Arithmétique et Espaces de Modules de Revêtements

Pierre Dèbes

Résumé. Les espaces de modules de revêtements constituent un cadre approprié pour l'étude de certains problèmes arithmétiques mettant en jeu courbes algébriques et fonctions rationnelles. Dans un premier temps, nous revenons sur la construction de ces espaces ainsi que sur leurs propriétés géométriques. Puis nous nous intéressons à leur utilisation à des fins arithmétiques, par exemple pour le problème inverse de Galois, le problème de Hilbert-Siegel, etc. Enfin nous considérons quelques développements récents comme la construction de tours modulaires.

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

1. Introduction

Dans un article de 1891 [Hu], A. Hurwitz explique comment on peut mettre une structure de variété complexe sur l'ensemble des revêtements simples de degré fixé d de $\mathbb{P}^1$ ("simple" signifiant ici que les fibres comportent au moins $d-1$ points). Par espaces de Hurwitz on entend aujourd'hui espaces de modules de revêtements de groupe d'automorphismes fixé et pour lesquels on impose certaines contraintes à la ramification. La construction générale et le développement de ces espaces sont essentiellement dûs à M. Fried. Il faut y associer aussi les noms de Fulton et Mumford pour leurs travaux sur les espaces de modules de courbes. Ce texte reprend, en insistant sur les implications arithmétiques, les différentes étapes de la théorie. Les sources principales sont [Fr2], [DeFr1-4], [FrVö], [Fr6].

Les espaces de Hurwitz constituent un outil de choix pour certains problèmes diophantiens mettant en jeu courbes algébriques et fonctions rationnelles; plus généralement, pour l'étude de l'arithmétique des revêtements de la droite. Par exemple le Problème Inverse de Galois (dans sa forme régulière sur $\mathbb{Q}(T)$) revient à trouver des points $\mathbb{Q}$-rationnels sur ces espaces. De façon générale, l'idée est de regarder les contraintes que le problème étudié impose aux données intrinsèques des

revêtements en question, comme le groupe d'automorphismes et la ramification, et de voir ensuite s'il existe sur l'espace de modules associé d'éventuelles solutions, sur $\mathbb{C}$ d'abord, puis sur le corps de base. Le problème conserve sa nature diophantienne mais cette approche permet d'une certaine façon, de classifier les équations en en abstrayant les propriétés structurelles.

Cette approche repose sur l'idée que la théorie des groupes, à travers la description des revêtements par leur monodromie, régit également l'arithmétique des revêtements. Le problème de Hilbert-Siegel en est une illustration (§4.1), où l'on voit la solution d'un problème arithmétique concret — l'étude de l'irréductibilité des polynômes du type $f(Y) - t$ ($f \in \mathbb{Q}[Y]$, $t \notin f(\mathbb{Q})$) — provenir de la classification des groupes simples. Plus généralement, on vise à développer des outils de pure théorie des groupes, permettant d'apprécier les propriétés arithmétiques des revêtements de monodromie fixée.

Pour les applications, le problème majeur est de trouver des points rationnels sur les espaces de Hurwitz. On a des réponses sur $\mathbb{Q}$ pour les "petites" valeurs des paramètres ou bien sur de "gros" corps K. Ces questions arithmétiques nécessitent une étude géométrique préalable (§2): il faut commencer par déterminer les composantes irréductibles de ces espaces, leurs corps de définition, leur structure géométrique, par exemple, si elles sont (uni-)rationnelles, etc.

Les succès les plus marquants de la théorie des espaces de Hurwitz concernent le problème inverse de Galois. Nous y revenons au §3. Il y a d'autres applications (§4): au problème de Hilbert-Siegel, au problème de Davenport, au théorème de Mason-Stothers, à un critère d'existence de points rationnels, etc. Afin d'illustrer la méthode, nous détaillerons un peu plus l'une d'elles, la première (§4.1 & §4.2).

On peut espérer que de nouveaux développements viendront de la considération de *tours modulaires* (§5). Ces objets ont été introduits par M. Fried [Fr6]. Une tour modulaire est une tour d'espaces de Hurwitz associés de façon naturelle à un espace de Hurwitz donné $\mathcal{H}$; chaque niveau de la tour se projette sur $\mathcal{H}$ par un revêtement de Frattini. L'exemple fondateur est celui de la tour des courbes modulaires. Ce cas particulier est riche en résultats arithmétiques (théorèmes de Serre, de Mazur-Merel, etc.). On peut se demander si des résultats de même nature subsistent dans le cas général des tours modulaires.

La plupart des questions développées dans cet article ont pour origine des problèmes diophantiens sur lesquels A. Schinzel a eu une grande influence. Ainsi, l'approche modulaire des problèmes de Hilbert-Siegel et de Davenport (§4) a été motivée par ses travaux sur les équations à variables séparées $h(x) = g(y)$. C'est aussi un résultat de Schinzel avec Lewis [LeSc] qui est à l'origine de notre travail [DeFr1], présenté en §4.4, sur l'existence de points rationnels dans les familles de courbes. Avec cet article, écrit à l'occasion du 60ème anniversaire d'A. Schinzel, l'auteur souhaite lui témoigner son estime et sa reconnaissance.

2. Espaces de modules de revêtements

Dans cette section, on introduit les espaces de Hurwitz (§2.1), on revient brièvement sur leur construction (§2.2), ainsi que leurs propriétés géométriques (§2.5); la plupart proviennent de la présentation des espaces de Hurwitz comme revêtement de l'espace $\mathcal{U}_r$ (§2.3). De premiers exemples sont donnés en §2.4.

2.1. Présentation

Les objets qui sont au centre de cet exposé sont les revêtements finis $f : X \to \mathbb{P}^1$ de la droite projective $\mathbb{P}^1$, définis sur la clôture algébrique $\overline{K}$ d'un corps K de caractéristique 0. Plus simplement, on peut les voir comme la donnée d'une courbe irréductible X définie sur $\overline{K}$ et d'une fonction rationnelle non constante $f \in \overline{K}(X)$. Il y a une notion classique d'isomorphisme (l'équivalence des revêtements). Les classes d'équivalence ont les invariants suivants.

Invariants.
• Le groupe de monodromie G du revêtement f, qui est isomorphe au groupe de Galois de la clôture galoisienne de l'extension $\overline{K}(X)/\overline{K}(T)$ et anti-isomorphe au groupe d'automorphismes de la clôture galoisienne du revêtement f.
• Le degré $d = \deg(f)$ et l'action de monodromie $G \hookrightarrow S_d$, correspondant à l'action de G sur une fibre non ramifiée du revêtement.
• L'ensemble $\mathbf{t} = \{t_1, \ldots, t_r\} \subset \mathbb{P}^1(\mathbb{C})$ des points de ramification. On notera $\mathcal{U}_r$ l'espace paramétrant cette donnée, *i.e.*, la variété des ensembles de r points distincts de $\mathbb{P}^1$. En associant à chaque $\mathbf{t}$ les coefficients du polynôme dont les racines sont $t_1, \ldots, t_r$, on voit $\mathcal{U}_r$ comme l'espace projectif $\mathbb{P}^r$ privé du lieu discriminant. On notera aussi $\mathcal{U}^r$ l'espace $(\mathbb{P}^1)^r$ privé des r-uplets dont deux coordonnées sont égales. La variété $\mathcal{U}_r$ correspond au quotient de $\mathcal{U}^r$ par l'action de S_r.
• L'inertie $\mathbf{C} = \{C_1, \ldots, C_r\}$ [1], *i.e.*, la donnée des classes de conjugaison des cycles de ramification, ou, de façon équivalente, des générateurs des groupes d'inertie, au-dessus des points de ramification.

Théorème 2.1 (Fried [Fr2])**.** *On suppose donnés une représentation transitive $G \hookrightarrow S_d$ et un entier $r \geq 3$.*
(a) *Il existe un espace de modules grossier $\mathcal{H}_G$ pour la catégorie $\mathcal{C}_{r,G}$ des revêtements de $\mathbb{P}^1$ définis sur $\mathbb{C}$, avec r points de ramification et de groupe $G \subset S_d$.*
(b) *L'espace $\mathcal{H}_G$ est une variété algébrique lisse définie sur $\mathbb{C}$ dont les points complexes correspondent bijectivement aux classes d'isomorphisme d'objets de la catégorie $\mathcal{C}_{r,G}$. On notera $[f]$ le point sur $\mathcal{H}_G(\mathbb{C})$ correspondant à un revêtement f. De plus l'espace $\mathcal{H}_G$ a la propriété suivante. Si $\mathcal{P}$ est une variété algébrique paramétrant une famille $\mathcal{F}$ de revêtements dans $\mathcal{C}_{r,G}$, alors l'application $\mathcal{P} \to \mathcal{H}_G$ envoyant tout point $p \in \mathcal{P}$ sur le point $[\mathcal{F}_p] \in \mathcal{H}_G$ est un morphisme algébrique.*

[1] Certaines des classes C_i peuvent être répétées. Plutôt qu'un ensemble, il faut voir $\mathbf{C}$ comme un r-uplet modulo l'action de S_r.

(c) *$\mathcal{H}_G$ a un modèle défini sur $\mathbb{Q}$. Ce modèle a les propriétés suivantes. Soit K un corps de caractéristique 0. Dans toute classe $[f] \in \mathcal{H}_G(\overline{K})$, il existe un revêtement f défini sur $\overline{K}$. De plus, l'action de $G_K = G(\overline{K}/K)$ sur $\mathcal{H}_G(\overline{K})$ coincide avec l'action sur les revêtements correspondants. C'est-à-dire, $[f]^\tau = [f^\tau]$ pour tout $[f] \in \mathcal{H}_G(\overline{K})$ et tout $\tau \in G_K$.*
(d) *On appelle corps des modules du revêtement f le corps $\mathbb{Q}([f])$; sous des hypothèses convenables* [DeDo1]*, c'est le plus petit corps de définition de f.*
(e) *L'application $\psi : \mathcal{H}_G \to \mathcal{U}_r$ associant à $[f] \in \mathcal{H}_G(\mathbb{C})$ l'ensemble $\mathbf{t}$ des points de ramification de f est un morphisme étale et défini sur $\mathbb{Q}$.*

Variante: Il y a un énoncé similaire pour les G-*revêtements* de $\mathbb{P}^1$ de groupe G (au lieu de revêtements). Un G-revêtement est la donnée d'un revêtement galoisien $f : X \to \mathbb{P}^1$ et d'un isomorphisme $G(K(X)/K(T)) \simeq G$. On distingue généralement les deux situations en mettant en exposant de $\mathcal{H}_G$ l'indication *ab* (pour les revêtements *purs*) ou *in* (pour les G-revêtements). Pour simplifier, nous ne le ferons que quand nous l'estimerons nécessaire à la compréhension.

2.2. Construction

2.2.1. 1ère approche (Fried [Fr2], Coombes-Harbater [CoHa], Fried-Völklein [FrVo], Emsalem [Em]). Les différentes étapes de la construction sont les suivantes.

• On pose $\mathcal{H}_G(\mathbb{C}) \stackrel{\text{déf}}{=} \coprod(\mathbf{t}, \varphi_{\mathbf{t}})$ où $\mathbf{t}$ parcourt $\mathcal{U}_r(\mathbb{C})$ et $\varphi_{\mathbf{t}}$ l'ensemble des homomorphismes $\pi_1(\mathbb{P}^1 - \mathbf{t}) \to G \subset S_d$ (à équivalence près).

• On munit $\mathcal{H}_G(\mathbb{C})$ d'une topologie. On utilise pour cela les isomorphismes

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

(obtenus par rétraction) où $\mathbf{D} = \{D_1, \ldots, D_r\}$ est une famille de petits disques D_i autour de t_i. Essentiellement, deux points $(\mathbf{t}, \varphi_{\mathbf{t}})$ et $(\mathbf{t}', \varphi_{\mathbf{t}'})$ sont considérés comme proches si $\mathbf{t}$ et $\mathbf{t}'$ sont proches dans $\mathcal{U}_r(\mathbb{C})$ (dans un même polydisque $\mathbf{D}$) et si $\varphi_{\mathbf{t}}$ et $\varphi_{\mathbf{t}'}$ sont égaux *via* l'isomorphisme χ. Pour cette topologie, la projection $\psi : \mathcal{H}_G(\mathbb{C}) \to \mathcal{U}_r(\mathbb{C})$ est un revêtement topologique.

• D'après le théorème de Grauert-Remmert [GrRe], le revêtement ψ, dont la base $\mathcal{U}_r(\mathbb{C})$ est une variété algébrique, est prolongeable en un revêtement analytique compact $\overline{\psi} : \overline{\mathcal{H}_G(\mathbb{C})} \to \mathbb{P}_r(\mathbb{C})$.

• Ce revêtement analytique compact provient d'un morphisme algébrique $\overline{\psi} : \overline{\mathcal{H}_G} \to \mathbb{P}_r$ défini sur $\mathbb{C}$: cela résulte des théorèmes GAGA [Se1].

• On montre ensuite que $\overline{\psi}$ peut être défini sur $\overline{\mathbb{Q}}$. On utilise pour cela un résultat général de descente des revêtements d'une base définie sur un corps algébriquement clos [Se2;Ch.6].

• Descente de Weil [We]. On montre enfin que $\overline{\psi}$ peut être défini sur $\mathbb{Q}$. Pour cela, on considère, pour tout $\tau \in G_{\mathbb{Q}}$, l'application

$$\varepsilon_\tau : \begin{cases} \mathcal{H}_G^\tau(\overline{\mathbb{Q}}) & \to & \mathcal{H}_G(\overline{\mathbb{Q}}) \\ [f]^\tau & \to & [f^\tau] \end{cases}$$

Une première étape est de montrer que les ε_τ sont continus (voir ci-dessous). Ensuite, de $\psi\varepsilon_\tau = \psi^\tau$, on déduit que les ε_τ sont des isomorphismes analytiques; alors ce doivent être des isomorphismes algébriques à cause de l'unicité de la structure algébrique sur $\mathcal{H}_G$ (induisant la structure analytique). Enfin on vérifie la condition de cocycle de Weil: $\varepsilon_u \varepsilon_v^u = \varepsilon_{uv}$ $(u, v \in G_{\mathbb{Q}})$. Le critère de descente de Weil donne alors les deux parties de la conclusion (c) du Th.2.1.

Continuité des ε_τ. On peut se placer sur un revêtement $\widetilde{\mathcal{H}}$ de $\mathcal{H}_G$ (plutôt que $\mathcal{H}_G$ lui-même): la continuité des ε_τ résulte de celle des $\widetilde{\varepsilon}_\tau : \widetilde{\mathcal{H}}^\tau \to \widetilde{\mathcal{H}}$. Il y a plusieurs revêtements $\widetilde{\mathcal{H}}$ de $\mathcal{H}_G$ possibles:
- (Fried-Völklein): $\widetilde{\mathcal{H}} = \mathcal{H}_{\widetilde{G}}$ où $\widetilde{G}$ est une extension de G de centralisateur dans $S_{\tilde{d}}$ trivial (ou de centre trivial pour la situation "G-revêtements"). Les revêtements paramétrés par $\widetilde{\mathcal{H}}$ n'ont alors pas d'automorphismes. Cela nécessite un lemme préalable de théorie des groupes disant que tout groupe G a une extension $\widetilde{G}$ ayant les propriétés requises.
- (Emsalem): $\widetilde{\mathcal{H}}$ est l'espace des modules des revêtements $f \in \mathcal{H}_G$ "pointés" par un point sur X (au-dessus d'un point-base t_o). Ces revêtements pointés n'ont pas d'automorphismes.

Dans les deux cas, l'absence d'automorphismes entraîne l'existence d'une *famille* $\widetilde{\mathcal{F}}$ de revêtements (éventuellement pointés) au-dessus de $\widetilde{\mathcal{H}}$ (voir §2.5.3). La continuité des $\widetilde{\varepsilon}_\tau$ s'ensuit. Voici essentiellement pourquoi.

Supposons que $([f_n]^\tau)_n$ tend vers $[f]^\tau$ dans $\widetilde{\mathcal{H}}^\tau$. Il existe une famille au-dessus de $\widetilde{\mathcal{H}}^\tau$, à savoir la famille $\widetilde{\mathcal{F}}^\tau$. Il en résulte ceci: *les* représentants des $([f_n]^\tau)_n$ dans la famille $\widetilde{\mathcal{F}}^\tau$ tendent vers *le* représentant de $[f]^\tau$ dans la famille $\widetilde{\mathcal{F}}^\tau$. Convenons que f_n $(n > 0)$ et f sont *les* revêtements de la famille $\widetilde{\mathcal{F}}$ représentant les points $[f_n]$ $(n > 0)$ et $[f]$. Alors f_n^τ $(n > 0)$ et f^τ sont *les* revêtements de la famille $\widetilde{\mathcal{F}}^\tau$ représentant les points $([f_n]^\tau)$ $(n > 0)$ et $[f]^\tau$. Conclusion: f_n^τ tend vers f^τ; *a fortiori*, $[f_n^\tau]$ tend vers $[f^\tau]$ sur $\widetilde{\mathcal{H}}$.

2.2.2. 2ème approche (Bertin [Be]). J. Bertin reprend des techniques purement algébriques mises en place par Mumford et Gieseker dans le contexte de la construction de l'espace $\mathcal{M}_g$ de modules des courbes. Il les utilise pour construire l'espace des modules $H_{g,G}$ des courbes lisses de genre $g \geq 2$ données avec une action d'un groupe G. L'espace $\mathcal{M}_g$ s'obtient à partir du schéma de Hilbert des courbes de genre g et de degré $m(2g-2)$ dans $\mathbb{P}_n$ $(n = card(G))$. Ici il faut ne s'intéresser qu'aux courbes qui sont laissées invariantes par l'action de G. L'espace $H_{g,G}$ s'obtient comme sous-variété de $\mathcal{M}_g$ fixée par l'action de G (étendue au schéma de Hilbert). Cette construction a l'avantage d'être valable en toute caractéristique. Cette approche conduit également à une construction d'une compactification $\overline{H}_{g,G}$ de $H_{g,G}$; elle fournit une description intéressante des points du bord de $\overline{H}_{g,G}$ comme courbes stables de genre g munie d'une action *stable* (voir [Be]

pour une définition précise) de G. Cette étude du "bord" éclaire d'autre part un peu plus le phénomène de "collision des points de ramification".

Il y a une autre différence avec la construction précédente. Si les objets correspondant aux points de $H_{g,G}$ peuvent être vus comme des revêtements $X \to X/G$, la base n'est pas fixée comme pour les revêtements paramétrés par les points de $\mathcal{H}_G$. Cela rend l'espace $\mathcal{H}_G$ peut-être plus approprié pour des considérations diophantiennes, puisque ce choix de la base correspond au choix d'une coordonnée et donc d'une équation pour la courbe du haut. Chez Bertin, la base n'est fixée qu'à isomorphisme près. Le schéma $H_{g,G}$ est en fait un quotient de l'espace $\mathcal{H}_G$ (pour $g = 0$, le quotient par $\mathrm{PGL}(2,\mathbb{C}) = \mathrm{Aut}(\mathbb{P}^1)$). En conséquence, l'interprétation du corps de définition des points sur $H_{g,G}$ diffère quelque peu. Ainsi, les points k-rationnels sur l'espace $H_{0,G}$ correspondent, non pas à des revêtements de $\mathbb{P}^1$ définis sur k, mais à des revêtements d'une k-courbe de genre 0 (et donc éventuellement d'une conique sans k-points).

Pour les questions liées à la construction, la compactification et la réduction des espaces de modules de courbes ou de revêtements, on pourra aussi consulter les articles [Fu], [DelMu], [HarMu] et les plus récents [Ek], [Mo] et [Wew].

2.3. Le revêtement $\mathcal{H}_G \to \mathcal{U}_r$

Pour tout $\mathbf{t} \in \mathcal{U}_r(\mathbb{C})$, la fibre $\psi^{-1}(\mathbf{t})$ est en bijection avec

• l'ensemble des classes d'équivalence de revêtements de monodromie $G \subset S_d$ et de points de ramification donnés, ou, de façon équivalente,

• l'ensemble des homomorphismes surjectifs $\pi_1(\mathbb{P}^1 - \mathbf{t}) \to G$, à équivalence près dans S_d, du groupe fondamental $\pi_1(\mathbb{P}^1 - \mathbf{t})$ (qui est isomorphe au groupe libre $F(x_1, \ldots, x_r)/x_1 \cdots x_r$) dans G, ou, de façon équivalente,

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

Le groupe fondamental de $\mathcal{U}_r(\mathbb{C})$ est un groupe de tresses, le groupe H_r des tresses d'Hurwitz. Il peut être décrit par générateurs et relations. Plus précisément, le groupe des tresses d'Artin B_r est le groupe engendré par $r-1$ générateurs $Q_1, \ldots, Q_{r-1}$ modulo les relations

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

Si on ajoute la relation $Q_1 \cdots Q_{r-1} Q_{r-1} \cdots Q_1 = 1$, on obtient le groupe des tresses d'Hurwitz. Pour un certain choix (standard) d'un isomorphisme entre $\pi_1(\mathbb{P}^1 - \mathbf{t})$ et le groupe libre $F(x_1, \ldots, x_r)/x_1 \cdots x_r$, l'action de monodromie associée au revêtement $\mathcal{H}_G \to \mathcal{U}_r$ est l'action de H_r sur $\mathrm{ni}_G^{\mathrm{ab}}$ donnée par la formule suivante (qu'on trouve déjà dans [Hu]; voir aussi [Fr2] et [FrVo]): pour $\mathbf{g} = (g_1, \ldots, g_r) \in \mathrm{ni}_G^{\mathrm{ab}}$,

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

Proposition 2.2. *Les composantes connexes (et donc irréductibles* [2]*) de* $\mathcal{H}_G$ *correspondent aux orbites de l'action de* H_r *sur* $\mathrm{ni}_G^{\mathrm{ab}}$.

Localement sur $\mathcal{H}_G(\mathbb{C})$, l'inertie $\mathbf{C} = \{C_1, \ldots, C_r\}$ ne change pas (*e.g.* [DeFr1; Lemma 1.5]); l'inertie est donc constante dans toute composante irréductible de $\mathcal{H}_G(\mathbb{C})$. Etant donné $\mathbf{C}$, on note $\mathcal{H}_G(\mathbf{C})(\mathbb{C})$ le sous-ensemble de $\mathcal{H}_G(\mathbb{C})$ constitué des points représentant des revêtements d'inertie $\mathbf{C}$; c'est une réunion de composantes connexes de $\mathcal{H}_G(\mathbb{C})$, qui est connexe (et irréductible) si et seulement si H_r agit transitivement sur l'ensemble

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

Sans l'indication "à l'ordre près", l'ensemble obtenu est un sous-ensemble de $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ noté $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$.

2.4. Premiers exemples

2.4.1. Une famille de polynômes de degré 5 [DeFr1]. On prend $G = S_5$ (plongé dans lui-même), $r = 4$; $C_2 = C_3$ est la classe des 2-cycles, C_1 est la classe des produits de deux 2-cycles disjoints et C_4 celle des 5-cycles. Un premier calcul conduit à la liste des éléments $(g_1, \ldots, g_4)$ de $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. Ceux pour lesquels $g_i \in C_i$, $i = 1, \ldots, 4$ et $g_4 = (54321)$ sont les suivants (on donne g_1, g_2, g_3):

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

L'espace de Hurwitz $\mathcal{H}_G(\mathbf{C})$ paramètre des revêtements $f : X \to \mathbb{P}^1$ de genre $g = 0$ ($2(5 + g - 1) = 2 + 1 + 1 + 4 = 8$). Si on impose que le point de ramification d'inertie dans C_4 est ∞, le revêtement $f : \mathbb{P}^1 \to \mathbb{P}^1$ est donné par un polynôme.

On vérifie que Q_1^2 et Q_2^2 agissent sur la liste ci-dessus de la façon suivante:

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

L'action de H_r sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ est donc transitive. L'espace $\mathcal{H}_G(\mathbf{C})$ est irréductible.

---

[2] car le revêtement $\psi : \mathcal{H}_G \to \mathcal{U}_r$ est étale.

[3] Stricto sensu ce n'est pas le normalisateur $Nor_{S_d}(G)$ qui agit mais le sous-groupe des éléments qui laissent globalement invariant l'ensemble $\{C_1, \ldots, C_r\}$.

2.4.2. Irréductibilité de $\mathcal{M}_g$. Etant donné un entier $g \geq 0$, on prend $G = S_d$ où $d \geq g+1$, $r = 2g+2d-2$, $C_i = C$ est la classe des 2-cycles, $i = 1, \ldots, r$. Toute courbe de genre g peut être présentée comme revêtement simple de $\mathbb{P}^1$, *i.e.*, avec seulement des points de ramification d'inertie associée dans C. Cela donne une surjection $\mathcal{H}_G(\mathbf{C}) \to \mathcal{M}_g$. Des calculs de Lurröth et Clebsch [Cl] montrent que l'action de H_r sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ est transitive. L'espace $\mathcal{H}_G(\mathbf{C})$ est irréductible; son image $\mathcal{M}_g$ l'est donc aussi. Historiquement, l'espace $\mathcal{H}_G(\mathbf{C})$, considéré par Hurwitz, est le premier espace de modules de revêtements qui apparait dans la littérature [Hu]. L'argument ci-dessus pour prouver l'irréductibilité de $\mathcal{M}_g$ en caractéristique 0 est donné dans un article de Severi [Sev]. Le cas de caractéristique $p > 0$ sera traité par la suite par Fulton [Fu] et Deligne-Mumford [DelMu].

2.4.3. Irréductibilité des courbes modulaires (Fried). Les courbes modulaires peuvent être présentées comme quotients d'espaces de Hurwitz paramétrant des revêtements galoisiens de $\mathbb{P}^1$ de groupe diédral avec 4 points de ramification (voir §3.1.4). Comme précédemment, on montre que cet espace de Hurwitz est irréductible en vérifiant la transitivité de l'action de H_4 associée.

2.5. Préalable géométrique

L'utilisation des espaces de Hurwitz pour des questions arithmétiques dépend de la possibilité d'y trouver des points rationnels. La recherche de points K-rationnels commence par celle de composantes irréductibles définies sur K. Pour cela, on dispose des résultats suivants.

2.5.1. Critères d'irréductibilité.

• *Critère général.* L'espace $\mathcal{H}_G(\mathbf{C})$ est irréductible si et seulement si H_r agit transitivement sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. De plus, $\mathcal{H}_G$ est défini sur $\mathbb{Q}$, donc $G_{\mathbb{Q}}$ permute les espaces $\mathcal{H}_G(\mathbf{C})$. Précisément, on a, pour tout $\tau \in G_{\mathbb{Q}}$,

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

où $\chi : G_{\mathbb{Q}} \to \mathbb{Z}/n\mathbb{Z}$ ($n = card(G)$) est le caractère cyclotomique. Le corps de définition de $\mathcal{H}_G(\mathbf{C})$ est un corps cyclotomique, qu'on peut explicitement déterminer, et qui est égal à $\mathbb{Q}$ sous des hypothèses supplémentaires assez simples, par exemple, si les classes $C_1, \ldots, C_r$ sont *rationnelles* (*i.e.*, invariantes par toute élévation à une puissance première à l'ordre de leurs éléments).

Observations: l'application de ce critère demande des calculs compliqués, faisables en pratique uniquement pour des petites valeurs de r.

• *Critère de Conway-Parker* [FrVo;appendix]. Supposons le groupe G de centre trivial et de multiplicateur de Schur engendré par les commutateurs. Si chaque classe $C \neq \{1\}$ est répétée suffisamment souvent dans $\mathbf{C}$, alors H_r agit transitivement sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. En conséquence, $\mathcal{H}_G(\mathbf{C})$ est irréductible et défini sur $\mathbb{Q}$.

Observations: ce critère n'est utilisable que pour des grandes valeurs de r; de plus la borne pour r n'est pas effective.

• *Inertie de type Harbater-Mumford* (Fried) [Fr6]. Un élément $\mathbf{g} \in \mathrm{ni}_G(\mathbf{C})$ est dit de type HM s'il est de la forme $\mathbf{g} = (g_1, g_1^{-1}, \ldots, g_s, g_s^{-1})$. Fried a montré que, sous quelques hypothèses techniques (dont $Z(G) = \{1\}$), les éléments $\mathbf{g} \in \mathrm{ni}_G(\mathbf{C})$ de type HM sont dans une même orbite de H_r et que la composante connexe correspondante est définie sur $\mathbb{Q}$.

2.5.2. Critères d'(uni-)rationalité. Rappelons qu'une K-variété V est dite *rationnelle* si son corps de fonctions $K(V)$ est une extension transcendante pure de K, ou, de façon équivalente, si V est birationnelle sur K à un ouvert d'un espace projectif $\mathbb{P}^r$; V est dite *unirationnelle* si $K(V)$ est contenu dans une extension transcendante pure de K. On dispose de critères de rationalité pour la variété $\mathcal{H}'_G(\mathbf{C})$. Le ' indique qu'on a adjoint les points de ramification: $\mathcal{H}'_G(\mathbf{C})$ est une composante connexe (quelconque) du produit fibré de $\mathcal{H}_G(\mathbf{C})$ avec $\mathcal{U}^r$ (défini en §2.1) au-dessus de $\mathcal{U}_r$; le corps des fonctions de $\mathcal{H}'_G(\mathbf{C})$ est celui de $\mathcal{H}_G(\mathbf{C})$ avec les indéterminées $t_1, \ldots, t_r$ adjointes.

• *Rigidité* (Belyi, Fried, Matzat, Shih, Thompson; voir [Se2]). Le cardinal des ensembles $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$ [resp. $\mathrm{sni}_G(\mathbf{C})^{\mathrm{in}}$] peut être calculé explicitement, à la main ou par ordinateur pour des petites valeurs de r; il existe aussi une formule faisant intervenir les caractères de G. La rigidité est un ensemble d'hypothèses qui garantit que ce nombre vaut 1. Dans ce cas, le revêtement $\psi' : \mathcal{H}'_G(\mathbf{C})^{\mathrm{ab}} \to \mathcal{U}^r$ [resp. $\psi' : \mathcal{H}'_G(\mathbf{C})^{\mathrm{in}} \to \mathcal{U}^r$] est un isomorphisme; le corps de définition d'un revêtement [resp. d'un G-revêtement] d'inertie $\mathbf{C}$ est celui de ses points de ramification.

• *Un autre cas de rationalité* [FrBi],[Fr4], [Fr5]. Supposons $\mathcal{H}' = \mathcal{H}'_G(\mathbf{C})$ irréductible. On peut en privilégiant une des variables $t_1, \ldots, t_r$, par exemple t_1, voir la flèche $\mathcal{H}' \to \mathcal{U}^r$ comme une famille $\mathcal{H}'_{t_2,\ldots,t_r}$ de revêtements de $\mathbb{P}^1$ paramétrée par les $r-1$ autres variables. La ramification de ces revêtements est connue: ils sont ramifiés aux points $t_2, \ldots, t_r$ et les cycles de ramification associés sont donnés par des formules explicites dans un groupe de tresses approprié. Le genre de la courbe $\mathcal{H}'_{t_2,\ldots,t_r}$ s'obtient grâce à la formule de Riemann-Hurwitz. Dans certaines situations, l'examen de la ramification permet également de conclure à l'existence générique d'un point rationnel au-dessus d'un des points de ramification $t_2, \ldots, t_r$. Si c'est le cas et si le genre est nul, la variété $\mathcal{H}'$ est une variété rationnelle.

• *Critères d'unirationalité* (Fried [DeFr4]). Fried a établi un critère d'unirationalité de l'espace $\mathcal{H}' = \mathcal{H}'_G(\mathbf{C})$. Il conjecture d'autre part que, sous certaines hypothèses sur G et si r assez grand, l'espace $\mathcal{H}'_G(\mathbf{C})$ est unirationnel.

2.5.3. Existence de familles de Hurwitz. Les espaces de Hurwitz ont été introduits *a priori* comme des espaces de modules grossiers. Se pose naturellement la question de l'existence d'une famille au-dessus d'un espace de Hurwitz $\mathcal{H}$, *i.e.*, d'un revêtement $\mathcal{T} \to \mathcal{H} \times \mathbb{P}^1$ tel que, pour tout $[f] \in \mathcal{H}$, le revêtement-fibre $\mathcal{T}_{[f]} \to [f] \times \mathbb{P}^1$ au-dessus de $\{[f]\}$ soit un revêtement équivalent à f. Et dans le cas où il existe une famille, est-elle universelle?

Dans son article [Fr2], Fried montre que la réponse à ces deux questions est positive dans le cas où les revêtements paramétrés par $\mathcal{H}$ n'ont pas d'automorphismes (non triviaux), ou, de façon équivalente, si $\mathrm{Cen}_{S_d}(G) = \{1\}$; $\mathcal{H}$ est dans ce cas un espaces de modules *fin*. Le point est que les familles de Hurwitz existent au

moins localement; l'absence d'automorphismes permet ensuite de construire une famille au-dessus de $\mathcal{H}$ entier par recollement. Ce résultat, démontré pour les revêtements purs, s'étend au cas des G-revêtements ([CoHa], [FrVo]); l'absence d'automorphismes s'exprime dans ce cas par la condition $Z(G) = \{1\}$. Les espaces de Hurwitz sont également des espaces de modules fins dans la situation de revêtements *pointés* ([CoHa], [Em]); là aussi, le point est qu'un revêtement pointé n'a pas d'automorphismes.

Le problème est plus difficile dans le cas où les objets ont des automorphismes non triviaux. Il y a alors une obstruction à l'existence d'une famille au-dessus de $\mathcal{H}$, qui est de nature cohomologique. Dans la situation de G-revêtements, l'obstruction peut être mesurée par une classe dans $H^2(\pi_1(\mathcal{H}), Z(G))$. Le problème est plus complexe dans la situation de revêtements purs puisqu'il se pose en termes de cohomologie non abélienne: l'obstruction "vit" dans le groupe $H^2(\pi_1(\mathcal{H}), \mathrm{Cen}_{S_d}(G))$. On peut, en procédant comme dans [DeDo1], ramener la question dans $H^2(\pi_1(\mathcal{H}), Z(G))$. D'un point de vue théorique, l'outil le mieux adapté est la notion de *gerbe*, introduite par Grothendieck et Giraud (voir [DeDoEm]).

3. Le problème inverse de Galois

Cette section revient sur les résultats sur le problème inverse de Galois obtenus par le biais des espaces de Hurwitz. On s'intéresse en fait à la forme *régulière* du problème inverse de Galois.

Problème. *Etant donné un corps K, tout groupe fini G est-il le groupe de Galois d'une extension galoisienne $E/K(T)$ régulière* [4] *sur K? ou, de façon équivalente, le groupe d'automorphismes d'un revêtement galoisien $f : X \to \mathbb{P}^1$, défini sur K comme G-revêtement?*

Dans sa forme originale, le problème est posé avec $\mathbb{Q}$ à la place de $K(T)$. Cette forme se déduit de la forme régulière sur $\mathbb{Q}(T)$ grâce au théorème d'irréductibilité de Hilbert. Etant donné un groupe fini G, réaliser G sur $\mathbb{Q}(T)$ régulièrement revient à trouver au moins un point $\mathbb{Q}$-rationnel sur un espace de Hurwitz $\mathcal{H}_G^{\mathrm{in}}$ de G-revêtements. Dans la suite de cette section, on distingue deux types de résultats suivant que l'on travaille avec un groupe donné (§3.1) ou sur un corps fixé (§3.2). Nous renvoyons à [De1] et [DeDes] respectivement pour plus de détails et une bibliographie plus complète.

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

3.1. Le problème avec G fixé sur $\mathbb{Q}$

3.1.1. Le cas rigide (Thompson, et al.). C'est le cas le plus simple (voir §2.5.2): $\mathcal{H}'_G(\mathbf{C})^{\text{in}}$ est isomorphe sur $\mathbb{Q}$ à $\mathcal{U}^r$ (*via* ψ'). Les hypothèses rigides, qui entraînent que les revêtements en question sont déterminés par leurs points de ramification, sont assez contraignantes. Certains groupes les satisfont cependant, le groupe symétrique S_d, le Monstre [Th], par exemple. Ce cas ne nécessite pas strictement l'introduction des espaces de Hurwitz, mais il est le point de départ de la méthode modulaire et en a assuré la promotion.

3.1.2. Autres cas de rationalité (Matzat). En utilisant le second critère de rationalité expliqué plus haut (§2.5.2), Matzat a réussi à réaliser sur $\mathbb{Q}(T)$ (régulièrement) un certain nombre de groupes simples, en particulier des groupes sporadiques (seul M_{23} résiste encore, tous les autres ont été réalisés). La méthode a été développée par l'école d'Heidelberg (Matzat, Malle, et al.), ce qui a donné lieu à de nombreux travaux, à de nombreuses variantes du critère original et de nombreuses autres réalisations de groupes (voir [MaMa] pour un point des résultats). Cette approche est un des grands succès de la théorie des espaces de Hurwitz. Elle est cependant vraisemblablement insuffisante pour traiter la totalité du problème. Elle s'applique groupe par groupe et demande des calculs assez compliqués. Sa systématisation est improbable: le genre de $\mathcal{H}'_{t_2,\dots,t_r}$ (Cf. §2.5.2), qui doit être nul dans la méthode, n'est pas borné en général [DeFr3;§4].

3.1.3. Un raffinement de Völklein-Strambach [StrVo]. La méthode précédente consiste à trouver une composante rationnelle de $\mathcal{H}_G(\mathbf{C})$ qui soit définie sur $\mathbb{Q}$; on utilise pour cela la présentation de $\mathcal{H}_G(\mathbf{C})$ comme revêtement de $\mathcal{U}_r$. Völklein et Strambach fixent une sous-variété fermée $\mathcal{P}$ de $\mathcal{U}_r$ et regardent à quelles conditions on peut trouver une variété rationnelle définie sur $\mathbb{Q}$ au-dessus de $\mathcal{P}$. La variété $\mathcal{P}$ avec laquelle ils travaillent est celle des ensembles de r points symétriques par rapport à l'origine. Son groupe fondamental a une description concrète: ils l'appellent le groupe de tresses de type symplectique. La méthode précédente peut être mise en place dans ce contexte; ils obtiennent des critères de rationalité de même nature. Comme application, ils parviennent à réaliser certains groupes $\mathrm{Sp}_n(4^s)$.

3.1.4. Groupes diédraux et courbes modulaires [Fr3] [DeFr3]. Décider si un espace de Hurwitz a ou non des points rationnels est un problème difficile. Par exemple, dans la situation suivante, cela est équivalent à trouver à trouver des points rationnels sur une courbe modulaire.

On prend $G = D_p = \mathbb{Z}/p \times^s \mathbb{Z}/2$, $r = 4$ et toutes les classes C_i, $i = 1, \dots, 4$ égales à la classe C des involutions de G. On montre qu'il existe un morphisme surjectif, défini sur $\mathbb{Q}$

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

En conséquence, d'après le théorème de Mazur, si $p > 7$, $\mathcal{H}(\mathbb{Q}) = \emptyset$; le groupe diédral D_p ne peut donc être réalisé sur $\mathbb{Q}(T)$ régulièrement avec ces contraintes sur la ramification. En fait, quelques observations supplémentaires montrent que

le groupe diédral D_p ne peut être réalisé avec moins de 6 points de ramification (alors qu'il en suffit de 3 pour le Monstre). Nous conjecturons que pour r_o fixé, on ne peut réaliser régulièrement sur $\mathbb{Q}(T)$ qu'un nombre fini de groupes diédraux D_p avec moins de r_o points de ramification. Cela résulterait de conjectures de Mazur-Kamieny [MaKa] sur la finitude des nombres premiers qui sont ordre d'un point rationnel sur une variété abélienne de dimension donnée sur $\mathbb{Q}$.

Indications sur la construction de χ. Supposons donné un revêtement $f : E \to \mathbb{P}^1$ défini et galoisien sur $\mathbb{Q}$, de groupe D_p, ramifié en 4 points et d'inertie dans $\mathbf{C}$. La formule de Riemann-Hurwitz donne le genre g de E: $2g-2 = 2p(-2)+4p$ soit $g = 1$. Quitte à remplacer E par $Pic^o(E)$, on peut supposer que E a un point $\mathbb{Q}$-rationnel et donc est une courbe elliptique sur $\mathbb{Q}$. Les éléments d'ordre p de D_p sont des automorphismes de E d'ordre p définis sur $\mathbb{Q}$. Ce sont des translations par un point p de p-torsion définis sur $\mathbb{Q}$. On sait que la donnée (E, p) correspond à un point de la courbe modulaire $X_1(p)$ qui n'est pas une pointe.

Inversement, soit (E, p) une courbe elliptique munie d'un point de p-torsion, tous deux définis sur $\mathbb{Q}$. Le revêtement $E \to E/ < \mathrm{p} >$ est cyclique d'ordre p. La courbe $E_o = E/ < \mathrm{p} >$ est une courbe elliptique définie sur $\mathbb{Q}$. Si on compose le revêtement précédent avec le revêtement $E_o \to E_o/ < -1 >= \mathbb{P}^1$ (où -1 est l'involution canonique de E), on obtient un revêtement $E \to \mathbb{P}^1$ défini et galoisien sur $\mathbb{Q}$, de groupe D_p, ramifié en 4 points et d'inertie dans $\mathbf{C}$. □

3.2. Le problème avec K fixé pour tout G

Plutôt que de chercher à réaliser un groupe donné sur $\mathbb{Q}(T)$, on peut fixer un corps K et chercher à réaliser le plus grand nombre possible de groupes sur $K(T)$.

3.2.1. Réduction du problème [FrVo]. Fried et Völklein ont montré qu'à chaque groupe fini G, on peut associer une infinité d'espaces de Hurwitz $\mathcal{H}_G^{\mathrm{in}}(\mathbf{C})$, irréductibles et définis sur $\mathbb{Q}$ tels que l'existence d'un point K-rationnel sur l'un d'eux suffit pour conclure que G est groupe de Galois sur $K(T)$ régulièrement.

Le point ici est que les espaces $\mathcal{H}_G^{\mathrm{in}}(\mathbf{C})$ sont irréductibles. Fried et Völklein utilisent le critère de Conway-Parker (§2.5.1). Plus précisément, ils commencent par se placer sur une extension $\widetilde{G}$ de G vérifiant les hypothèses du critère de Conway-Parker ($Z(G) = \{1\}$, etc.); il faut donc démontrer un lemme préalable de théorie des groupes qui assure l'existence d'une telle extension. Puis ils considèrent un uplet $\widetilde{\mathbf{C}}$ où chaque classe de conjugaison de $\widetilde{G}$ non triviale est répétée aussi souvent que le requiert le critère de Conway-Parker. L'espace $\mathcal{H}_{\widetilde{G}}^{\mathrm{in}}(\widetilde{\mathbf{C}})$ est alors irréductible, défini sur $\mathbb{Q}$ et tout point K-rationnel dessus fournit une réalisation régulière sur K de $\widetilde{G}$ et donc de G.

Observations. Conway et Parker ne donnent pas une borne effective du nombre de répétitions nécessaires de chaque classe de conjugaison. Mais il y a maintenant une alternative à l'utilisation de Conway-Parker, et qui elle est effective. Il s'agit du critère d'irréductibilité des espaces de Hurwitz $\mathcal{H}_G(\mathbf{C})$ pour une inertie $\mathbf{C}$ de type Harbater-Mumford (voir §2.5.1).

3.2.2. Les résultats. Cette approche a permis la résolution du problème inverse de Galois (forme régulière) sur les corps K suivants:

• K Pseudo Algébriquement Clos de caractéristique 0 (Fried-Völklein [FrVo]). Les ultra-produits de corps finis constituent les exemples type de corps PAC. Le résultat de Fried-Völklein fournit cette conséquence: tout groupe G est réalisable régulièrement sur $\mathbb{F}_p(T)$, pour tout p sauf un nombre fini.

• $K = \mathbb{Q}^{tr} = \{\text{nombres algébriques totalement réels}\}$ (Dèbes-Fried [DeFr3]),

• $K = \mathbb{Q}^{tp} = \{\text{nombres algébriques totalement } p\text{-adiques}\}$ (Dèbes [De2])

Pour ces deux derniers cas, on utilise un résultat de Pop [Po;appendix] selon lequel une variété lisse définie sur $\mathbb{Q}$ a des points totalement p-adiques si elle a des points p-adiques (y compris pour $p = \infty$). Les points réels d'un espace de Hurwitz peuvent être déterminés de façon très explicite car l'action de la conjugaison complexe sur les revêtements de $\mathbb{P}^1$ est parfaitement connue ([Hu], [KrNe], [DeFr2]). Pour construire des espaces de Hurwitz $\mathcal{H}_G^{\text{in}}$ avec des points p-adiques (*i.e.*, des revêtements définis sur $\mathbb{Q}_p$), on utilise des techniques de recollements d'espaces analytiques formels ou rigides, dues à Harbater [Ha].

• B. Deschamps [Des] a repris la construction précédente et montré que l'espace de Hurwitz $\mathcal{H}_G^{\text{in}}(\mathbf{C})$ contenant des points p-adiques pouvait être construit indépendant de p. Précisément, il démontre qu'à chaque groupe fini G, on peut associer une infinité d'espaces de Hurwitz $\mathcal{H}_G^{\text{in}}(\mathbf{C})$, irréductibles et définis sur $\mathbb{Q}$ et possédant des points p-adiques pour tout nombre premier, y compris $p = \infty$.

• Les résultats précédents ont été généralisés par Pop [Po]. Le problème inverse de Galois (forme régulière sur $K(T)$) est maintenant résolu pour tout corps K *ample*. Un corps K est dit ample si toute courbe lisse définie sur K a une infinité de points K-rationnels si elle en a au moins un. Les corps PAC, les corps valués complets, les corps $\mathbb{Q}^{tp}$, etc. sont amples.

4. Autres applications arithmétiques

Cette section en donne quatre. Nous développons plus particulièrement la première, qui concerne le problème de Hilbert-Siegel (§4.1 et §4.2). D'autres applications au problème de Davenport et au théorème de Mason-Stothers (§4.3) sont mentionnées plus rapidement. On termine par un critère d'existence de points rationnels sur des revêtements utilisant la monodromie sous-jacente des espaces de Hurwitz (§4.4).

4.1. Le problème de Hilbert-Siegel [Fr5]

Fried appelle ainsi le problème suivant (en référence à une observation de Siegel dans [Si]). Il s'agit de déterminer les polynômes $h(Y) \in \mathbb{Q}[Y]$ tels que $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z} - h(\mathbb{Q})$. On supposera h indécom-

posable (dans le cas contraire $h(Y) = h_1(h_2(Y))$ et $h(Y) - t$ est réductible pour tout t de la forme $t = h_1(z)$, $z \in \mathbb{Q}$). On a le résultat suivant.

Théorème 4.1 (Fried)**.** *Les seuls polynômes indécomposables $h(Y) \in \mathbb{Q}[Y]$ pour lesquels $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z}-h(\mathbb{Q})$ sont de degré* 5*.*

Schéma de preuve. Considérons une factorisation non triviale $h(Y)-T = Q(Y)R(Y)$ dans $\overline{\mathbb{Q}(T)}$. Soit $F \subset \overline{\mathbb{Q}(T)}$ le corps engendré par les coefficients de Q et R. Le corps F est une extension stricte de $\overline{\mathbb{Q}}(T)$, laquelle correspond à un revêtement $f : C \to \mathbb{P}^1$. Les nombres rationnels $t \in \mathbb{Q}$ tels que $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ correspondent (sauf éventuellement pour un nombre fini d'entre eux) aux spécialisations $\mathbb{Q}$-rationnelles d'un des corps F associés aux diverses factorisations possibles de $h(Y) - T$ dans $\overline{\mathbb{Q}(T)}$ [5], ou, de façon équivalente, aux valeurs $f(\mathrm{m})$ prises par f en un point $\mathbb{Q}$-rationnel m sur une des courbes C correspondantes.

Supposons que $h(Y) - t$ soit réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z}-h(\mathbb{Q})$. D'après le théorème de Siegel sur les points entiers des courbes algébriques, il existe au moins une des courbes C (en dehors de la courbe $h(y) = t$) qui est $\mathbb{Q}$-birationnelle à $\mathbb{P}^1$ et telle que la fonction g a ou bien un pôle $\mathbb{Q}$-rationnel ou bien deux pôles quadratiques réels. Autrement dit, il existe des fractions rationnelles non-constantes $g_1(Z), \ldots, g_s(Z) \in \mathbb{Q}(Z)$ avec $s \geq 1$ vérifiant:

• $h(Y) - g_i(Z)$ réductible dans $\overline{\mathbb{Q}}(Z)[Y]$, $i = 1, \ldots, s$,

• Le dénominateur de chaque $g_i(Z)$ est de la forme $(Z - a)^\ell$ avec $a \in \mathbb{Q}$ ou $(z^2 + pZ + q)^\mu$ avec $p^2 - 4q > 0$,

• $g_i(Z)$ ne se déduit pas de $h(Z)$ par changement de variable $(z \leftrightarrow (az+b)/(cz+d))$, $i = 1, \ldots, s$.

• Pour tout $t \in \mathbb{Z}-h(\mathbb{Q})$ (sauf un nombre fini), $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ si et seulement si il existe $i \in \{1, \ldots, s\}$ tel que $t = g_i(z)$ avec $z \in \mathbb{P}^1(\mathbb{Q})$.

Fixons un indice i et posons $g_i = g$. La première condition signifie que le produit fibré des deux revêtements de $\mathbb{P}^1$ induits par $h(Y)$ et $g(Y)$ est réductible. Le point suivant de la preuve de Fried est de montrer que les clôtures galoisiennes sur $\overline{\mathbb{Q}}(T)$ des deux polynômes $h(Y) - T$ et $g(Y) - T$ sont nécessairement égales [Fr1]. Notons G le groupe de Galois de cette extension galoisienne. Les deux revêtements correspondent à deux représentations transitives $T_h : G \to S_n$ et $T_g : G \to S_m$. Les deux revêtements sont de genre 0; cela fournit, *via* la formule de Riemann-Hurwitz, une première condition sur les représentations T_h et T_g. Les quatre points ci-dessus se traduisent de la façon suivante. On note $T_g(1)$ [resp. $T_h(1)$] le fixateur de 1 dans la représentation T_g [resp. T_h].

• La restriction de T_g à $T_h(1)$ n'est pas transitive,

• Il existe $\sigma \in G$ tel que $T_h(\sigma)$ est un n-cycle et $T_g(\sigma)$ est, soit un m-cycle, soit le produit de deux μ-cycles,

[5] L'existence de telles spécialisations de F entraîne que F est une extension régulière de $\mathbb{Q}$

• $T_h(1)$ ne contient aucun conjugué de $T_g(1)$.

Enfin, il est classique que l'hypothèse "$h(Y)$ indécomposable" est équivalente à la condition

• La représentation $T_h : G \to S_n$ est primitive.

Le reste de la preuve est un travail de théorie des groupes. En utilisant la classification des groupes simples, on montre que l'existence de telles représentations n'est possible que si $n = 5$, $m = 10$ et $G = S_5$ ou $G = A_5$. □

Remarque 4.2. Cette approche du problème a été développée par P. Mueller [Mu]. Soit $f(T, Y) \in \mathbb{Q}[T, Y]$ absolument irréductible. Supposons que, pour une infinité de $t \in \mathbb{Z}$, $f(t, Y)$ est réductible mais n'a pas de facteur linéaire. Peut-on conclure que nécessairement $\deg_Y(f) = 5$? Mueller a montré que oui si le groupe de Galois de $f(T, Y)$ sur $\overline{\mathbb{Q}}(T)$ est le groupe symétrique ou si $\deg_Y(f)$ est premier.

4.2. Etude d'un cas exceptionnel où $\deg(h) = 5$ ([DeFr1], [DeFr4])

La résolution du problème de Hilbert-Siegel conduit à une description précise des cas exceptionnels de degré 5. L'un d'eux est le suivant. Les deux revêtements h et g sont de groupe S_5, sont ramifiés en $r = 4$ points de $\mathbb{P}^1$. Les cycles de ramification sont du type suivant (dans S_5):

• pour h: (2)(2) ; (2) ; (2) ; (5)

On notera $\mathbf{C}$ l'ensemble des 4 classes de conjugaison de S_5 correspondantes. On retrouve l'exemple vu en §2.4.1. La représentation $T_h : S_5 \to S_5$ est donnée par l'action standard de S_5 sur $\{1, \ldots, 5\}$. La représentation $T_g : S_5 \to S_{10}$ est donnée par l'action de S_5 sur les 10 paires $\{i, j\}$ d'éléments distincts de $\{1, \ldots, 5\}$. (Ce cas exceptionnel correspond à la situation où l'on part d'une décomposition *a priori* $h(Y) - T = Q(Y)R(Y)$ dans $\overline{\mathbb{Q}(T)}$ avec un des facteurs de degré 2). On en déduit le type des cycles de ramification (dans S_{10}):

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

On s'intéresse ici à la question suivante: existe-t-il un polynôme $h(Y) \in \mathbb{Q}[Y]$ satisfaisant les hypothèses de ce cas et qui est réellement exceptionnel, *i.e.*, pour lequel $h(Y) - t$ est réductible dans $\mathbb{Q}[Y]$ pour une infinité de $t \in \mathbb{Z} - h(\mathbb{Q})$? Introduisons l'espace de Hurwitz $\mathcal{H} = \mathcal{H}_{S_5}(\mathbf{C})$ [6]. L'espace $\mathcal{H}$ est irréductible (§2.4.1). De plus, comme $\mathrm{Cen}_{S_5}(S_5) = \{1\}$ et $\mathrm{Cen}_{S_{10}}(S_5) = \{1\}$, $\mathcal{H}$ est un espace de modules fin (§2.5.3): il existe au-dessus de $\mathcal{H}$ une famille universelle $\mathcal{F}_5$ [resp. $\mathcal{F}_{10}$] de revêtements de degré 5 [resp. de degré 10] ayant les caractéristiques ci-dessus. La question se reformule ainsi:

[6] A priori, S_5 est plongé, d'une part dans lui-même et d'autre part dans S_{10}, et il faudrait distinguer les deux situations. Mais on vérifie que le nombre d'éléments dans $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ est le même dans les deux situations, si bien que les deux espaces de Hurwitz sont isomorphes.

Question 4.3. *Existe-t-il un point* $[h] \in \mathcal{H}(\mathbb{Q})$ *tel que*

(*) *le revêtement correspondant* $h : \mathbb{P}^1 \to \mathbb{P}^1$ *de la famille* $\mathcal{F}_5$ *est un revêtement polynomial et le revêtement correspondant* $\gamma_{[h]} : Y_{[h]} \to \mathbb{P}^1$ *de la famille* $\mathcal{F}_{10}$ *a la propriété que* $\gamma_{[h]}(Y_{[h]}(\mathbb{Q})) \cap \mathbb{Z}$ *est infini et que* $\gamma_{[h]}(Y_{[h]}(\mathbb{Q})) \cap h(\mathbb{Q}) \cap \mathbb{Z}$ *est fini?*

On peut décrire plus concrètement le revêtement $\gamma_{[h]}$: en termes de corps de fonctions, le revêtement $h : \mathbb{P}^1 \to \mathbb{P}^1$ correspond à l'extension $\overline{\mathbb{Q}}(y_1)/\overline{\mathbb{Q}}(T)$, où y_1 est l'une des 5 racines dans $\overline{\mathbb{Q}(T)}$ de $h(Y) - T$. Le revêtement $\gamma_{[h]} : Y_{[h]} \to \mathbb{P}^1$ correspond alors à l'extension $\overline{\mathbb{Q}}(y_1 + y_2, y_1 y_2)/\overline{\mathbb{Q}}(T)$.

Théorème 4.4 (Dèbes-Fried [DeFr4])**.** *L'ensemble des points* $[h] \in \mathcal{H}(\mathbb{Q})$ *tels que* (*) *a lieu est Zariski-dense. En conséquence, il existe* $h(Y) \in \mathbb{Q}[Y]$ *indécomposable et tel que* $h(Y) - t$ *est réductible dans* $\mathbb{Q}[Y]$ *pour une infinité de* $t \in \mathbb{Z} - h(\mathbb{Q})$.

Schéma de la preuve. La preuve comporte les points suivants.

• $\mathcal{F}_{10}$ est une famille de revêtements de genre 0. De plus, l'ensemble des points de $\mathcal{H}(\mathbb{C})$ pour lesquels le revêtement correspondant dans la famille $\mathcal{F}_{10}$ a les trois propriétés suivantes, est Zariski-dense:

- le revêtement est défini sur $\mathbb{R}$,
- ∞ est le point de ramification d'inertie dans C_4,
- les deux points dans la fibre au-dessus de ∞ sont réels.

Ce premier point est une condition nécessaire pour que la conclusion du Th.4.4 soit vraie. Pour étudier les conditions ci-dessus, qui sont de nature "réelle", on dispose de critères de pure théorie des groupes portant sur l'ensemble $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$. Nous renvoyons à [DeFr4] pour plus de détails.

• $\mathcal{H}$ est unirationnel: Soit $\mathcal{M} = (\mathbb{A}^1)^2 \times (\mathbb{A}^1 - \{0\})^2$. Pour tout $\mathbf{x} = (\beta, s, t, \alpha) \in \mathcal{M}$, le polynôme

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

induit un revêtement de la famille $\mathcal{F}_5$ (à équivalence près). Inversement, tout point $[h] \in \mathcal{H}$ correspondant à un revêtement polynômial représente la classe d'équivalence d'un revêtement associé à un polynôme comme ci-dessus. D'où une flèche $\mathcal{M} \twoheadrightarrow \mathcal{H}$.

• $\mathcal{H}$ est défini sur $\mathbb{Q}$: car les classes de conjugaison dans $\mathbf{C}$ sont rationnelles (§2.5.1).

• Calcul du revêtement $\gamma_{[h_{\mathbf{x}}]}$ noté plus simplement $\gamma_{\mathbf{x}}$. Le diviseur constitué des deux points au-dessus de ∞ (correspondant aux deux 5-cycles du 4ème cycle de ramification) est de degré 2 et rationnel sur $\mathbb{Q}(\mathbf{x})$. Le calcul d'une base du système linéaire associé fournit un plongement de $Y_{[h_{\mathbf{x}}]} = Y_{\mathbf{x}}$ dans $\mathbb{P}^2$. L'image de ce plongement est la conique $C_{\mathbf{x}}$:

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

On obtient la flèche du revêtement $\gamma_{\mathbf{x}}$ en exprimant T en fonction de U et V

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

• On trouve un sous-ensemble Zariski-dense $\mathcal{O}$ de points $\mathbf{x} \in \mathcal{M}(\mathbb{Q})$ tels que la conique $C_{\mathbf{x}}$ ait un point $\mathbb{Q}$-rationnel. L'ensemble des points $(\beta, c+d, cd, \alpha)$ avec $c, d \in \mathbb{Q}$ convient: le point $(2c, \frac{c-5d}{2})$ est sur $C_{\mathbf{x}}$ (Cf. [DeFr1;Lemma 3.18]).

• En utilisant la paramétrisation d'Euler, on identifie, pour $\mathbf{x} \in \mathcal{O}$ la conique $C_{\mathbf{x}}$ à $\mathbb{P}^1$. Précisément, on obtient

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

En reportant U et V dans l'expression de T ci-dessus, on obtient une fraction rationnelle $g_{\mathbf{x}}(w)$ de degré 10, de dénominateur une puissance d'un trinôme.

• Pour terminer la preuve, il reste à étudier les valeurs de cette fraction rationnelle, et, plus précisément, à vérifier que

- $g_{\mathbf{x}}(\mathbb{Q}) \cap \mathbb{Z}$ est infini pour tout $\mathbf{x}$ dans un sous-ensemble Zariski-dense de $\mathcal{O}$: cela se fait en utilisant la forme explicite de $g_{\mathbf{x}}$.

- $g_{\mathbf{x}}(\mathbb{Q}) \cap h_{\mathbf{x}}(\mathbb{Q}) \cap \mathbb{Z}$ est fini: cela est équivalent à montrer que le produit fibré $\mathbb{P}^1 \times_{\mathbb{P}^1} Y_{\mathbf{x}}$ des revêtements $h_{\mathbf{x}}$ et $\gamma_{\mathbf{x}}$ n'a qu'un nombre fini de points $\mathbb{Q}$-rationnels au-dessus d'entiers $z \in \mathbb{Z}$. Cela résulte du théorème de Siegel si ce produit fibré n'a que des composantes irréductibles de genre > 0. Un calcul basé sur la formule de Riemann-Hurwitz et le lemme d'Abhyankar [DeFr4] montre qu'il y a deux composantes irréductibles: l'une est de genre 1 et l'autre de genre 2. □

Remarque 4.5 (Familles de Siegel)**.** On peut voir le paragraphe §4.2 comme un cas particulier d'un problème général, qui est l'étude d'une réciproque du théorème de Siegel. Etant donnés une courbe algébrique C, une fonction rationnelle $f : C \to \mathbb{P}^1$, définis sur $\mathbb{Q}$ et un idéal fractionnaire $\mathcal{A}$ de $\mathbb{Q}$, le théorème de Siegel donne une condition nécessaire pour que $C(\mathbb{Q}) \cap f^{-1}(\mathcal{A})$ soit infini: C est de genre 0 et f a soit un unique pôle rationnel soit deux pôles quadratiques réels conjugués. La réciproque que nous considérons est la suivante. Soit $\mathcal{P}$ l'espace des paramètres d'une famille lisse $\Phi : \mathcal{P} \times \mathbb{P}^1 \to \mathcal{P} \times \mathbb{P}^1$, définie sur $\mathbb{Q}$, de fractions rationnelles (de degré n). Supposons que pour un ensemble Zariski-dense de points $\mathbf{p} \in \mathcal{P}(\mathbb{Q})$, la fonction $\Phi_{\mathbf{p}}$ a deux pôles quadratiques réels conjugués. La famille Φ est alors appelée une *famille de Siegel*. On demande si la condition du théorème de Siegel — $\Phi_{\mathbf{p}}(\mathbb{Q}) \cap \mathcal{A}$ infini — est vraie pour tout point $\mathbf{p}$ dans un sous-ensemble Zariski-dense de $\mathcal{P}$. Ci-dessus, nous avons montré que la famille de fractions rationnelles (de degré 10) paramétrée par le pull-back de $\mathcal{O}$ par l'application $(\beta, c, d, \alpha) \to (\beta, c+d, cd, \alpha)$ vérifiait cette réciproque du théorème de Siegel.

4.3. Davenport, Mason et al.

4.3.1. Le problème de Davenport. Le problème de Hilbert-Siegel est un cas particulier du problème général de la classification des paires de revêtements de $\mathbb{P}^1$ de produit fibré réductible. La méthode a consisté à traduire le problème en termes de bi-représentations du groupe de Galois associé. Les contraintes plus spécifiques données par le théorème de Siegel ont permis de conclure. En utilisant la même démarche, on peut apporter une réponse au problème, posé par Davenport, qui est de classer les polynômes $h(y), g(y) \in \mathbb{Z}[Y]$ qui prennent les mêmes valeurs modulo p, pour tout premier p, sauf un nombre fini. L'énoncé suivant a été démontré par Fried [Fr5]; d'importantes contributions sont dues à Schinzel (dans le cadre de ses travaux sur les équations à variables séparées $h(x) = g(y)$ [DaLeSc], [Sc]) et à Feit (pour la partie de théorie des groupes [Fe1-3]).

Théorème 4.6. *Soient K un corps de nombres et O_K son anneau d'entiers. Soient $h(Y), g(Y) \in O_K[Y]$ tels que h est indécomposable et "linéairement indépendant" de g (i.e., $h(y) \neq g(ay+b)$, $a, b \in \mathbb{C}$). Supposons que, pour tout premier p de O_K sauf un nombre fini, les ensembles de valeurs $h(O_K/p)$ et $g(O_K/p)$ prises par h et g sur O_K/p coincident. Alors on a*

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

En particulier, si $K = \mathbb{Q}$, il n'existe pas de polynômes $h(Y)$, $g(Y)$ vérifiant de telles hypothèses.

Chacun des degrés n ci-dessus est réellement une exception sur $\mathbb{Q}(\zeta_n)$: on peut trouver des paires $h(Y), g(Y) \in O_{\mathbb{Q}(\zeta_n)}[Y]$ vérifiant les hypothèses du théorème et $\deg(h) = n$; les paires exceptionnelles (h, g) ont récemment été classifiées par P. Cassou-Noguès et J-M. Couveignes [CaCou]. En revanche, pour $K = \mathbb{Q}$, on ne connait même pas d'exemples avec h décomposable.

4.3.2. Sur le théorème de Mason-Stothers [Za1]. Les espaces de Hurwitz apparaissent aussi dans un travail de U. Zannier. Il s'intéresse au cas d'égalité dans le théorème de Mason-Stothers [7] (analogue polynomial de la conjecture *abc* — si $a, b, c \in \mathbb{C}[Y]$ sont trois polynômes premiers entre eux tels que $a - b = c$, alors le nombre de racines distinctes dans $\mathbb{C}$ de abc est strictement plus grand que le maximum des degrés de a, b et c —). A un triplet (a, b, c), il associe le revêtement $f : \mathbb{P}^1 \to \mathbb{P}^1$ induit par la fraction rationnelle a/b. Puis traduit les conditions d'égalité dans le théorème de Mason-Stothers en termes de la ramification de ce revêtement: le revêtement est ramifié en 0, 1 et ∞ avec certaines conditions sur les indices de ramification. Si bien qu'il arrive à entièrement poser le problème en

[7] Zannier signale dans [Za2] que ce résultat qu'on attribue généralement à Mason est en fait apparu précédemment dans un article de Stothers [St].

termes d'existence de sous-groupes de S_n engendrés par des éléments $\sigma_1, \ldots, \sigma_{r-1}$ vérifiant certaines conditions. Il donne ensuite une construction combinatoire de sous-groupes du type requis.

Les espaces de Hurwitz apparaissent explicitement quand on se pose des questions de rationalité. C'est le théorème d'existence de Riemann qui permet en dernier lieu d'associer aux sous-groupes de S_n construits un revêtement $f : X \to \mathbb{P}^1$, de genre 0, et donc une fraction rationnelle a/b. Mais les polynômes a et b sont *a priori* à coefficients dans $\mathbb{C}$. L'existence de polynômes à coefficients dans $\mathbb{Q}$ revient à montrer que le revêtement f peut être défini sur $\mathbb{Q}$, et donc à trouver des points $\mathbb{Q}$-rationnels sur des espaces de Hurwitz. Zannier explique que c'est possible quand on fait certaines hypothèses qui garantissent l'unicité du revêtement f: c'est le cas "rigide". Il suggère que plus généralement, on pourrait utiliser les résultats connus sur l'arithmétique des espaces de Hurwitz. L'intérêt d'obtenir des solutions sur $\mathbb{Q}$ est que, par spécialisation, on peut espérer obtenir un triplet d'entiers pour lequel on serait proche du cas d'égalité dans la conjecture *abc* numérique.

4.4. Critère d'existence de points rationnels [DeFr1]

Nous terminons ces applications par la description d'un critère qui utilise la structure modulaire même des espaces de Hurwitz — de façon précise, la monodromie du revêtement $\mathcal{H}_G(\mathbf{C}) \to \mathcal{U}_r$ — pour détecter des points rationnels sur les revêtements paramétrés par les points de $\mathcal{H}_G(\mathbf{C})$.

Soit $f : X \to \mathbb{P}^1$ un revêtement défini sur un corps K. *Via* le choix d'un isomorphisme $\pi_1(\mathbb{P}^1 - \mathbf{t}) \simeq F(x_1, \ldots, x_r)/x_1 \cdots x_r$, f peut être vu (à isomorphisme près) comme la donnée de l'ensemble $\mathbf{t} = \{t_1, \ldots, t_r\}$ de ses points de ramification et d'un r-uplet $\mathbf{g} = (g_1, \ldots, g_r) \in \mathrm{ni}_G(\mathbf{C})$, où G est le groupe et $\mathbf{C}$ l'inertie du revêtement f. Pour $i = 1, \ldots, r$, considérons la décomposition de g_i en cycles à supports disjoints dans S_d: $g_i = \beta_{i1} \cdots \beta_{i\ell_i}$. On sait que, pour $i = 1, \ldots, r$, les points dans la fibre $f^{-1}(t_i)$ correspondent aux cycles β_{ij} de la décomposition de g_i, la longueur de chaque cycle étant égale à l'indice de ramification correspondant. On sait aussi (*e.g.* [Fr2;p.62]) que l'action de G_K sur l'ensemble des points de ramification a la propriété suivante. Pour $\tau \in G_K$ et $i = 1, \ldots, r$, si $t_i^\tau = t_j$, alors il existe $\gamma \in S_d$ et un entier a premier à l'ordre des éléments de C_i tels que $C_j = \gamma C_i^a \gamma^{-1}$. Il en résulte que, pour tout $i \in \{1, \ldots, r\}$, le diviseur $\sum_j (t_j)$, où j parcourt l'ensemble I des indices tels que $C_j = \gamma C_i^a \gamma^{-1}$ avec γ et a comme ci-dessus, est un diviseur K-rationnel de $\mathbb{P}^1$.

Fixons un indice $i \in \{1, \ldots, r\}$ et la longueur λ d'un des cycles g_{ik}. Notons $g(i, \lambda)$ l'ensemble des cycles de longueur λ intervenant dans la décomposition des g_{jk} où j décrit I et $P_f(i, \lambda)$ l'ensemble des points de X correspondant aux cycles dans $g(i, \lambda)$. Considérons le sous-groupe

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

Supposons que le groupe G du revêtement est de centralisateur $\mathrm{Cen}_{S_d}(G)$ trivial. Alors l'élément γ associé dans la définition à tout élément $Q \in H_{\mathbf{g}}$ est unique. L'action de Q combinée à celle de la conjugaison par γ^{-1} fixe le r-uplet $\mathbf{g}$ et donc permute les cycles dans $g(i,\lambda)$; on obtient ainsi une action de $H_{\mathbf{g}}$ sur $g(i,\lambda)$.

En plus de la condition $\mathrm{Cen}_{S_d}(G) = \{1\}$, nous supposerons que $H(r)$ agit transitivement sur $\mathrm{sni}_G(\mathbf{C})^{\mathrm{ab}}$. Alors l'action de $H_{\mathbf{g}}$ sur $g(i,\lambda)$ ne dépend pas (à équivalence près) du r-uplet $\mathbf{g}$ choisi dans $\mathrm{sni}_G(\mathbf{C})$ (voir [DeFr1;Remark 3.13]). Notons $\mathcal{H}$ l'espace de Hurwitz $\mathcal{H} = \mathcal{H}_G(\mathbf{C})$. La condition de transitivité ci-dessus entraîne que $\mathcal{H}$ est irréductible. D'après l'hypothèse $\mathrm{Cen}_{S_d}(G) = \{1\}$, les revêtements paramétrés par $\mathcal{H}$ n'ont pas d'automorphismes; en conséquence, il existe une famille universelle de Hurwitz $\mathcal{F}$ au-dessus de $\mathcal{H}$. Notons $f_{\mathrm{gen}} : X_{\mathrm{gen}} \to \mathbb{P}^1$ le revêtement générique de $\mathcal{F}$ et $F = \overline{\mathbb{Q}}(\mathcal{H})$ le corps des fonctions de $\mathcal{H}$, lequel est un corps de définition de f_{gen}.

Théorème 4.7 (Dèbes-Fried) [DeFr1;Th.3.14]**.** *Les orbites de $H_{\mathbf{g}}$ sur $g(i,\lambda)$ correspondent exactement aux orbites de G_F sur $P_{f_{\mathrm{gen}}}(\mathbf{g},\lambda)$.*

Il s'agit d'un énoncé sur le revêtement générique de $\mathcal{F}$. L'intérêt des familles de Hurwitz est que, ce type de propriété, une fois établi sur le revêtement générique, s'étend à tous les revêtements de la famille. Une application pratique du Th.4.7 est la suivante. Supposons que le groupe $H_{\mathbf{g}}$ possède une unique [8] orbite d'une longueur donnée ℓ. Le Th.4.7 permet d'en déduire que, pour tout revêtement $f : X \to \mathbb{P}^1$ de la famille de Hurwitz $\mathcal{F}$, il existe sur X un diviseur de longueur ℓ, rationnel sur le corps de définition de f.

Dans le cas où X est de genre 0 ou 1, le Th.4.7 conduit à un critère pratique d'existence de points rationnels sur X, en le combinant au fait suivant [DeFr1; Cor3.15 et Cor.3.17]. Pour trouver un point rationnel sur une courbe de genre 0, il suffit de trouver un diviseur rationnel de degré impair, et sur une courbe de genre 1, il suffit de trouver des diviseurs rationnels de degrés premiers entre eux. Plus généralement, cela conduit à la notion de points rationnels produits par la ramification [DeFr1;§3.2]: ce sont les points rationnels, qui comme diviseurs, sont dans le groupe engendré, par les diviseurs rationnels à support dans l'ensemble des points ramifiés de f, et les diviseurs de fonctions rationnelles. Des questions se posent naturellement [DeFr1;§3 & §4]. Ainsi, pour les genres 0 et 1, dans quelle mesure l'existence générique de points rationnels sur X est-elle équivalente à l'existence générique de points rationnels produits par la ramification (auquel cas le Th.4.7 devient un critère décisif quant à l'existence de points rationnels sur le revêtement générique de la famille de Hurwitz)? On peut également se demander si, pour ce qui est des points rationnels produits par la ramification, leur existence générique équivaut à leur existence sur toutes les courbes X de la famille considérée? On montre en fait, grâce au théorème d'irréductibilité de Hilbert, que cette seconde

[8] Soit k le corps de définition minimal de $\mathcal{H}$. L'unicité assure ici que l'orbite en question sera une orbite, non seulement du groupe de Galois $G_{\overline{\mathbb{Q}}(\mathcal{H})}$ mais aussi du groupe de Galois $G_{k(\mathcal{H})}$.

question a une réponse positive pour les genres 0 et 1 [DeFr1;Th.3.11]. Cette seconde question est évidemment à relier à la question similaire où l'on s'intéresse aux points rationnels quelconques (et pas seulement à ceux produits par la ramification). D'après un travail de Lewis et Schinzel [LeSc] (à l'origine de [DeFr1]), le résultat subsiste pour des familles de courbes de genre 0; mais on pense que le résultat devient faux dès le genre 1.

5. Tours modulaires

Les tours modulaires constituent un développement récent de la théorie des espaces de Hurwitz. Cette section présente leur construction (§5.1). L'exemple fondateur est celui de la tour des courbes modulaires (§5.2). En suivant cet exemple, on est conduit naturellement à certaines questions de nature arithmétique sur les tours modulaires en général (§5.3). La notion de tour modulaire est due à Fried; cette section est une présentation succinte de son article [Fr6].

5.1. Construction

On se donne un groupe fini G, plongé dans S_d, un nombre premier p divisant $|G|$, un entier $r \geq 3$ et un ensemble $\mathbf{C} = \{C_1, \ldots, C_r\}$ de classes de conjugaison de G dont les éléments ont un ordre premier à p.

On note ${}_p\tilde{G}$ le p-revêtement universel de Frattini de G. Rappelons (voir [FrJa] pour plus de détails) qu'un homomorphisme surjectif de groupes (un revêtement) $\psi : H \to G$ est dit *de Frattini* si, pour tout sous-groupe H' de H, $\psi(H') = G \Rightarrow H' = H$, ou, de façon équivalente, si son noyau est contenu dans l'intersection des sous-groupes maximaux de G. Par exemple, l'homomorphisme $\mathbb{Z}/(p_1^{\alpha_1} \cdots p_r^{\alpha_r})\mathbb{Z} \to \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$ est de Frattini $(\alpha_1, \ldots, \alpha_r > 0)$. Le produit fibré de deux revêtements de Frattini a la propriété de Frattini. Il y a un objet universel pour les revêtements de Frattini d'un groupe G donné. On le note $\tilde{G}$ et on peut montrer que $\tilde{G}$ est un revêtement profini projectif de G. Par exemple, pour $G = \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$, on a $\tilde{G} = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$. Il existe aussi un objet universel pour les revêtements de Frattini $\psi : H \to G$ de G de noyau $\ker(\psi)$ un p-groupe. C'est cet objet qu'on appelle le p-revêtement universel de Frattini de G et qu'on note ${}_p\tilde{G}$. Par exemple, pour $G = \mathbb{Z}/(p_1 \cdots p_r)\mathbb{Z}$, on a ${}_{p_1}\tilde{G} = \mathbb{Z}_{p_1} \times \mathbb{Z}/p_2\mathbb{Z} \cdots \times \mathbb{Z}/p_r\mathbb{Z}$.

On définit ensuite, à partir du noyau ker de l'homomorphisme ${}_p\tilde{G} \to G$, une suite de quotients caractéristiques de ${}_p\tilde{G}$:

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

et on note ${}_p^n\tilde{G}$ le quotient ${}_p\tilde{G}/\ker_n$ $(n \geq 0)$. Par exemple, pour $G = \mathbb{Z}/p\mathbb{Z}$, on a $\ker_n = p^{n+1}\mathbb{Z}_p$ et ${}_p^n\tilde{G} = \mathbb{Z}/p^{n+1}\mathbb{Z}$.

Lemme 5.1. *Si C est une classe de conjugaison d'éléments de ${}_p^n\tilde{G}$ d'ordre ρ premier à p, alors il existe une unique classe de conjugaison de ${}_p^{n+1}\tilde{G}$ relevant C et dont les éléments sont d'ordre ρ.*

Preuve. Notons $\phi : {}_p^{n+1}\tilde{G} \to {}_p^n\tilde{G}$ la surjection naturelle. Soient $g \in C$ et $H = \phi^{-1}(< g >)$. On a une suite exacte $1 \to \ker_n/\ker_{n+1} \to H \to < g > \to 1$. D'après le lemme de Schur-Zassenhaus, comme g est d'ordre premier à p, cette suite est scindée; de plus, il y a unicité de la section $< g > \to H$, à conjugaison près. □

Grâce à ce lemme, on peut définir , pour tout $n \geq 0$, un r-uplet, noté $\mathbf{C}^n = (C_1^n, \ldots, C_r^n)$ de classes de conjugaisons de ${}_p^n\tilde{G}$, de telle façon que C_i^{n+1} relève C_i^n et soit de même ordre, $i = 1, \ldots, r$ (par ordre, on entend ici l'ordre des éléments dans la classe). Cette définition fournit naturellement, pour tout $n \geq 0$, une flèche

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

Dans le cas de revêtements purs, il faut encore définir, de façon compatible, une représentation T_n de ${}_p^n\tilde{G}$ dans un groupe symétrique ($n \geq 0$). Notons $G(1)$ le fixateur de 1 dans la représentation $G \subset S_d$ et choisissons le premier p ne divisant pas l'ordre de $G(1)$. En appliquant comme ci-dessus le lemme de Schur-Zassenhaus, on obtient qu'il existe une copie de $G(1)$ dans l'image inverse de $G(1)$ par le morphisme ${}_p^n\tilde{G} \to G$, unique à conjugaison près ($n \geq 0$). On définit T_n comme l'action par translation à gauche de ${}_p^n\tilde{G}$ sur les classes à gauche modulo cette copie de $G(1)$ ($n \geq 0$).

A tout entier $n \geq 0$, on peut maintenant associer un espace de Hurwitz

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

Pour tout $n \geq 0$, il y a un morphisme naturel $\psi_n : \mathcal{H}_{n+1} \to \mathcal{H}_n$. La collection des espaces $\mathcal{H}_n$ et des morphismes ψ_n ($n \geq 0$) est appelée *tour modulaire* associée au triplet $(G \subset S_d, p, \mathbf{C})$.

5.2. Le cas du groupe diédral

Comme en §3.1.4, on prend ici $G = D_p = \mathbb{Z}/p \times^s \mathbb{Z}/2$, $r = 4$ et les quatre classes $C_1, \ldots, C_4$ égales à la classe C des involutions de G. On a alors ${}_p\tilde{D}_p = \mathbb{Z}_p \times^s \mathbb{Z}_2 := D_{p^\infty}$ et pour tout $n \geq 0$, ${}_p^n\tilde{D}_p = D_{p^n}$. On sait (§3.1.4) qu'il existe un morphisme surjectif et défini sur $\mathbb{Q}$

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

D'autre part, on a pour tout $n > 0$, un diagramme commutatif

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

où la flèche verticale de droite $\times p$ est la multiplication par p. En d'autres termes, il existe un morphisme de la tour modulaire associée au triplet $(G \subset S_d, p, \mathbf{C})$ vers la tour des courbes modulaires $(X_1(p^n))_{n>0}$.

5.3. Questions arithmétiques sur les tours modulaires

Comme précédemment, on s'intéresse aux corps de définition des composantes irréductibles et, éventuellement, à l'existence de points rationnels sur ces composantes. Ci-dessous, nous précisons ces questions en poursuivant le parallèle avec la tour des courbes modulaires.

5.3.1. Composantes irréductibles. Soit $\mathcal{T}$ une composante irréductible de $\mathcal{H}_1$ (correspondant à une orbite $\mathcal{O}$ de H_r sur $\mathrm{ni}_G(\mathbf{C})^{\mathrm{ab}}$ (ou $\mathrm{ni}_G(\mathbf{C})^{\mathrm{in}}$ dans la situation de G-revêtements comme en §5.2 par exemple). On cherche à quelle condition cette composante se relève au niveau n.

Proposition 5.2 [Fr6]**.** *Pour $\mathbf{g} \in \mathcal{O}$, on définit le sous-ensemble $\nu_n(\mathbf{g}) \subset {}^n_p\tilde{G}$ par*

$$\nu_n(\mathbf{g}) = \left\{ \tilde{g}_1 \cdots \tilde{g}_r \;\middle|\; \begin{array}{l} \tilde{g}_i \in {}^n_p\tilde{C}_i, i = 1, \ldots, r \text{ (à l'ordre près)} \\ \text{et } \tilde{\mathbf{g}} \text{ relève } \mathbf{g} \end{array} \right\}$$

(a) *L'ensemble $\nu_n(\mathbf{g})$ ne dépend que de $\mathcal{O}$ et définit donc un invariant $\nu_n(\mathcal{O})$.*

(b) *Il existe une composante irréductible de $\mathcal{H}_n$ au-dessus de $\mathcal{T}$ ssi $1 \in \nu_n(\mathcal{O})$.*

(c) *Si $1 \in \nu_n(\mathcal{O})$, alors tout élément $\mathbf{g} \in \mathcal{O}$ se relève dans $\mathrm{ni}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$. En conséquence les composantes irréductibles de $\mathcal{H}_n$ s'envoient surjectivement sur celles de $\mathcal{H}_1$.*

Preuve. (b) Le sens ($\Rightarrow$) est trivial. Inversement, supposons $1 \in \nu_n(\mathcal{O})$. Il existe donc un r-uplet $\tilde{\mathbf{g}}$ tel que $\tilde{g}_1 \cdots \tilde{g}_r = 1$ et $\tilde{g}_i \in {}^n_p\tilde{C}_i$, $i = 1, \ldots, r$ (à l'ordre près). Pour conclure que $\tilde{\mathbf{g}} \in \mathrm{ni}_{{}^n_p\tilde{G}}(\mathbf{C}^n)$, et donc que la composante $\mathcal{T}$ se relève dans $\mathcal{H}_n$, il reste à voir que $\tilde{g}_1, \ldots, \tilde{g}_r$ engendrent le groupe ${}^n_p\tilde{G}$. Cela provient de la propriété de Frattini du revêtement ${}^n_p\tilde{G} \to G$.

Soient $\mathbf{g}^o, \mathbf{g} \in \mathcal{O}$; $\mathbf{g}$ est de la forme $(\mathbf{g}^o)Q$ avec $Q \in H_r$. Si $\tilde{\mathbf{g}}^o_n$ relève $\mathbf{g}^o$, alors $\tilde{\mathbf{g}}_n = (\mathbf{g}^o_n)Q$ relève $\mathbf{g}$ et $\tilde{g}_1 \cdots \tilde{g}_r = \tilde{g}^o_1 \cdots \tilde{g}^o_r$. On en déduit (a) et (c). $\square$

Remarque 5.3. La preuve de (b) montre l'utilité de la propriété de Frattini. Les revêtements de Frattini ont cette autre propriété notable: ils ne peuvent pas être scindés (sauf à être des isomorphismes). D'une certaine façon, être scindé et être de Frattini sont deux propriétés à l'opposé l'une de l'autre dans le paysage des extensions de groupes. Rappelons aussi ce fait utile: le revêtement universel de Frattini est un revêtement projectif [FrJa].

Une composante $\mathcal{T}$ de $\mathcal{H}_1$ est dite *obstruée* au niveau n s'il n'existe pas de composante irréductible $\mathcal{T}_n$ de $\mathcal{H}_n$ se projetant sur $\mathcal{T}$. Une condition nécessaire et suffisante est que $1 \notin \nu_n(\mathcal{O})$. Ce phénomène n'arrive pas avec la tour des courbes modulaires puisque chaque niveau de la tour est irréductible. En général, les composantes d'une tour modulaire au-dessus d'une composante donnée de $\mathcal{H}_1$ forment un arbre, avec des chaines finies ou infinies.

On définit ensuite $\nu(\mathcal{O})$ comme la limite projective des $\nu_n(\mathcal{O})$ $(n \geq 1)$. Le résultat ci-dessous dit essentiellement que $\nu(\mathcal{O})$ est un invariant qui peut permettre de distinguer arithmétiquement deux composantes irréductibles de $\mathcal{H}_1$, et donc de trouver éventuellement des composantes irréductibles définies sur $\mathbb{Q}$.

Théorème 5.4 [Fr6;Th.3.16]**.** *Supposons G de centre trivial. Soit $\mathcal{H}_1 = \bigcup_{i=1}^{t} \mathcal{H}_{1i}$ la décomposition de $\mathcal{H}_1$ en composantes irréductibles. Supposons que $\mathcal{H}_1$ est défini sur $\mathbb{Q}$ (e.g. $C_1, \dots, C_r$ sont rationnelles). Alors $G_{\mathbb{Q}}$ permute les composantes $\mathcal{H}_{1i}$. Plus précisément, pour tout $\tau \in G_{\mathbb{Q}}$, on a*

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

où $\chi : G_{\mathbb{Q}} \to (\mathbb{Z}_p)^{\times}$ est le caractère cyclotomique modulo $(p^n)_{n\geq 1}$. [9]

En particulier, si $\nu(\mathcal{H}_{1i})^t = \nu(\mathcal{H}_{1i})$ pour tout $t \in (\mathbb{Z}_p)^{\times}$ et $\nu(\mathcal{H}_{1i}) \neq \nu(\mathcal{H}_{1j})$ pour $j \neq i$, alors $\mathcal{H}_{1i}$ est défini sur $\mathbb{Q}$. En effet, la première condition entraîne que, pour tout $\tau \in G_{\mathbb{Q}}$, $\mathcal{H}_{1i}$ et $\mathcal{H}_{1i}^{\tau}$ on même invariant ν. Comme, d'après la seconde condition, cet invariant distingue $\mathcal{H}_{1i}$ des autres composantes, $\mathcal{H}_{1i} = \mathcal{H}_{1i}^{\tau}$, pour tout $\tau \in G_{\mathbb{Q}}$.

5.3.2. Système projectif de points rationnels. Considérons un système projectif de points $(\mathbf{p}_n)_{n>0}$ sur la tour des courbes modulaires. Chaque point $\mathbf{p}_n$ correspond à la donnée d'un point de p^n-torsion sur une courbe elliptique E (la même pour tout n). Supposons que E est définie sur un corps K. Le groupe G_K opère sur l'ensemble des points de p-torsion de E: il s'agit de l'action de G_K sur le $\mathbb{Z}_p$-module de Tate V_p associé à E. Notons $j : X_1(p) \to \mathbb{P}^1$ l'application qui a un point $(E, \mathbf{p}) \in X_1(p)$ associe l'invariant canonique de la courbe elliptique E. L'action précédente est une action sur l'ensemble des systèmes projectifs de points $(\mathbf{p}_n)_{n>0}$ au-dessus de l'invariant $j(E)$ de E.

[9] Pour tout $n \geq 1$, l'élément $\nu_n(\mathcal{O}) \in {}_p^n\tilde{G}$ appartient à ker_o/ker_n qui est par construction un p-groupe, disons d'ordre p^N. En conséquence, toute puissance $\nu_n(\mathcal{O})^t$ avec $t \in \mathbb{Z}/p^N\mathbb{Z}$ a un sens.

On obtient de la même façon une représentation de G_K dans la situation plus générale d'une tour modulaire:

(*) Le groupe G_K opère sur l'ensemble des systèmes projectifs de points $(\mathbf{p}_n)_{n>0}$ au-dessus d'un élément fixé $\mathbf{t} \in \mathcal{U}_r(K)$.

Dans le cas des courbes modulaires, un théorème célèbre de Serre permet d'affirmer que, si K est un corps de nombres,

(**) étant donnés un système projectif de points $(\mathbf{p}_n)_{n>0}$ au-dessus de $j \in \mathbb{P}^1(K)$ et une extension finie F/K, $\mathbf{p}_n \notin \mathcal{H}_n(F)$, sauf pour un nombre fini d'entiers n.

En effet, il n'y a qu'un nombre fini de points de p-torsion F-rationnels sur une courbe elliptique définie sur K donnée. On peut penser que cet énoncé subsiste en général, avec $\mathbf{t} \in \mathcal{U}_r(K)$ au lieu de $j \in \mathbb{P}^1(K)$ et avec éventuellement quelques hypothèses supplémentaires. En particulier, il semble naturel de fixer un système projectif $(\mathcal{T}_n)_{n>0}$ de composantes irréductibles définies sur K telles que pour tout $n > 0$, $\mathbf{p}_n \in \mathcal{T}_n(K)$.

Références

[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] P. Deligne and D. Mumford, 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] T. Ekedahl, 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] J. Harris and D. Mumford, 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] S. Mochizuki, 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] S. Wewers, 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).