithmetica, 72, (1995), 107–137.

[Za2] —, Acknowledgement of Priority, Acta Arithmetica, 74/4, (1996).

Univ. Lille, Mathématiques, 59655 Villeneuve d'Ascq Cedex, France.
E-mail address: pde@ccr.jussieu.fr