THÈSE DE DOCTORAT DE L'UNIVERSITÉ LILLE I

Spécialité : **Mathématiques Pures**

présentée par :

Anna Cadoret

pour obtenir le grade de docteur de l'Université Lille I

Théorie de Galois inverse et arithmétique des espaces de Hurwitz

---

soutenue le 16 Décembre 2004 devant le jury composé de :

M. Jean-Marc COUVEIGNES	(Univ. Toulouse II)	Rapporteur
M. Pierre DÈBES	(Univ. Lille I)	Directeur
M. Michel EMSALEM	(Univ. Lille I)	
M. Marc HINDRY	(Univ. Paris VII)	
M. Helmut VOELKLEIN	(Univ. Essen)	Rapporteur
M. Stefan WEWERS	(Univ. Bonn)	

Remerciements

Je tiens avant tout à exprimer ma profonde gratitude envers Pierre Dèbes pour avoir encadré ma thèse d'une façon remarquable, pour tout ce qu'il m'a appris, pour l'énergie qu'il ma consacrée, pour sa gentillesse et sa grande disponibilité. Il a toujours su me guider et m'encourager. Il s'est aussi attaché à me transmettre ses exigences de clarté et de rigueur en matière d'exposition. Il a répondu à toutes mes attentes et j'ai pris beaucoup de plaisir à apprendre avec lui le métier de mathématicien.

Je suis reconnaissante à Jean-Marc Couveignes et à Helmut Voelklein d'avoir bien voulu rapporter cette thèse et assister à ma soutenance. Je suis heureuse que Michel Emsalem, Marc Hindry et Stefan Wewers aient accepté de faire partie de mon jury, et je les en remercie sincèrement.

Je remercie également Mike Fried pour l'enthousiasme qu'il a toujours montré à l'égard de mon travail ; nombre de ses idées irriguent d'ailleurs cette thèse. Je pense aussi à tous ceux qui se sont intéressés à mes résultats et ont bien voulu me faire part de leurs commentaires ou répondre à mes questions.

Je suis redevable à Daniel Bertrand d'être à l'origine de ma rencontre avec Pierre Dèbes et à Yves Laszlo non seulement d'avoir encadré mon stage de D.E.A. mais aussi de m'avoir offert la possibilité de travailler dans les excellentes conditions de Chevaleret.

C'est lors de mon stage de maîtrise que j'ai été initiée à la recherche mathématique. Je le dois à Ivan Correa, qui dirigea mon mémoire sur les algèbres non associatives, et aux longues heures que nous avons passées dans son bureau de La Serena, buvant des litres de café brûlant pour lutter contre le froid et pouvoir continuer à travailler...

Je voudrais aussi saluer ici mes compagnons de route : ceux rencontrés et retrouvés au détour des conférences, les thésards du plateau 7C à Chevaleret, les occupants successifs du bureau M2 318 à l'U.S.T.L. et, bien sûr, la chaleureuse équipe du G.T.E.M. lillois.

Je dois accorder une mention spéciale au Tio, dont la présence don quichottesque m'a toujours fait le plus grand bien.

Et surtout à Nikolaz, pour tout ce que nous avons su partager ces dernières années.

Reste enfin ceux qui sont là, inconditionnellement, depuis toujours et pour qui je ne trouverai pas les mots. Mon père et ma mère.

À Marie Lebas

À Claude Peucat

Introduction

Cette thèse se compose de deux grandes parties.

La première partie a pour objet de donner - en français - une vue d'ensemble de notre travail. Elle contient un chapitre de préliminaires qui tente d'exposer de façon concise les principaux outils utilisés dans la suite et un chapitre de présentation qui fait un bilan relativement détaillé des résultats obtenus et de leur cohérence, en les replaçant dans le contexte du problème de Galois inverse régulier.

La deuxième partie se divise en quatre chapitres. Les trois premiers reprennent les articles suivants :

Chapitre 3 : Counting real Galois covers of the projective line (à paraitre au P.J.M.).

Chapitre 4 : Harbater-Mumford subvarieties of moduli spaces of covers (soumis).

Chapitre 5 : Rational points on Hurwitz towers (soumis).

avec, à l'occasion, quelques modifications ou compléments que nous signalons en en-tête de chapitre. Le chapitre 6 est original.

On a conservé dans leur intégralité les sections introductives des chapitres 3, 4, 5. Celles-ci contiennent des rappels sur les notations et les notions permettant de lire la suite sans se référer au chapitre 1. Inversement, la lecture du chapitre 1 permet de sauter ces sections introductives (ou de ne s'en servir que comme aide-mémoire pour les notations).

Le chapitre 3 considère le problème suivant : étant donné un groupe fini G, un diviseur de points de branchement réel $\mathbf{t}$ de cardinal $r \geq 3$ et un r-uplet $\mathbf{C} = (C_1, ..., C_r)$ de classes de conjugaison non triviales de G, combien y-a-t-il de G-revêtements de $\mathbb{P}^1_{\mathbb{C}}$ définis sur $\mathbb{R}$ ou de corps des modules $\mathbb{R}$ et d'invariants G, $\mathbf{C}$, $\mathbf{t}$? J.-P. Serre a montré que le nombre total de G-revêtements d'invariants G, $\mathbf{C}$, $\mathbf{t}$ pouvait être calculé à partir de la table des caractères de G. Nous réutilisons cette méthode dans le contexte des G-revêtements définis sur $\mathbb{R}$ ou de corps des modules $\mathbb{R}$ pour lesquels il existe une caractérisation des descriptions de cycles de branchement due à P. Dèbes et M. Fried du même type que celle donnée par le théorème d'existence de Riemann dans le cas général. Nous obtenons ainsi des formules explicites. Ces formules permettent d'évaluer le nombre de G-revêtements de corps des modules $\mathbb{R}$ mais non définis sur $\mathbb{R}$ et, en particulier, d'exhiber de nombreuse familles infinies de G-revêtements non définis sur leur corps des modules avec des groupes de Galois arbitrairement grands. De même, on peut comparer le nombre de G-revêtement défini sur $\mathbb{R}$ au nombre total de G-revêtements. Quand ces deux nombres coincident, on obtient des réalisations régulières sur le corps $\mathbb{Q}^{tr}$ des nombres algébriques totalement réels avec un diviseurs de point de branchement rationnel ; nous donnons ainsi une réalisation régulière non rigide des groupes prodihédraux D_{2a^∞} sur $\mathbb{Q}^{tr}$ avec diviseur de points de branchement rationnel.

Le chapitre 4 donne un résultat d'irréductibilité sur les espaces de Hurwitz dessymétrisés dans l'esprit du théorème de Conway-Parker pour les espaces de Hurwitz symétrisés ou du théorème 3.21 [F95a] de Fried pour les composantes H-M des espaces de Hurwitz dessymétrisés mais avec, de plus, une interprétation modulaire en termes de points de branchement. Si G est, par exemple, un groupe fini possédant deux classes de conjugaison A, B telles que $G =< A >=< B >$ et $G =< a, b >$, quelque soit $a \in A$, $b \in B$ alors, en posant $\mathbf{C}_s = (A, A^{-1}, (B, B^{-1})^{s-1})$, pour s suffisamment grand l'espace de Hurwitz dessymétrisé $\mathcal{H}'_{2s,G}(\mathbf{C}_s)$ classifiant les G-revêtements d'invariants G, $\mathbf{C}_s$ avec points de branchements ordonnés possède une composante géométriquement irréductible $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C}_s)$, définie sur le même corps $\mathbb{Q}'_{\mathbf{C}_s}$ que $\mathcal{H}'_{2s,G}(\mathbf{C}_s)$ et dont les sous-variétés fermées obtenues en spécialisant tous les

points de branchement sauf le premier restent géométriquement irréductibles. Dans le cas général, ce résultat reste vrai en remplaçant "tous les points de branchement sauf le premier" par "tous les points de branchement sauf les $r(G)$ premiers" où $r(G)$ est une constante ne dépendant que de G ; on obtient donc des sous-variétés fermées géométriquement irréductibles de dimension $r(G)$ et ce sont ces sous-variétés fermées que l'on appelle sous-variétés de Harbater-Mumford. En combinant techniques de recollement pour les corps complets, variétés de descente et principe local-global, on peut en outre, pour tout ensemble fini Σ de places de $\mathbb{Q}'_{\mathbf{C}}$ de caractéristique résiduelle première à l'ordre de G, construire ces sous-variétés de sorte que leur image symétrisée (*i.e.* via le morphisme $\mathcal{H}'_{r_s,G}(\mathbf{C}_s) \to \mathcal{H}_{r_s,G}(\mathbf{C}_s)$ possèdent des points $\mathbb{Q}'^{\Sigma}_{\mathbf{C}}$-rationnels correspondant à des G-revêtements définis sur $\mathbb{Q}'^{\Sigma}_{\mathbf{C}}$ (où $\mathbb{Q}'^{\Sigma}_{\mathbf{C}}$ l'extension maximale de $\mathbb{Q}'_{\mathbf{C}}$ totalement décomposée en chacune des places $P \in \Sigma$). Par ailleurs, notre résultat est compatible avec les extensions de Frattini ; on peut en particulier remplacer les espaces de Hurwitz dessymétrisés $\mathcal{H}'_{2s,G}(\mathbf{C})$ par les tours modulaires $(\mathcal{H}'_{2s,p^{n+1}\tilde{G}}(\mathbf{C}_{n+1}) \twoheadrightarrow \mathcal{H}'_{2s,p^n\tilde{G}}(\mathbf{C}_n))_{n\geq 0}$ associées à G, $\mathbf{C}$, p (p étant un nombre premier divisant $|G|$ mais pas l'ordre des éléments de $C_1, ..., C_s$), obtenant ainsi la conservation d'une propriété arithmétique forte le long de la tour modulaire. En termes de G-revêtements, on obtient par exemple que pour tout $n \geq 0$ le n-ième 5-quotient caractéristique $^n_5\tilde{M}_{23}$ du groupe de Matthieu M_{23} est groupe de Galois d'une extension régulière de $\mathbb{Q}(i\sqrt{7})^{\Sigma}$ avec un diviseur de ramification de la forme $\{t_1\} + \mathbf{t}_{\Sigma}$ où $\mathbf{t}_{\Sigma}$ est rationel (Pour tout ensemble fini Σ de places de $\mathbb{Q}(i\sqrt{7})$ de caractéristique résiduelle ne divisant pas $|M_{23}|$).

Le chapitre 5 étudie le problème de Galois inverse régulier pour les groupes profinis G qui sont extension d'un groupe fini G_0 par un groupe pronilpotent projectif de rang fini P. On montre que de tels groupes ne peuvent être groupe de Galois d'une extension $K/\overline{k}(T)$ de corps des modules k quand k est un corps de nombres ou un corps fini de caractéristique ne divisant ni $|G_0|$ ni p si P est un pro-p groupe. Géométriquement, ce résultat signifie qu'aucune tour d'espaces de Hurwitz associée à G ne possède de système projectif de points k-rationnels. On montre dans un premier temps que G ne peut être réalisé régulièrement sur k puis que toute extension galoisienne régulière $K/\overline{k}(T)$ de corps des modules k et de groupe G est définie sur une extension finie k_0/k. On donne ensuite quelques applications des résultats précédents au problème de Galois inverse (régulier) pour G, par exemple la variante q-adique suivante : *Soit q un nombre premier ne divisant pas $|G|$ et $k/\mathbb{Q}_q$ une extension finie. Alors il existe une réalisation régulière de G sur k ssi G est engendré par un nombre fini d'éléments d'ordre fini. Toute réalisation régulière de G sur k a alors un diviseur de points de branchement fini et ayant mauvaise réduction modulo q.* On termine en montrant que la Strong Torsion Conjecture pour les variétés abéliennes implique l'une des conjectures de Fried sur la disparition des points rationnels le long d'une tour modulaire.

Le chapitre 6, enfin, étudie les courbes de Hurwitz standards *i.e.* les courbes obtenues en fixant tous les points de branchement sauf le premier sur un espace de Hurwitz dessymétrisé. Nous démontrons d'abord une formule générique - qui généralise la formule classique du cas $r = 4$ au cas r quelconque - permettant de calculer le genre d'une telle courbe. Puis nous décrivons une nouvelle méthode de genre 0 pour $r = 4$ basée sur le principe de Hasse.

Table des matières

Première partie

Chapitre 1

Préliminaires

Sommaire

Introduction

L'objet de ce chapitre consacré aux préliminaires est d'introduire - de façon aussi cohérente que possible - les notions étudiées dans cette thèse et les outils utilisés. Nous rappelons d'abord les différentes manières de manipuler la notion de G-revêtement et celles, associées, de corps des modules et corps de définition. Nous introduisons ensuite les espaces de modules pour les G-revêtements, leur description combinatoire et quelques unes de leurs propriétés arithmétiques puis énonçons les résultats fondamentaux pour les G-revêtements sur les corps complets. Nous terminons par deux outils géométrico-arithmétiques, le principe local-global et les variétés de descentes. Nous ne donnons ici aucune preuve des résultats énoncés qui - pour la plupart - sont classiques ; nous renvoyons pour cela à la riche littérature sur le sujet.

1.1 Catégories des G-revêtements de la droite projective

La première partie de cette section a pour but de définir les objets centraux de cette thèse que sont les G-revêtements de la droite projective. Nous en présentons succintement les différentes catégories (topologique, analytique, géométrique, arithmétique ou combinatoire) et les invariants qui peuvent leur être associés. Le théorème d'existence de Riemann (et sa généralisation par Grothendieck) montre que ces différentes catégories sont équivalentes. Dans la seconde partie de cette section nous rappelons les notions de corps de module et corps de définition d'un G-revêtement ainsi que la construction de

l'obstruction cohomologique.

Dans tout ce qui suit, étant donné un corps k algébriquement clos, on supposera toujours fixée un système compatible $(\zeta_n)_{n\geq 1}$ de raçines primitives n-ièmes de l'unité (*i.e.* $\zeta_{mn}^m = \zeta_n$, $n, m \geq 1$). Quand $k = \mathbb{C}$, on prendra $\zeta_n = \mathrm{e}^{\frac{2\pi i}{n}}$, $n \geq 1$.

1.1.1 Théorème d'existence de Riemann

1.1.1.1 Théorème d'existence de Riemann pour les G-revêtements

Dans tout ce qui suit on se fixe un groupe fini G, un entier $r \geq 3$ et un sous ensemble $\mathbf{t} \subset \mathbb{P}^1(\mathbb{C})$ de cardinal r. On notera X^{top} l'espace topologique $\mathbb{P}^1(\mathbb{C})$, X^{an} la droite projective complexe munie de sa structure de surface de Riemann et X^{alg} la droite projective complexe munie de sa structure de variété algébrique complexe. On notera $\mathcal{R}_{\mathbf{t}}^{\mathrm{top}}$ la catégorie des revêtements topologiques finis galoisiens de $X^{\mathrm{top}} \setminus \mathbf{t}$ (resp. $\mathcal{R}_{\mathbf{t}}^{\mathrm{an}}$ la catégorie des revêtements analytiques finis galoisiens non ramifiés de $X^{\mathrm{an}} \setminus \mathbf{t}$, $\mathcal{R}_{\mathbf{t}}^{\mathrm{alg}}$ la catégorie des revêtements algébriques finis galoisiens étales de $X^{\mathrm{alg}} \setminus \mathbf{t}$). A ces catégories on peut associer des G-catégories, $\mathcal{R}_{\mathbf{t},G}^{\mathrm{top}}$, $\mathcal{R}_{\mathbf{t},G}^{\mathrm{an}}$, $\mathcal{R}_{\mathbf{t},G}^{\mathrm{alg}}$, un G-objet étant un couple (f, α) où f est un objet de la catégorie initiale et $\alpha : \mathrm{Aut}(f) \to G$ un isomorphisme de groupes et un morphisme de G-objets de (f_1, α_1) dans (f_2, α_2) un morphisme u de f_1 dans f_2 dans la catégorie initiale vérifiant de plus $\alpha_2 \circ u^\star = \alpha_1$. Le théorème d'existence de Riemann pour les G-revêtements s'énonce alors

Theorem 1.1 (théorème d'existence de Riemann (1)) *Les catégories $\mathcal{R}_{\mathbf{t},G}^{\mathrm{top}}$, $\mathcal{R}_{\mathbf{t},G}^{\mathrm{an}}$, $\mathcal{R}_{\mathbf{t},G}^{\mathrm{alg}}$ sont équivalentes.*

On peut résumer les grandes lignes de la preuve de ce théorème par le schéma suivant, où $\tilde{\mathcal{R}}_{\mathbf{t},G}^{\mathrm{an}}$ (resp. $\tilde{\mathcal{R}}_{\mathbf{t},G}^{\mathrm{alg}}$) désigne la catégorie des G-revêtements analytiques (resp. algébriques) finis de X^{an} (resp. X^{alg}) ramifiés seulement au dessus de $\mathbf{t}$:

$$\mathcal{R}_{\mathbf{t},G}^{\mathrm{top}} \underset{\text{oubli}}{\overset{\text{local}}{\rightleftarrows}} \mathcal{R}_{\mathbf{t},G}^{\mathrm{an}} \underset{\text{restriction}}{\overset{\text{complétion}}{\rightleftarrows}} \tilde{\mathcal{R}}_{\mathbf{t},G}^{\mathrm{an}} \underset{\text{principe } G.A.G.A}{\overset{}{\rightleftarrows}} \tilde{\mathcal{R}}_{\mathbf{t},G}^{\mathrm{alg}} \underset{\text{complétion}}{\overset{\text{restriction}}{\rightleftarrows}} \mathcal{R}_{\mathbf{t},G}^{\mathrm{alg}}$$

On peut énoncer le principe G.A.G.A. en termes de G-revêtements comme suit :

Theorem 1.2 *Etant donnés un recouvrement de $\mathbb{P}^1(\mathbb{C})$ par deux ouverts métriques X_1 et X_2 d'intersection X_0 le foncteur de changement de base naturel*

$$\tilde{\mathcal{R}}_{\mathbb{P}^1(\mathbb{C}),G}^{\mathrm{alg}} \quad \to \quad \tilde{\mathcal{R}}_{X_1,G}^{\mathrm{an}} \times_{\tilde{\mathcal{R}}_{X_0,G}^{\mathrm{an}}} \tilde{\mathcal{R}}_{X_2,G}^{\mathrm{an}}$$

est une équivalence de catégories (ici, le terme de droite désigne le 2-produit fibré de $\tilde{\mathcal{R}}_{X_1,G}^{\mathrm{an}}$ et $\tilde{\mathcal{R}}_{X_2,G}^{\mathrm{an}}$ au dessus de $\tilde{\mathcal{R}}_{X_0,G}^{\mathrm{an}}$).

Nous renvoyons par exemple à [D95] ou [V99] pour des preuves détaillées de ce théorème.

Dans tout ce qui suit, notons $\pi_{\mathbf{t}}^\star$ le groupe fondamental $\pi_1^\star(X^\star \setminus \mathbf{t})$ et $\mathcal{P}_{\mathbf{t},G}^\star$ la catégorie dont les objets sont les épimorphismes de groupes $\Phi : \pi_{\mathbf{t}}^\star \twoheadrightarrow G$ et les morphismes de Φ_1 dans Φ_2 l'ensemble des $g \in G$ tels que $i_g \circ \Phi_1 = \Phi_2$, où $i_g \in \mathrm{Inn}(G)$ est la conjugaison intérieure par $g \in G$. Par définition du groupe fondamental, les catégories $\mathcal{P}_{\mathbf{t},G}^\star$ et $\mathcal{R}_{\mathbf{t},G}^\star$ sont équivalentes pour $\star$ =top, an, alg. En particulier, on déduit du théorème 1.1 le théorème suivant

Theorem 1.3 (théorème d'existence de Riemann (2)) *On a les isomorphismes canoniques de groupes fondamentaux*

$$\pi_{\mathbf{t}}^{\mathrm{an}} \simeq \pi_{\mathbf{t}}^{\mathrm{alg}} \simeq \widehat{\pi_{\mathbf{t}}^{\mathrm{top}}}$$

où $\widehat{\pi_{\mathbf{t}}^{\mathrm{top}}}$ est la complétion profinie de $\pi_{\mathbf{t}}^{\mathrm{top}}$.

1.1.1.2 Invariants canoniques de l'inertie

A $\mathbf{t} \subset \mathbb{P}^1(\mathbb{C})$ on peut associer un bouquet topologique $\underline{\gamma}$ c'est à dire un r-uplet de classes d'homotopie de chemins $\gamma_1, ..., \gamma_r$ basés en un point $t_0 \notin \mathbf{t}$ tels que (i) $\gamma_1, ..., \gamma_r$ engendre le groupe fondamental topologique $\pi_{\mathbf{t}}^{\text{top}}$ avec la seule relation $\gamma_1 \cdots \gamma_r = 1$ et (ii) γ_i est un chemin fermé simple tournant une fois, dans le sens direct, autour de t_i, $i = 1, ..., r$. La donnée de $\underline{\gamma}$ définit une présentation de $\pi_{\mathbf{t}}^{\text{top}}$, *i.e.* un isomorphisme $\rho_{\underline{\gamma}} : F_{r-1} \to \pi_{\mathbf{t}}^{\text{top}}$, $\Gamma_i \to \gamma_i$, où $F_{r-1} =< \Gamma_1, ..., \Gamma_r | \Gamma_1 \cdots \Gamma_r = 1 >$ est le groupe libre à $r-1$ générateurs. Cela donne en particulier une équivalence (non canonique) de catégorie entre $\mathcal{P}_{\mathbf{t},G}^{\text{top}}$ et la catégorie $\mathcal{N}_{r,G}$ dont les objets sont les r-uplets $\mathbf{g} = (g_1, ..., g_r) \in G^r$ tels que (1) $G =< g_1, ..., g_r >$ et (2) $g_1 \cdots g_r = 1$ et les morphismes de $\mathbf{g}_1 = (g_{1,1}, ..., g_{1,r})$ dans $\mathbf{g}_2 = (g_{2,1}, ..., g_{2,r})$ l'ensemble des $g \in G$ tels que $g g_{1,i} g^{-1} = g_{2,i}$, $i = 1, ..., r$.

Toutes les G-catégories $\mathcal{C}_{\mathbf{t},G}$ définies ci-dessus sont en fait des groupoïdes ; notons $\sim$ la relation d'isomorphisme sur l'ensemble $\text{Ob}(\mathcal{C}_{\mathbf{t},G})$ des objets de $\mathcal{C}_{\mathbf{t},G}$. Le choix d'une présentation $\rho_{\underline{\gamma}}$ comme ci-dessus définit pour chacune de ces catégories $\mathcal{C}_{\mathbf{t},G}$ une équivalence de catégories $F_{\mathcal{C}_{\mathbf{t},G}} : \mathcal{C}_{\mathbf{t},G} \approx \mathcal{N}_{r,G}$ donc, par passage au quotient, une bijection $F_{\mathcal{C}_{\mathbf{t},G}} : \text{Ob}(\mathcal{C}_{\mathbf{t},G})/\sim \to \text{Ob}(\mathcal{N}_{r,G})/\sim$ [1]. Cela permet de définir une application "invariant canonique de l'inertie" $\text{Inv}_{\mathcal{C}_{\mathbf{t},G}} = F_{\mathcal{C}_{\mathbf{t},G}} \circ \text{Inv}$ à valeur dans l'ensemble $\mathcal{C}_r(G)$ des r-uplets $\mathbf{C} = (C_1, ..., C_r)$ de classes de conjugaison de G tels que $\mathbf{C} \cap \text{Ob}(\mathcal{N}_{r,G}) \neq \emptyset$,

$$\begin{array}{ccccc} \text{Ob}(\mathcal{C}_{\mathbf{t},G}) & \xrightarrow{F_{\mathcal{C}_{\mathbf{t},G}}} & \text{Ob}(\mathcal{N}_{r,G}) & \xrightarrow{\text{Inv}} & \mathcal{C}_r(G) \\ \downarrow & & \downarrow & \nearrow & \\ \text{Ob}(\mathcal{C}_{\mathbf{t},G})/\sim & \xrightarrow{F_{\mathcal{C}_{\mathbf{t},G}}} & \text{Ob}(\mathcal{N}_{r,G})/\sim & & \end{array} \quad \text{où} \quad \begin{array}{rccc} \text{Inv} : & \text{Ob}(\mathcal{N}_{r,G}) & \to & \mathcal{C}_r(G) \\ & \mathbf{g} = (g_1, ..., g_r) & \to & (C_{g_1}^G, ..., C_{g_r}^G) \end{array}$$

est surjective et constante sur les classes d'isomorphismes des objets de $\mathcal{C}_{\mathbf{t},G}$. En outre la définition de $\text{Inv}_{\mathcal{C}_{\mathbf{t},G}}$ est indépendante du choix de la présentation $\rho_{\underline{\gamma}}$. En utilisant les définition explicites des équivalences de catégories que nous n'avons pas rappelées, on retrouve les descriptions usuelles de l'invariant canonique de l'inertie :

- description topologique : Soit $\underline{\gamma}$ un bouquet topologique pour $\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t}$ basé en $t_0 \notin \mathbf{t}$. La monodromie induit un (anti)epimorphisme de groupes $BCD_{\underline{\gamma}} : \pi_{\mathbf{t}}^{\text{top}} \to \text{Aut}(f)$ et on dit que $\alpha \circ BCD_{\underline{\gamma}}(\gamma_i)$ est le générateur topologique distingué de l'inertie associé à t_i ; sa classe de conjugaison $C_{t_i} := C^G_{\alpha \circ BCD_{\underline{\gamma}}(\gamma_i)}$ ne dépend pas du choix de $\underline{\gamma}$, $i = 1, ..., r$ et on dit que le r-uplet $\underline{C} = (C_{t_1}, ..., C_{t_r}) \in \mathcal{C}_r(G)$ est l'invariant canonique topologique de l'inertie de (f, α).
- description algébrique : On suppose ici que k est un corps algébriquement clos de caractéristique 0 ou de caractéristique $p > 0$ et que (f, α) est alors ordinairement ramifié. Soit P_{t_i} la place de $k(T)$ associé à t_i, Q_{t_i} une place de $k(X)$ au-dessus de P_{t_i} et $u \in Q_{t_i}$ une uniformisante. On peut alors définir un monomorphisme (car la ramification est ordinaire) de groupes (indépendant du choix de l'uniformisante $u \in Q_{t_i}$) $\phi_{t_i} : I(Q_{t_i}|P_{t_i}) \to k$, $\omega \to \omega(u)/u[\text{mod } P_{t_i}]$. L'image de ϕ_{t_i} est le groupe des racines e_{t_i}-ièmes de l'unité où $e_{t_i} = |I(Q_{t_i}|P_{t_i})|$ est l'ordre du groupe d'inertie au dessus de t_i. On dit que $\omega_{t_i} := \alpha \circ \phi_{t_i}^{-1}(\zeta_{e_{t_i}}) \in G$ est le générateur algébrique distingué de l'inertie associé à t_i ; sa classe de conjugaison $C_{t_i} := C^G_{\alpha \circ \omega_{t_i}}$ ne dépend pas du choix de $Q_{t_i}|P_{t_i}$, $i = 1, ..., r$ et on dit que le r-uplet $\underline{C} = (C_{t_1}, ..., C_{t_r}) \in \mathcal{C}_r(G)$ est l'invariant canonique algébrique de l'inertie de (f, α).

Les invariants topologiques et algébriques de l'inertie coïncident.

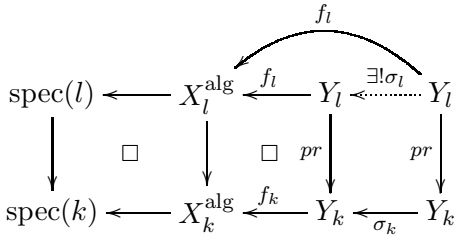
1.1.1.3 Changement de base

Via le foncteur de complétion la catégorie $\mathcal{R}_{\mathbf{t}}^{\text{alg}}$ est équivalente à la catégorie des revêtements algébriques finis galoisiens de X^{alg} ramifiés seulement au dessus de $\mathbf{t}$; on ne fera pas la distinction entre ces deux catégories. Les définitions de $\mathcal{R}_{\mathbf{t}}^{\text{alg}}$, $\mathcal{R}_{\mathbf{t},G}^{\text{alg}}$ s'étendent pour un corps k de caractéristique

[1] On dit que $\text{Ob}(\mathcal{N}_{r,G})$ est la classe de Nielsen associée à r, G et on la note plutôt $\text{ni}_r(G)$; de même, pour $\text{Ob}(\mathcal{N}_{r,G})/\sim$ on note $\overline{\text{ni}}_r(G)$.

0 (non nécessairement algébriquement clos), en remplaçant X^{alg} par la structure X_k^{alg} de k-variété de la droite projective ; on notera $\mathcal{R}_{\mathbf{t},k}^{\mathrm{alg}}$, $\mathcal{R}_{\mathbf{t},G,k}^{\mathrm{alg}}$ les catégories ainsi obtenues. Pour un corps k de caractéristique $p>0$, on imposera de plus aux revêtements d'être ordinairement ramifiés au dessus de $\mathbf{t}$; on notera donc $\mathcal{R}_{\mathbf{t},k}^{\mathrm{tame,alg}}$, $\mathcal{R}_{\mathbf{t},G,k}^{\mathrm{tame,alg}}$ les catégories correspondantes.

Etant donné une extension de corps $i : k \hookrightarrow l$, on dispose d'un foncteur naturel de changement de base $i^\star : \begin{array}{ccc} \mathcal{R}_{\mathbf{t},G,k}^{\mathrm{alg}} & \to & \mathcal{R}_{\mathbf{t},G,l}^{\mathrm{alg}} \\ (f_k,\alpha_k) & \to & i^\star(f_k,\alpha_k)=(f_l,\alpha_l) \end{array}$ défini par le diagramme cartésien



avec $\alpha_l : \begin{array}{ccc} \mathrm{Aut}(f_l) & \to & G \\ \sigma_l & \to & \alpha_k(\sigma_k) \end{array}$

En particulier, pour tout l-G-revêtement (f,α), les antécédents de (f,α) par $i^\star$ s'appellent les modèles de (f,α) sur k.

On peut maintenant énoncer le théorème de descente de Grothendieck [Gr61], Exp. XIII, cor. 2.12 qui généralise le théorème d'existence de Riemann à tout corps algébriquement clos de caractéristique 0 ou - avec restrictions - de caractéristique $p>0$:

Theorem 1.4 (Grothendieck) *Soit k un corps algébriquement clos de caractéristique 0 et $i : k \hookrightarrow \mathbb{C}$ un plongement complexe. Alors $i^\star : \mathcal{R}_{\mathbf{t},k}^{\mathrm{alg}} \approx \mathcal{R}_{\mathbf{t}}^{\mathrm{alg}}$ est une équivalence de catégories qui induit un isomorphisme*

$$\pi_{\mathbf{t}}^{alg} \to \pi_{k,\mathbf{t}}^{alg}$$

Soit k un corps séparablement clos de caractéristique $p>0$, A un anneau de valuation discrète de corps résiduel k et de corps des fraction K de caractéristique 0, $\tilde{t}_1^0,...,\tilde{t}_r^0 : spec(A) \to \mathbb{P}_A^1$ des sections relevant $t_1,...,t_r$ et $\tilde{t}_1,...,\tilde{t}_r : spec(\overline{K}) \to \mathbb{P}_{\overline{K}}^1$ leur tiré en arrière sur la fibre générique géométrique. On a alors un foncteur de spécialisation $s : \mathcal{R}_{\mathbf{t},k}^{\mathrm{alg,\ tame}} \Rightarrow \mathcal{R}_{\tilde{\mathbf{t}},\overline{K}}^{\mathrm{alg}}$ qui est essentiellement surjectif et devient une équivalence de catégorie si on suppose en outre que $p \not| |G|$. En terme de groupes fondamental cela signifie qu'on a un épimorphisme de groupes

$$\pi_{\overline{K},\mathbf{t}}^{alg} \twoheadrightarrow \pi_{k,\mathbf{t}}^{tame,alg}$$

et, en ne considèrant que les p'-parties des groupes fondamentaux, cette épimorphisme devient un isomorphisme

$$\pi_{\overline{K},\mathbf{t}}^{alg\ (p')} \to \pi_{k,\mathbf{t}}^{alg\ (p')}$$

Rappelons enfin que, via le foncteur corps de fonctions [Ha77], Chap. I §6, la G-catégorie $\mathcal{R}_{\mathbf{t},G,k}^{\mathrm{alg}}$ (resp. $\mathcal{R}_{\mathbf{t},G,k}^{\mathrm{tame,alg}}$) est équivalente à la G-catégorie $\mathcal{E}_{\mathbf{t},G,k}$ associée à la catégorie $\mathcal{E}_{\mathbf{t},k}$ des extensions galoisiennes finies régulières de $k(T)$ non ramifiées hors de $\mathbf{t}$ (resp. à la G-catégorie $\mathcal{E}_{\mathbf{t},G,k}^{\mathrm{tame}}$ associée à la catégorie $\mathcal{E}_{\mathbf{t},k}^{\mathrm{tame}}$ des extensions galoisiennes finies régulières de $k(T)$ non ramifiées hors de $\mathbf{t}$ et ordinairement ramifiée au dessus de $\mathbf{t}$). En particulier,

Theorem 1.5 ((RIGP/k), k corps algébriquement clos de caractéristique 0) *Pour tout sous-ensemble Γ_k-invariant $\mathbf{t} \subset \mathbb{P}^1(k)$ de cardinal r, la donnée d'une présentation $\rho_{\underline{\gamma}} : F_{r-1} \to \pi_{k,\mathbf{t}}^{\mathrm{alg}}$ définit une bijection entre les classes d'isomorphismes d'extensions galoisiennes finies $K/k(T)$ de groupe G non ramifiées hors de $\mathbf{t}$ et $\overline{\mathrm{ni}}_r(G)$.*

1.1.1.4 Action galoisienne

Dans tout ce qui suit on se fixe un corps k, une clôture séparable k^s, un entier $r \geq 3$ et un sous ensemble Γ_k-invariant $\mathbf{t} \subset \mathbb{P}^1(k^s)$ de cardinal r. Soit $k(T)^s$ une cloture séparable de $k(T)$ et $M_{k,\mathbf{t}}/k^s(T)$ l'extension algébrique maximale (dans $k(T)^s$) non ramifiée hors de $\mathbf{t}$ et ordinairement ramifiée au-dessus de $\mathbf{t}$. Les extensions $M_{k,\mathbf{t}}/k^s(T)$ et $M_{k,\mathbf{t}}/k(T)$ sont galoisiennes de groupes $\pi_{k,\mathbf{t}}^{\text{tame, alg}} = \text{Gal}(M_{k,\mathbf{t}}|k^s(T))$ et $\pi_{k,\mathbf{t}}^{\text{tame ar}} = \text{Gal}(M_{k,\mathbf{t}}|k(T))$ respectivement. On a alors la suite exacte courte fondamentale de la théorie de Galois

$$1 \to \pi_{k,\mathbf{t}}^{\text{tame,alg}} \to \pi_{k,\mathbf{t}}^{\text{tame,ar}} \to \Gamma_k \to 1$$

et chaque point k-rationnel $t_0 \in \mathbb{P}^1(k)$ en définit un scindage $s_{t_0} : \Gamma_k \to \pi_{k,\mathbf{t}}^{\text{tame,ar}}$. Le paragraphe 1.1.1.3 donne une description précise de $\pi_{k,\mathbf{t}}^{\text{tame,alg}}$. On peut aussi décrire partiellement l'action de Γ_k sur $\pi_{k,\mathbf{t}}^{\text{tame,alg}}$. Pour cela, introduisons la notion de présentation Galois-compatible de $\pi_{k,\mathbf{t}}^{\text{tame,alg}}$. Une présentation $\rho : \widehat{F_{r-1}} \to \pi_{k,\mathbf{t}}^{\text{tame,alg}}$ de $\pi_{k,\mathbf{t}}^{\text{tame,alg}}$ est dite Galois-compatible si
(i) $\rho(\Gamma_i)$ engendre un groupe d'inertie $I(Q_{t_i}|P_{t_i})$ au-dessus de t_i, $i = 1, ..., r$.
(ii) Via l'isomorphisme canonique $\phi_{t_i} I(Q_{t_i}|P_{t_i}) \to \widehat{\mathbb{Z}}(1) := \varprojlim_{n \geq 1} \mu_n$ (défini par passage à la limite projective des isomorphismes du paragraphe 1.1.1.2) on demande que $\phi_{t_i}(\rho(\Gamma_i)) = \phi_{t_j}(\rho(\Gamma_j))$, $1 \leq i \neq j \leq r$.

Les présentations induites via les isomorphismes de groupes fondamentaux ci-dessus par les présentation $\rho_{\underline{\gamma}}$ associées à des bouquets topologiques sont Galois-compatibles. Une présentation $\rho : \widehat{F_{r-1}} \to \pi_{k,\mathbf{t}}^{\text{tame,alg}}$ Galois-compatible étant fixé, l'action de Γ_k sur $\pi_{k,\mathbf{t}}^{\text{tame,alg}}$ a la propriété suivante :

Lemma 1.6 (Branch cycle agument) *Pour tout $\sigma \in \Gamma_k$, ${}^{s(\sigma)}\gamma_i$ est conjugué à $\gamma_{\pi(\sigma)(i)}^{\chi(\sigma)}$, $i = 1, ..., r$, où $\chi : \Gamma_k \to \widehat{\mathbb{Z}}^\star$ est le caractère cyclotomique de k et $\pi(\sigma) \in \mathcal{S}_r$ la permutation induite par σ sur $\mathbf{t} = \{t_1, ..., t_r\}$.*

1.1.2 Corps des modules et corps de définition

On garde les hypothèse du paragraphe 1.1.1.4. Soit $(f : X \to \mathbb{P}^1_{k^s}, \alpha)$ un k^s-G-revêtement d'invariants G, $\mathbf{t}$, $\mathbf{C}$ correspondant à un épimorphisme de groupes $\Phi_{(f,\alpha)} : \pi_{k,\mathbf{t}}^{\text{tame,alg}} \twoheadrightarrow G$.

1. On dira que k est un corps de définition de (f, α) si l'une des deux conditions équivalentes suivante est remplies :
   (i) (f, α) admet un k-modèle *i.e.* il existe un k-G-revêtement (f_k, α_k) d'invariants G, $\mathbf{t}$, $\mathbf{C}$ tel que $(f, \alpha) = i^\star(f_k, \alpha_k)$.
   (ii) $\Phi_{(f,\alpha)} : \pi_{k,\mathbf{t}}^{\text{tame,alg}} \twoheadrightarrow G$ s'étend en un épimorphisme $\Phi_{(f,\alpha),k} : \pi_{k,\mathbf{t}}^{\text{tame,ar}} \twoheadrightarrow G$.
2. On dira que k est un corps des modules de (f, α) si l'une des deux conditions équivalentes suivante est remplie :
   (i) $k = (k^s)^{M_k((f,\alpha))}$ où $M_k((f, \alpha)) = \{\sigma \in \Gamma_k \mid (f, \alpha) \sim \sigma^\star(f, \alpha)\} <_f \Gamma_k$ est le sous-groupe (fermé, d'indice fini) de Γ_k fixant la classe d'isomorphisme de (f, α).
   (ii) Il existe une application $h^s_{k,(f,\alpha)} : \Gamma_k \to G$ telle que $\Phi_{(f,\alpha)}({}^{s(\sigma)}\gamma) = h^s_{k,(f,\alpha)}(\sigma)\Phi_{(f,\alpha)}(\gamma)(h^s_{k,(f,\alpha)}(\sigma))^{-1}$, $\gamma \in \pi_{k,\mathbf{t}}^{\text{tame,alg}}$.
   Plus généralement, on dira que $(k^s)^{M_k((f,\alpha))}$ est *le* corps des modules de (f, α) *relativement à* k et on le notera $k_{m,(f,\alpha)}$. Si $k = Q(\mathbf{t})$ est le corps de définition du diviseur $\mathbf{t}$ (ici, $Q \hookrightarrow k$ est le sous-corps premier de k) on dira seulement que $k_{m,(f,\alpha)}$ est *le* corps des modules de (f, α).

L'extension $k_{m,(f,\alpha)}/k$ est finie (de degré $\leq |\overline{\text{ni}}_r(G)|$ par le branch cycle argument) et contenue dans tout corps de définition de (f, α) mais la réciproque est fausse en général ; plus précisément, $k_{m,(f,\alpha)}$ est l'intersection des corps de définition de (f, α) donc, (f, α) admet un plus petit corps de définition si et seulement si (f, α) est définie sur $k_{m,(f,\alpha)}$, [CoH85], prop. 2.7. On peut donner une mesure cohomologique $[\omega_{(f,\alpha)}] \in H^2(k_{m,(f,\alpha)}, Z(G))$ à ce que le corps des modules soit un corps de définition. Pour

simplifier, supposons que $k = k_{m,(f,\alpha)}$. L'obstruction à ce que $k_{m,(f,\alpha)}$ soit un corps de d'efinition de (f,α) est l'obstruction à pouvoir choisir un morphisme de groupe pour $h^s_{k,(f,\alpha)}$; considèrons donc l'application $\overline{\phi}^s_{k,(f,\alpha)} : \begin{array}{ccc} \Gamma_k & \to & G/Z(G) \\ \sigma & \to & h^s_{k,(f,\alpha)}(\sigma)[\text{mod Z}(G)] \end{array}$, qui est un morphisme de groupes bien défini, ne dépendant que de s et pas de $h^s_{k,(f,\alpha)}$. En munissant $Z(G)$ de sa structure de Γ_k module trivial, soit la cochaine

$$\omega_{(f,\alpha)} : \begin{array}{ccc} \Gamma_k \times \Gamma_k & \to & Z(G) \\ (\sigma,\tau) & \to & (h^s_{k,(f,\alpha)}(\sigma\tau))^{-1} h^s_{k,(f,\alpha)}(\sigma) h^s_{k,(f,\alpha)}(\tau) \end{array}$$

qui définit $[\omega_{(f,\alpha)}] \in H^2(k, Z(G))$. Alors, $[\omega_{(f,\alpha)}] \in H^2(k, Z(G))$ ne dépend pas de la section $s : \Gamma_k \hookrightarrow \pi^{\text{tame ar}}_{k,\mathbf{t}}$ et $[\omega_{(f,\alpha)}]$ est nul dans $H^2(k, Z(G))$ si et seulement k est un corps de définition de (f,α) ou, de fçon équivalente, si et seulement si il existe un morphisme $\overline{\phi}^s_{k,(f,\alpha)} : \Gamma_k \to G$ rendant le diagramme suivant commutatif

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z(G) & \longrightarrow & G & \longrightarrow & G/Z(G) & \longrightarrow & 1 \\ & & & & & \swarrow^{\exists \phi^s_{k,(f,\alpha)}} & \uparrow{\scriptstyle \overline{\phi}^s_{k,(f,\alpha)}} & & \\ & & & & & & \Gamma_k & & \end{array}$$

C'est en particulier le cas si $Z(G) = \{1\}$ ou si $Z(G)$ est un facteur direct de G.

1.2 Espaces de modules pour la catégorie des G-revêtements

1.2.1 Groupes de tresses

Les espaces de modules pour les G-revêtements sont naturellement présentés comme des revêtements topologiques des espaces de configurations $\mathcal{U}^r(\mathbb{C}) = \{\mathbf{t}' = (t_1, ..., t_r) \in \mathbb{P}^1(\mathbb{C}) \mid t_i \neq t_j,\ 1 \leq i \neq j \leq r\}$ et $\mathcal{U}_r(\mathbb{C}) = \mathcal{U}^r(\mathbb{C})/\mathcal{S}_r = \{\mathbf{t} \subset \mathbb{P}^1(\mathbb{C}) \mid |\mathbf{t}| = r\}$. Nous rappelons ici les résultats sur les groupes fondamentaux de $\mathcal{U}^r(\mathbb{C})$ et $\mathcal{U}_r(\mathbb{C})$ que nous utiliserons en 1.2.2.1 ; pour les preuves, nous renvoyons à [FV91], [V99] et [Ri04] p. 21-33, dont nous synthétisons ici les résultats. Notons $\sigma_r : \mathcal{U}^r(\mathbb{C}) \to \mathcal{U}_r(\mathbb{C})$ la projection canonique, qui est un revêtement topologique galoisien de groupe $\mathcal{S}_r$.

Pour tout $\mathbf{t}' = (t_1, ..., t_r) \in \mathcal{U}^r(\mathbb{C})$, notons $\mathbf{t} = \sigma_r(\mathbf{t}')$ et fixons un chemin continu fermé injectif $c : [0,1] \to \mathbb{P}^1(\mathbb{C})$ tel que $c(u_k) = t_k$, $k = 1, ..., r$ avec $0 < u_1 < ... < u_r < 1$; la courbe $c([0,1])$ sépare $\mathbb{P}^1(\mathbb{C})$ en deux composantes connexes que l'on note $\mathcal{C}_1$ (la composante à droite de c) et $\mathcal{C}_2$ (la composante à gauche de c). On peut alors construire un $r-1$-uplet de chemins continus fermés injectifs $(c_k : [0,1] \to \mathbb{P}^1(\mathbb{C}))_{1 \leq k \leq r-1}$ tels que (i) $c_k(0) = c_k(1) = t_k$ et $c_k(1/2) = t_{k+1}$, (ii) $c_k(]0,1/2[) \subset C_2$ et $c_k(]1/2,1[) \subset C_1$ et (iii) la courbe $c_k([0,1])$ sépare $\mathbb{P}^1(\mathbb{C})$ en deux composantes connexes que l'on note $\mathcal{C}_{k,1}$ (la composante à droite de c_k) et $\mathcal{C}_{k,2}$ (la composante à gauche de c_k) vérifiant $c(]u_k, u_{k+1}[) \subset \mathcal{C}_{k,1}$ et $\cup_{1 \leq l \neq k \leq r} c_l([0,1]) \setminus \{t_k, t_{k+1}\} \subset \mathcal{C}_{k,2}$, $k = 1, ..., r-1$. On peut ainsi définir les tresses topologiqes standard $q_k : \begin{array}{ccc} [0,1] & \to & \mathcal{U}^r(\mathbb{C}) \\ u & \to & (t_1, ..., t_{k-1}, c_k(u/2), c_k(1-u/2), t_{k+2}, ..., t_r) \end{array}$, $k = 1, ..., r-1$.

Par ailleurs, notons H_r le groupe de tresses de Hurwitz *i.e.* le groupe défini par les générateurs $Q_1, ..., Q_{r-1}$ et les relations (1) $Q_i Q_{i+1} Q_i = Q_{i+1} Q_i Q_{i+1}$, $i = 1, ..., r-2$. (2) $Q_i Q_j = Q_j Q_i$, $i, j = 1, ..., r-1$ avec $|i-j| > 1$. (3) $Q_1 \cdots Q_{r-1} Q_{r-1} \cdots Q_1 = 1$.

et SH_r le groupe de tresses pures de Hurwitz *i.e.* le noyau du morphisme de groupes $H_r \to \mathcal{S}_r$, $Q_i \to (i, i+1)$. En notant SH^0_r le groupe défini par les générateurs $A_{i,j}$, $1 \leq i < j \leq r$ et les relations

$$A^{-1}_{r,s} A_{i,j} A_{r,s} = \begin{array}{ll} A_{i,j} & , r < s < i < j \text{ ou } i < r < s < j. \\ A_{r,j} A_{i,j} A^{-1}_{r,j} & , r < s = i < j. \\ A_{r,j} A_{s,j} A_{i,j} A^{-1}_{s,j} A^{-1}_{r,j} & , r = i < s < j. \\ A_{r,j} A_{s,j} A^{-1}_{r,j} A^{-1}_{s,j} A_{i,j} A_{s,j} A_{r,j} A^{-1}_{s,j} A^{-1}_{r,j} & , r < i < s < j. \end{array}$$

, l'application $A_{1,2} \cdots A_{1,r} = 1$

cation $SH_r^0 \to SH_r$, $A_{i,j} \to Q_i \cdots Q_{j-2} Q_{j-1}^{-2} Q_{j-2}^{-1} \cdots Q_i^{-1}$ est une présentation de SH_r (*cf.* [Bi74], lemme 1.8.2 avec correction des relations dans [H87], appendice 2). Finalement, on peut énoncer le classique :

Theorem 1.7 (Fadell et Van Buskirk) *Les applications*

$$u_r : \begin{array}{ccc} H_r & \to & \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) \\ Q_i & \to & [\sigma_r \circ q_i] \end{array} \quad \text{et} \quad v_r : \begin{array}{ccc} SH_r^0 & \to & \pi_1^{\mathrm{top}}(\mathcal{U}^r(\mathbb{C}), \mathbf{t}') \\ A_{i,j} & \to & [q_i \cdots q_{j-2} q_{j-1}^{-2} q_{j-2}^{-1} \cdots q_i^{-1}] \end{array}$$

sont des isomorphismes de groupes.

Nous aurons aussi besoin de définir les actions de tresses $T_{r,\mathbf{t}'}$ et $T_{r,\mathbf{t}}$ et de les expliciter. Notons $\mathcal{B}_0$ le groupe topologique des homéomorphismes continus de $\mathbb{P}^1(\mathbb{C})$ préservant l'orientation canonique muni de la topologie compact-ouvert et considèrons les fibrations localement triviales $\epsilon_{r,\mathbf{t}'} : \begin{array}{ccc} \mathcal{B}_0 & \to & \mathcal{U}^r(\mathbb{C}) \\ h & \to & (h(t_1), ..., h(t_r)) \end{array}$ et $\epsilon_{r,\mathbf{t}} = \sigma_r \circ \epsilon_{r,\mathbf{t}'}$. Comme $\pi_0(\mathcal{B}_0) = \{1\}$, les connexions d'indice 0 des suites exactes longues d'homotopie associées à ces fibrations permettent de définir deux antiépimorphismes de groupes :

$$\delta_{r,\mathbf{t}'} : \begin{array}{ccc} \pi_1^{\mathrm{top}}(\mathcal{U}^r(\mathbb{C}), \mathbf{t}') & \to & \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t}')) \\ [a] & \to & [\overline{a}(1)] \end{array} \quad \text{et} \quad \delta_{r,\mathbf{t}} : \begin{array}{ccc} \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) & \to & \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})) \\ [q] & \to & [\overline{q}(1)] \end{array}$$

où $\overline{a} : [0,1] \to \mathcal{B}_0$ (resp. $\overline{q} : [0,1] \to \mathcal{B}_0$) est l'unique application continue telle que $\epsilon_{r,\mathbf{t}'} \circ \overline{a} = a$ et $\overline{a}(0) = \mathrm{Id}$ (resp. $\epsilon_{r,\mathbf{t}} \circ \overline{q} = q$ et $\overline{q}(0) = \mathrm{Id}$). On appelle alors action de tresses pures (resp. de tresses) le morphisme de groupes $T_{r,\mathbf{t}'} = \Lambda_{r,\mathbf{t}'} \circ \delta_{r,\mathbf{t}'}$ (resp. $T_{r,\mathbf{t}} = \Lambda_{r,\mathbf{t}} \circ \delta_{r,\mathbf{t}}$) avec $\Lambda_{r,\mathbf{t}'} : \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})) \to \mathrm{Out}(\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \backslash \mathbf{t}, t_0))$, l'application qui à $[h]$ associe la classe $[c] \to [\gamma_{h,t_0}][h \circ c][\gamma_{h,t_0}]^{-1}$ (où $\gamma_{h,t_0} : [0,1] \to \mathbb{P}^1(\mathbb{C})$ est un chemin continu joignant t_0 et $h(t_0)$) (resp. $\Lambda_{r,\mathbf{t}}$ *etc*).

Construisons pour terminer un bouquet topologique $\underline{\gamma} = (\gamma_1, ..., \gamma_r)$ pour $\mathbb{P}^1(\mathbb{C}) \backslash \mathbf{t}$ basé en $t_0 = c(0)$ comme suit : (i) $\gamma_k = \alpha_k \beta_k \alpha_k^{-1}$ où β_k est un chemin fermé continu injectif tournant une fois (dans le même sens que c_k) autour de t_k, (ii) α_k est un chemin continu injectif joignant t_0 à un point de β_k et tel que $\alpha_k(]0,1[) \subset \mathcal{C}_2 \setminus \cup_{1 \leq l \leq r} \mathcal{C}_{l,1}$, (iii) les $(\alpha_k)_{1 \leq k \leq r}$ ne se coupent qu'en t_0 et sont ordonnés de sorte que $\gamma_1 \cdots \gamma_r = 1$. Avec ces notations,on peut décrire explicitement les actions de tresses :

Theorem 1.8 (Actions de tresses) *On a* $T_{r,\mathbf{t}}(Q_i)(\underline{\gamma}) = (\gamma_1, ..., \gamma_{i-1}, \gamma_{i+1}^{\gamma_i}, \gamma_i, \gamma_{i+2}, ..., \gamma_r)$, $i = 1, ..., r-1$ *et le diagramme commutatif*

$$\begin{array}{ccc} \pi_1^{\mathrm{top}}(\mathcal{U}^r(\mathbb{C}), \mathbf{t}') & \hookrightarrow & \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) \\ & \searrow^{T_{r,\mathbf{t}'}} & \downarrow T_{r,\mathbf{t}} \\ & & \mathrm{Out}(\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0)) \end{array} .$$

1.2.2 Espaces de Hurwitz

Soit G un groupe fini et $r \geq 3$ un entier. Nous rappelons dans cette partie les principales propriétés des espaces de modules classifiant les G-revêtements de groupe G avec r points de branchement. Il existe différentes constructions de ces espaces de modules et nous renvoyons par exemple à [E01] ou [RoW04] pour des exposés de synthèse sur ce sujet. Nous présentons brièvement deux d'entre elles. La première [FV91], [V99], "à la main", décrit les structures topologiques, analytique et algébriques de ces espaces ; la seconde [W98], basée sur la théorie des champs algébriques, permet de donner une compactification naturelle de ces espaces de modules.

1.2.2.1 1ère construction

Posons

$$\mathcal{H}_{r,G} = \coprod_{\mathbf{t} \in \mathcal{U}_r(\mathbb{C})} \mathcal{R}_{\mathbf{t},G,\mathbb{C}}^{\mathrm{alg}} / \sim \quad \text{et} \quad \Psi_{r,G} : \begin{array}{ccc} \mathcal{H}_{r,G} & \to & \mathcal{U}_r(\mathbb{C}) \\ (\mathbf{t}, (f, \alpha)) & \to & \mathbf{t} \end{array}$$

On peut alors munir $\mathcal{H}_{r,G}$ d'une topologie $\mathcal{T}$ qui fasse de $\Psi_{r,G}$ un revêtement topologique. Pour cela, définissons une base de voisinage d'un point $(f,\alpha) \in \mathcal{R}^{\text{alg}}_{\mathbf{t},G,\mathbb{C}}/\sim$. A $\mathbf{t} = \{t_1,...,t_r\} \in \mathcal{U}_r(\mathbb{C})$ on peut associer la base de voisinages $(\mathcal{U}(\underline{D}) = \{\mathbf{t}_0 \in \mathcal{U}_r(\mathbb{C} \mid |\mathbf{t}_0 \cap D_i| = 1,\ i = 1,...,r)\})_{\underline{D}=(D_1,...,D_r)\in\mathcal{D}_\mathbf{t}}$, où $\mathcal{D}_\mathbf{t}$ est l'ensemble des r-uplets $\underline{D} = (D_1,...,D_r)$ de disques ouverts D_i centrés en t_i et deux à deux disjoints. Pour tout $\underline{D} = (D_1,...,D_r) \in \mathcal{D}_\mathbf{t}$ et tout $\mathbf{t} \in \mathcal{T}(\underline{D})$ on a alors des isomorphismes canoniques induits par l'inclusion

$$\pi_1^{\text{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}) \xrightarrow{\quad can \quad} \pi_1^{\text{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \cup_{1\leq i\leq r} D_i) \longrightarrow \pi_1^{\text{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}_0)$$

ce qui permet de poser

$$\mathcal{T}(\underline{D},(f,\alpha)) = \coprod_{\mathbf{t}_0\in\mathcal{U}(\underline{D})} \{(f_0,\alpha_0) \in \mathcal{R}^{\text{alg}}_{\mathbf{t}_0,G,\mathbb{C}}/\sim \mid \Phi_{(f_0,\alpha_0)} \sim \Phi_{(f,\alpha)} \circ can\}$$

et la topologie $\mathcal{T}$ sur $\mathcal{H}_{r,G}$ est celle définie par les bases de voisinages de la forme $(\mathcal{T}(\underline{D},(f,\alpha)))_{\underline{D}\in\mathcal{D}_\mathbf{t}}$.

On dispose donc maintenant d'un revêtement fini d'espace topologique et du revêtement topologique produit fibré défini par le carré cartésien :

$$\begin{array}{ccc} \mathcal{H}'_{r,G} & \xrightarrow{\Sigma_r} & \mathcal{H}_{r,G} \\ \downarrow{\scriptstyle \Psi'_{r,G}} & \square & \downarrow{\scriptstyle \Psi_{r,G}} \\ \mathcal{U}^r(\mathbb{C}) & \xrightarrow[\sigma_r]{} & \mathcal{U}_r(\mathbb{C}) \end{array}$$

Par la théorie des revêtements topologiques finis, on peut décrire les classes d'isomorphismes de ces revêtements en termes d'action des groupes fondamentaux $\pi_1^{\text{top}}(\mathcal{U}^r(\mathbb{C}),\mathbf{t}')$ et $\pi_1^{\text{top}}(\mathcal{U}_r(\mathbb{C}),\mathbf{t})$. Reprenons les notations du 1.2.1 : pour tout $\mathbf{t}' = (t_1,...,t_r) \in \mathcal{U}^r(\mathbb{C})$ d'image $\mathbf{t} = \sigma_r(\mathbf{t}')$ on a construit un bouquet topologique $\underline{\gamma} = (\gamma_1,...,\gamma_r)$ permettant de décrire explicitement les actions de tresses. Par ailleurs, on dispose d'une part de l'application de monodromie :

$$\mathrm{M}_{\Psi_{r,G}} : \pi_1^{\text{top}}(\mathcal{U}_r(\mathbb{C}),\mathbf{t}) \to \mathrm{Perm}(\Psi_{r,G}^{-1}(\mathbf{t}))$$

et d'autre part de l'application de composition :

$$\begin{array}{rccc} \mathrm{C}_{\Psi_{r,G}} : & \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})) & \to & \mathrm{Perm}(\Psi_{r,G}^{-1}(\mathbf{t})) \\ & [h] & \to & (f,\alpha) \to (h\circ f,\alpha) \end{array}$$

Notons $BCD_{\underline{\gamma}}$ (pour branch cycle description) l'isomorphisme $(\Psi_{r,G,\mathbb{C}})^{-1}(\mathbf{t}) \simeq \overline{\mathrm{ni}}_r(G)$ induit par la monodromie ; cette isomorphisme ne dépend en fait que de la classe d'équivalence de $\underline{\gamma}$ dans l'ensemble $\mathrm{Top}(\mathbf{t})$ des bouquets topologiques pour $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ muni de $\sim$ défini par : pour tout $\underline{\gamma}_i \in \mathrm{Top}(\mathbf{t})$ basé en $t_{0,i} \notin \mathbf{t}$, $i = 1,2$, $\underline{\gamma}_1 \sim \underline{\gamma}_2$ s'il existe un chemin continu $\lambda : [0,1] \to \mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ joignant $t_{0,1}$ à $t_{0,2}$ tel que $\underline{\gamma}_2 = \lambda \cdot \underline{\gamma}_1 \cdot \lambda^{-1}$. En particulier, l'action de tresses $\Lambda_{r,\mathbf{t}}$ définit une action

$$\begin{array}{rcl} \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})) \times \mathrm{Top}_\mathbf{t}/\sim & \to & \mathrm{Top}_\mathbf{t}/\sim \\ ([f],\underline{\gamma}) & \to & [f] \star \underline{\gamma} := (f\circ\gamma_1,...,f\circ\gamma_r) \end{array}$$

Theorem 1.9 (description combinatoire de $\Psi_{r,G}$ et $\Psi_{r,G}$) *Le diagramme*

$$\begin{array}{ccc} \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})) & \xrightarrow{\mathrm{C}_{\Psi_{r,G}}} & \mathrm{Perm}(\Psi_{r,G}^{-1}(\mathbf{t})) \\ \uparrow{\scriptstyle \delta_{r,\mathbf{t}}} & \nearrow{\scriptstyle \mathrm{M}_{\Psi_{r,G}}} & \\ \pi_1^{\text{top}}(\mathcal{U}_r(\mathbb{C}),\mathbf{t}) & & \end{array}$$

commute. Par ailleurs, pour tout $[f] \in \mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})$, *on a* $BCD_{\underline{\gamma}} \circ \mathrm{C}_{\Psi_{r,G}}([f]) = BCD_{[f^{-1}]\star\underline{\gamma}}$. *On en déduit que pour tout* $\mathbf{g} = (g_1, ..., g_r) \in \overline{\mathrm{ni}}_r(G)$,

$$BCD_{\underline{\gamma}}(\mathrm{M}_{\Psi_{r,G}}(Q_i)(BCD_{\underline{\gamma}}^{-1}(\mathbf{g}))) = (g_1, ..., g_{i-1}, g_{i+1}^{g_i}, g_i, g_{i+2}, ..., g_r),\ i = 1, ..., r-1$$

De même, l'action des $A_{i,j}$, $1 \leq i < j \leq r$ *sur* $\overline{\mathrm{ni}}_r(G)$ *se déduit de celle des* Q_i, $i = 1, ..., r-1$ *sur* $\overline{\mathrm{ni}}_r(G)$.

L'étape suivante consiste à montrer que les objets topologiques définis ci-dessus sont en fait munis de structures algébriques :

1. $\mathcal{U}_r$ possède une structure naturelle de variété analytique $\mathcal{U}_r^{\mathrm{an}}$ donc $\mathcal{H}_{r,G}$ hérite d'une unique structure de variété analytique $\mathcal{H}_{r,G}^{\mathrm{an}}$ qui fasse de $\Psi_{r,G}$ un revêtement $\Psi_{r,G}^{\mathrm{an}} : \mathcal{H}_{r,G}^{\mathrm{an}} \to \mathcal{U}_r^{\mathrm{an}}$ de variétés analytiques.
2. D'après le théorème de Grauert-Rummert, on peut compléter $\Psi_{r,G}^{\mathrm{an}}$ en un revêtement $\overline{\Psi}_{r,G}^{\mathrm{an}} : \overline{\mathcal{H}}_{r,G}^{\mathrm{an}} \to \overline{\mathcal{U}}_r^{\mathrm{an}}$ de variétés analytiques compactes.
3. Par des théorèmes de type G.A.G.A., $\overline{\Psi}_{r,G}^{\mathrm{an}} : \overline{\mathcal{H}}_{r,G}^{\mathrm{an}} \to \overline{\mathcal{U}}_r^{\mathrm{an}}$ possède une unique structure de revêtement de variétés algébriques complexes $\overline{\Psi}_{r,G}^{\mathrm{alg}} : \overline{\mathcal{H}}_{r,G}^{\mathrm{alg}} \to \overline{\mathcal{U}}_r^{\mathrm{alg}}$. En faisant le produit fibré de $\overline{\Psi}_{r,G}^{\mathrm{alg}}$ par $\mathcal{U}_{r,\mathbb{C}} \hookrightarrow \overline{\mathcal{U}}_r^{\mathrm{alg}}$, on obtient la structure de variété algébrique complexe $\Psi_{r,G,\mathbb{C}} : \mathcal{H}_{r,G,\mathbb{C}}^{\mathrm{alg}} \to \mathcal{U}_{r,\mathbb{C}}$ de $\Psi_{r,G}^{\mathrm{an}}$.
4. la descente de $\mathbb{C}$ à $\mathbb{Q}$ s'effectue en deux étapes. Le théorème de descente de Serre [S92], théorème 6.7 permet de descendre de $\mathbb{C}$ à $\overline{\mathbb{Q}}$ puis une application - non triviale - du critère de descente de Weil [We] permet de descendre de $\overline{\mathbb{Q}}$ à $\mathbb{Q}$ et de décrire l'action de $\Gamma_{\mathbb{Q}}$.

Finalement :

Theorem 1.10 ([FV91]) $\Psi_{r,G} : \mathcal{H}_{r,G} \to \mathcal{U}_r(\mathbb{C})$ *possède une unique structure* $\Psi_{r,G,\mathbb{Q}} : \mathcal{H}_{r,G,\mathbb{Q}} \to \mathcal{U}_{r,\mathbb{Q}}$ *de revêtement étale de variétés algébriques défini sur* $\mathbb{Q}$ *et compatible avec sa structure de revêtement de variétés analytiques. De plus*
- les composantes géométriquement irréductibles de $\mathcal{H}_{r,G,\mathbb{Q}}$ *sont en correspondance bijectives avec les composantes connexes de* $\mathcal{H}_{r,G}$.
- pour tout $\mathbf{p} \in \mathcal{H}_{r,G,\mathbb{Q}}(\mathbb{C})$ *correspondant à un G-revêtement* (f, α) *de points de branchement* $\mathbf{t} \in \mathcal{U}_r(\mathbb{C})$ *avec* $k = \mathbb{Q}(\mathbf{t})$, $\mathbf{p} \in \mathcal{H}_{r,G,\mathbb{Q}}(\overline{k})$ *et pour tout* $\sigma \in \Gamma_k$, ${}^{\sigma}\mathbf{p}$ *correspond au G-revêtement conjugué* $\sigma^{\star}(f, \alpha)$ *donc* $\mathbf{p} \in \mathcal{H}_{r,G,\mathbb{Q}}(k_{m,(f,\alpha)})$.

On a un énoncé similaire pour $\Psi'_{r,G} : \mathcal{H}'_{r,G} \to \mathcal{U}^r(\mathbb{C})$.

Terminons ce paragraphe en rappelant la définition des espaces de Hurwitz proprement dits. Pour tout $\mathbf{C} \in \mathcal{C}_r(G)$ soit $\mathrm{ni}(\mathbf{C})$ le sous-ensemble de $\mathrm{ni}_r(G)$ des r-uplets $\mathbf{g} = (g_1, ..., g_r) \in \mathrm{ni}_r(G)$ tels que (3) $g_i \in C_{\sigma(i)}$, $i = 1, ..., r$ pour une permutation $\sigma \in \mathcal{S}_r$ et $\mathrm{sni}(\mathbf{C})$ le sous-ensemble de $\mathrm{ni}_r(G)$ des r-uplets $\mathbf{g} = (g_1, ..., g_r) \in \mathrm{ni}_r(G)$ tels que (3)' $g_i \in C_i$, $i = 1, ..., r$. On notera $\overline{\mathrm{ni}}(\mathbf{C})$ et $\overline{\mathrm{sni}}(\mathbf{C})$ les ensembles quotient correspondants modulo l'action composantes par composantes de $\mathrm{Inn}(G)$. Comme $H_r.\mathrm{ni}(\mathbf{C}) = \mathrm{ni}(\mathbf{C})$, $\mathrm{ni}(\mathbf{C})$ correspond à une réunion $\mathcal{H}_{r,G}(\mathbf{C})$ de composantes géométriquement irréductibles de $\mathcal{H}_{r,G,\mathbb{Q}}$ qu'on appelle l'espace de Hurwitz associé à $\mathbf{C}$ et qui paramétrise les classes d'isomorphismes de G-revêtements d'invariant canonique de l'inertie $\mathbf{C}$. Autrement dit, si on note l'action naturelle du groupe symétrique $\mathcal{S}_r$ sur $\mathcal{C}_r(G)$ par $\begin{array}{ccc} \mathcal{S}_r \times \mathcal{C}_r(G) & \to & \mathcal{C}_r(G) \\ (\sigma, \mathbf{C} = (C_1, ..., C_r)) & \to & {}^{\sigma}\mathbf{C} = (C_{\sigma(1)}, ..., C_{\sigma(r)}) \end{array}$ on obtient $\mathcal{H}_{r,G,\overline{\mathbb{Q}}} = \coprod_{\mathbf{C} \in \mathcal{C}_r(G)/\mathcal{S}_r} \mathcal{H}_{r,G}(\mathbf{C})$. On peut aussi définir un espaces de Hurwitz dessymmétrisé $\mathcal{H}'_{r,G}(\mathbf{C})$. Un point du produit fibré $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$ correspond à un G-revêtement (f, α) donné avec un ordre $\mathbf{t}' = (t_1, ..., t_r)$ de ses points de branchement, ce qui permet de définir une application de monodromie :

$$\begin{array}{rccc} \mathrm{M} : & \mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r & \to & \{C_1, ..., C_r\}^r \\ & (h, (t_1, ..., t_r)) & \to & (C_{t_1}, ..., C_{t_r}) \end{array}$$

qui, étant continue, est constante sur chacune des composantes connexes de $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$. En particulier, $M^{-1}(\mathbf{C})$ est une réunion de composantes connexes de $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$; c'est cette variété que l'on notera $\mathcal{H}'_{r,G}(\mathbb{C})$. On a toujours un carré cartésien

$$\begin{array}{ccc} \mathcal{H}'_{r,G}(\mathbf{C}) & \xrightarrow{\Sigma_r} & \mathcal{H}_{r,G}(\mathbf{C}) \\ \downarrow{\scriptstyle \psi'_{r,G}} & \square & \downarrow{\scriptstyle \psi_{r,G}} \\ \mathcal{U}^r & \xrightarrow{\sigma_r} & \mathcal{U}_r \end{array}$$

Et, en fait, $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r = \coprod_{\sigma \in \mathcal{S}_r/\mathrm{Stab}_{\mathcal{S}_r}(\mathbf{C})} \mathcal{H}'_{r,G}({}^{\sigma}\mathbf{C})$. Enfin, le deuxième point du théorème 1.10 combiné au "branch cycle argument" décrit l'action de $\Gamma_{\mathbb{Q}}$ sur les espaces de Hurwitz : Pour tout $\sigma \in \Gamma_k$, ${}^{\sigma}\mathcal{H}_{r,G}(\mathbf{C}) = \mathcal{H}_{r,G}(\mathbf{C}^{\chi(\sigma)})$ et ${}^{\sigma}\mathcal{H}'_{r,G}(\mathbf{C}) = \mathcal{H}'_{r,G}(\mathbf{C}^{\chi(\sigma)})$. Donc, par le critère de descente de Weil, ces espaces sont définis sur des extensions cyclotomiques de $\mathbb{Q}$, que l'on notera $\mathbb{Q}_{\mathbf{C}}$ et $\mathbb{Q}'_{\mathbf{C}}$ respectivement. En particulier

- $\mathcal{H}_{r,G}(\mathbf{C})$ est défini sur $\mathbb{Q}$ si et seulement si $\mathbf{C}$ est une union rationnelle de classes de conjugaison (*i.e.* pour tout entier m premier à l'ordre des C_i, $i = 1, ..., r$, $\mathbf{C}^m = {}^{\sigma}\mathbf{C}$ pour une permutation $\sigma \in \mathcal{S}_r$).
- $\mathcal{H}'_{r,G}(\mathbf{C})$ est défini sur $\mathbb{Q}$ si et seulement si pour tout entier m premier à l'ordre des C_i, $i = 1, ..., r$, $\mathbf{C}^m = \mathbf{C}$.

1.2.2.2 2ème construction

La théorie des champs algébriques et de leur représentabilité donne un cadre plus formel pour construire et étudier les espaces de modules pour les G-revêtements ; elle permet notamment de les compactifier avec une interprétation modulaire du bord [W98]. Le principe consiste à construire des diagrammes commutatifs de catégories fibrées

$$\begin{array}{ccc} H_{r,G} & \hookrightarrow & \overline{H}_{r,G} \\ \downarrow{\scriptstyle \Psi_{r,G}} & & \downarrow{\scriptstyle \overline{\Psi}_{r,G}} \\ U_r & \hookrightarrow & \overline{U}_r \end{array} \quad \text{et} \quad \begin{array}{ccc} H'_{r,G} & \hookrightarrow & \overline{H}'_{r,G} \\ \downarrow{\scriptstyle \Psi'_{r,G}} & & \downarrow{\scriptstyle \overline{\Psi}'_{r,G}} \\ U^r & \hookrightarrow & \overline{U}^r \end{array}$$

puis de montrer que ces catégories fibrées sont en fait des champs algébriques admettant des espaces de modules grossiers.

(1) $\underline{U_r, U^r, \overline{U}_r, \overline{U}^r}$:

Pour tout schéma T, on appelle

- T-courbe r-marquée de genre 0 tout triplet $(x : X \to T, D, u)$ où $x : X \to T$ est un schéma propre et plat dont les fibres géométriques sont des courbes lisses de genre 0, $i_D : D \hookrightarrow X$ est un sous-schéma fermé tel que $x \circ i_D : D \to T$ est étale fini de degré constant r et $u : X \to \mathbb{P}^1_T$ est un T-isomorphisme.
- T-courbe r-pointée de genre 0 tout triplet $(x : X \to T, (s_i)_{1 \leq i \leq r}, u)$ où : $(s_i)_{1 \leq i \leq r}$ sont r sections de x telles que $s_i(T) \cap s_j(T) = \emptyset$, $1 \leq i \neq j \leq r$ et $(x : X \to T, \cup_{1 \leq i \leq r} s_i(T), u)$ est une T-courbe r-marquée de genre 0.

U_r (resp. U^r) désigne alors la catégorie fibrée des courbes r-marquées (resp. r-pointées) de genre 0. Ce sont des champs algébriques sur la catégorie des $\mathbb{Z}$-schémas ; U^r est représentable par le $\mathbb{Z}$-schéma $\mathcal{U}^r = \mathrm{spec}(\mathbb{Z}[T_1, ..., T_r]_{<\prod_{\leq i \neq j \leq r}(T_i - T_j)>})$ et U_r admet pour espace de modules grossiers le $\mathbb{Z}$-schéma $\mathcal{U}_r = \mathrm{spec}(\mathbb{Z}[T_1, ..., T_r]_{<\Delta_r>})$ (où $\Delta_r \in \mathbb{Z}[T_1, ..., T_r]$ est le polynome irréductible défini par $\prod_{\leq i \neq j \leq r}(X_i - X_j) = \Delta_r(\sigma_1(\underline{X}), ..., \sigma_r(\underline{X}))$).

Pour tout schéma T, on appelle T-courbe nodale genre 0 tout T-schéma $x : X \to T$ propre et plat dont les fibres géométriques sont des courbes de genre 0 n'ayant pour singularités éventuelles que des

points doubles ordinaires. On appelle

- T-courbe stable r-marquée de genre 0 tout couple $(x : X \to T, D)$ où : $x : X \to T$ est une T-courbe nodale genre 0, $i_D : D \hookrightarrow X^{lisse}$ est un sous-schéma fermé tel que $x \circ i_D : D \to T$ est étale fini de degré constant r et pour toute composante irréductible $C \hookrightarrow X$ on a $|C \cap (X^{sing} \cup supp(D))| \geq 3$.

- T-courbe stable r-pointée de genre 0 tout couple $(x : X \to T, (s_i)_{1 \leq i \leq r})$ où : $(s_i)_{1 \leq i \leq r}$ sont r sections de x telles que $s_i(T) \cap s_j(T) = \emptyset$, $1 \leq i \neq j \leq r$ et $(x : X \to T, \cup_{1 \leq i \leq r} s_i(T), u)$ est une T-courbe stable r-marquée de genre 0.

Lorsque les points marqués d'un objet de U_r (resp. U_r) coalescent, on peut les séparer par une série d'éclatements et obtenir ainsi des courbes stables r-marquées (resp. r-pointées). Pour garder trace dans cette déformation de la donnée u de l'isomorphisme initial entre X et $\mathbb{P}^1_T$, il faut adjoindre aux données d'une T-courbe stable r-marquée (resp. r-pointée) de genre 0 un cadre projectif $\lambda : X \to \mathbb{P}^1_T$ (*cf.* [W98] §2.3). On obtient ainsi $\overline{U}_r$ (resp. $\overline{U}^r$), la catégorie fibrée des courbes stabilisées r-marquées (rep. r-pointées) de genre 0. Ce sont des champs algébriques propres et lisses sur la catégories des $\mathbb{Z}$-schémas ; $\overline{U}^r$ est représentable par un $\mathbb{Z}$-schéma intègre, propre et lisse sur spec($\mathbb{Z}$), $\overline{\mathcal{U}}^r$, et $\overline{U}_r$ admet pour espace de modules grossiers un $\mathbb{Z}$-schéma intègre, propre et lisse sur spec($\mathbb{Z}$), $\overline{\mathcal{U}}^r$. On a de plus un carré cartésien de $\mathbb{Z}$-schémas où les flèches verticales sont des immersions ouvertes

$$\begin{array}{ccc} \mathcal{U}^r & \xrightarrow{\sigma_r} & \mathcal{U}_r \\ \downarrow & \square & \downarrow \\ \overline{\mathcal{U}}^r & \xrightarrow{\overline{\sigma}_r} & \overline{\mathcal{U}}_r \end{array}$$

(2) $\underline{H_{r,G},\ H'_{r,G},\ \overline{H}_{r,G},\ \overline{H}'_{r,G}}$:

Etant donnée une courbe stable r-marquée $(x : X \to T, D)$ (avec T connexe), on appelle G-revêtement admissible de $(x : X \to T, D)$ tout couple $(\rho : Y \to X, \alpha)$ où $\rho : Y \to X$ est un morphisme fini vérifiant : (i) la restriction $\rho|_{\rho^{-1}(X^{lisse})} : \rho^{-1}(X^{lisse}) \to X^{lisse}$ est ordinairement ramifiée le long de D, (ii) pour tout $y \in Y(k)$ point géométrique tel que $x_y := \rho \circ y \in X^{sing}(k)$, en notant $t_y := x \circ x_y \in T(k)$, on peut trouver pour tout système de coordonnées $(u, v) \in \tilde{\mathcal{O}}_{X,x_y}$ de X en x_y un couple $(r, s) \in \tilde{\mathcal{O}}_{Y,y}$, un entier $e \geq 1$ premier à la caractéristique de k et un élément $\tau \in \tilde{\mathcal{O}}_{T,t_y}$ tels que le morphisme de localisation étale induit par ρ, $\tilde{\mathcal{O}}_{X,x_y}[R, S]/ < R^e = u, S^e = v, RS = \tau > \to \tilde{\mathcal{O}}_{Y,y}$, $(R, S) \to (r, s)$, soit un isomorphisme. (Dans ce cas, $(x \circ \rho : Y \to T, \rho^{-1}(D))$ est une courbe stable r-marquée de genre 0 et $(r, s) \in \tilde{\mathcal{O}}_{Y,y}$ un système de coordonnées de Y en y), (iii) Les fibres géométriques de ρ sont des revêtements galoisiens de groupe de Galois isomorphe à G et $\alpha : \mathrm{Aut}(\rho) \to G$ est un isomorphisme de groupes. Quand $(x : X \to T, D)$ est en fait une courbe r-marquée de genre 0, on retrouve la notion usuelle de G-revêtement ordinairement ramifié au dessus de D.

H_r désigne alors la catégorie fibrée des G-revêtements admissibles de courbe r-marquée de genre 0 (*i.e.* des G-revêtements ordinairement ramifiés avec r points de branchement) et $\overline{H}_{r,G}$ celle des G-revêtements admissibles de courbes stables r-marquées de genre 0. On dispose de foncteurs naturels "points de branchement", $\Psi_{r,G} : H_{r,G} \to U_{r,G}$ et $\overline{\Psi}_{r,G} : \overline{H}_{r,G} \to \overline{U}_{r,G}$. Et

Theorem 1.11 (Compactification des espaces de modules pour les G-revêtements) *$\overline{H}_{r,G}$ est un champs algébrique qui admet pour espace de modules grossier un $\mathbb{Z}[\frac{1}{|G|}]$-schéma intègre, propre et lisse, $\overline{\mathcal{H}}_{r,G}$ muni d'un morphisme naturel $\overline{\Psi}_{r,G} : \overline{\mathcal{H}}_{r,G} \to \overline{\mathcal{U}}_{r,G}$ qui est un revêtement fini modérément ramifié le long de $\overline{\mathcal{U}}_{r,G} \setminus \mathcal{U}_{r,G}$ correspondant au foncteur $\overline{\Psi}_{r,G}$. Avec les notations du carré cartésien*

$$\begin{array}{ccc} \mathcal{H}_{r,G} & \hookrightarrow & \overline{\mathcal{H}}_{r,G} \\ {\scriptstyle \Psi_{r,G}}\downarrow & \square & \downarrow{\scriptstyle \overline{\Psi}_{r,G}} \\ \mathcal{U}_r & \hookrightarrow & \overline{\mathcal{U}}_r \end{array} \quad ,$$

$\Psi_{r,G} : \mathcal{H}_{r,G} \to \mathcal{U}_{r,G}$ est un revêtement étale de $\mathbb{Z}$-schémas intègres correspondant au foncteur $\Psi_{r,G}$. De plus,

(1) $\overline{\mathcal{H}}_{r,G}$ *est normal à fibres* $\overline{\mathcal{H}}_{r,G} \otimes_{\mathbb{Z}[\frac{1}{|G|}]} \mathbb{Q}$ *et* $\overline{\mathcal{H}}_{r,G} \otimes_{\mathbb{Z}[\frac{1}{|G|}]} \mathbb{F}_p$ *(où* p *est un nombre premier ne divisant pas* $|G|$*) normales.*
(2) Les composantes géométriquement irréductibles de $\mathcal{H}_{r,G} \otimes_{\mathbb{Z}} \mathbb{Q}$ *et* $\mathcal{H}_{r,G} \otimes_{\mathbb{Z}} \mathbb{F}_p$ *(où* p *est un nombre premier ne divisant pas* $|G|$*) sont en correspondance bijective.*
(3) $\mathcal{H}_{r,G} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq_{\mathbb{Q}} \mathcal{H}_{r,G,\mathbb{Q}}$.

On a des énoncés similaires pour $H'_{r,G}/\overline{H}'_{r,G}$, $H_{r,G}(\mathbf{C})/\overline{H}_{r,G}(\mathbf{C})$ *etc.*; on renverra à [E01] pour un exposé de synthèse.

Terminons par un corollaire important prouvé dans [DE03]. On suppose de plus que $r = 2s$ est pair et on se fixe un r-uplet $\mathbf{C}$ formé de s paires de la forme C_i, C_i^{-1}. On appelle sous-variété de Harbater-Mumford de $\mathcal{H}_{r,G}(\mathbf{C})$ la réunion des composantes géométriquement irréductibles correspondant aux H_r-orbites des r-uplets de la forme $\mathbf{g} = (g_1, g_1^{-1}, ..., g_s, g_s^{-1}) \in \overline{\text{ni}}(\mathbf{C})$ et on la note $\mathcal{H}_{r,G}^{HM}(\mathbf{C})$. En utilisant le fait que les composantes géométriquement irréductibles de $\overline{\mathcal{H}}_{r,G}(\mathbf{C})$ sont les adhérences dans $\overline{\mathcal{H}}_{r,G}(\mathbf{C})$ des composantes géométriquement irréductibles de $\mathcal{H}_{r,G}(\mathbf{C})$ et l'interprétation modulaire de $\overline{\mathcal{H}_{r,G}^{HM}(\mathbf{C})} \setminus \mathcal{H}_{r,G}^{HM}(\mathbf{C})$ on montre que le bord de $\mathcal{H}_{r,G}^{HM}(\mathbf{C})$ est $\Gamma_{\mathbb{Q}_\mathbf{C}}$-invariant et donc que

Corollary 1.12 $\mathcal{H}_{r,G}^{HM}(\mathbf{C})$ *est définie sur* $\mathbb{Q}_\mathbf{C}$.

Là encore, on a un énoncé similaire pour $\mathcal{H}_{r,G}^{\prime HM}(\mathbf{C})$.

1.2.3 Tours modulaires de M.Fried

Les tours modulaires introduites par M.Fried [F95a], [FK97], [BF02] constituent une généralisation de la théorie des espaces de Hurwitz dans le sens où, au lieu de n'associer à un groupe G et un r-uplet de classes de conjugaison non triviales $\mathbf{C}$ qu'un seul espace de Hurwitz $\mathcal{H}_{r,G}(\mathbf{C})$, on leur associe un ou plusieurs systèmes projectifs d'espaces de Hurwitz - les tours modulaires.

Plus précisément, on se fixe un groupe G et un r-uplet $\mathbf{C} = (C_1, ..., C_r)$ de classes de conjugaison non triviales de G tel que (1) l'ensemble $P(G, \mathbf{C})$ des nombres premiers p divisant l'ordre de G mais premiers à l'ordre des éléments de chacune des C_i, $i = 1, ..., r$ soit non vide et (2) la classe de Nielsen $\overline{\text{ni}}(\mathbf{C})$ est aussi non vide. Pour tout $p \in P(G, \mathbf{C})$, on considère le p-revêtement de Frattini universel de G, ${}_p\tilde{\phi} :_p \tilde{G} \twoheadrightarrow G$. Son noyau est un pro-$p$-groupe libre de rang fini ; sa série de Frattini

$$\ker_0 := \ker({}_p\tilde{\phi}),\ \ker_1 = \Phi(\ker_0) = \ker_0^p[\ker_0, \ker_0,],\ ..., \ker_{n+1} = \Phi(\ker_n) = \ker_n^p[\ker_n, \ker_n,], etc$$

forme donc un système de voisinages ouverts de 1 et, en notant

$$({}^{n+1}_p\tilde{G} :=\ {}_p\tilde{G}/\ker_{n+1} \twoheadrightarrow\ {}^n_p\tilde{G} :=\ {}_p\tilde{G}/\ker_n)_{n\geq 0}$$

le système de quotients caractéristiques associés on a donc : ${}_p\tilde{G} = \varprojlim_{n\geq 0} {}^n_p\tilde{G}$ De plus, par le lemme de Schur-Zassenhauss, il existe un unique $\mathbf{C}_n = (C_{n,1}, ..., C_{n,r}) \in \mathcal{C}_r({}^n_p\tilde{G})$ relevant $\mathbf{C}$ dans ${}^n_p\tilde{G}$ et tel que les éléments de $C_{i,n}$ sont de même ordre que ceux de C_i, $i = 1, ..., r$, $n \geq 0$. On obtient donc un système projectif $({}^{n+1}_p\tilde{G}, \mathbf{C}_{n+1}) \twoheadrightarrow ({}^n_p\tilde{G}, \mathbf{C}_n))_{n\geq 0}$ définissant un système projectif d'espaces de Hurwitz

$$(\mathcal{H}_{r,{}^{n+1}_p\tilde{G}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r,{}^n_p\tilde{G}}(\mathbf{C}_n))_{n\geq 0}$$

qu'on appelle la tour modulaire associée aux données $(G, \mathbf{C}, p)$. De même, on dispose de la tour modulaire dessymmétrisée correspondante

$$(\mathcal{H}'_{r,{}^{n+1}_p\tilde{G}}(\mathbf{C}_{n+1}) \to \mathcal{H}'_{r,{}^n_p\tilde{G}}(\mathbf{C}_n))_{n\geq 0}.$$

Nous étudions ces objets dans les chapitres 4 et 5.3 de cette thèse. Mentionons pour terminer l'exemple des groupes dihédraux, qui sert de fil conducteur à l'énoncé des conjectures dans la théorie des tours modulaires.

Example 1.13 (La tour modulaire des dihédraux) Notons $G = D_{2p}$ le groupe dihédral d'ordre $2p$ où $p \geq 3$ est un nombre premier et $\mathbf{C} = (I, I, I, I)$ le 4-uplet formé de 4 copies de la classe d'involutions de D_{2p}. Dans ce cas ${}_p\tilde{G} = D_{2p^\infty} = \mathbb{Z}_p \rtimes \mathbb{Z}/2\mathbb{Z}$ et ${}^n_p\tilde{G} = D_{2p^{n+1}}$, $\mathbf{C}_n = (I_n, I_n, I_n, I_n)$ est le 4-uplet formé de 4 copies de la classe d'involutions de D_{2p^n}, $n \geq 0$. On a alors pour tout $n \geq 1$, [D04], un diagramme commutatif

$$\begin{array}{ccc} \mathcal{H}_{r,D_{2p^{n+1}}}(\mathbf{C}_{n+1}) & \longrightarrow & X_1(p^{n+1}) \\ \downarrow & & \downarrow \times p \\ \mathcal{H}_{r,D_{p^n}}(\mathbf{C}_n) & \longrightarrow & X_1(p^n) \end{array}$$

autrement dit un morphisme de la tour modulaire associée à $(D_{2p}, \mathbf{C}, p)$ sur la tour usuelle $(X_1(p^n))_{n\geq 0}$ des courbes modulaires.

1.3 G-revêtements sur les corps complets

Les théorèmes d'existence de Riemann et de descente de Grothendieck permettent de résoudre très précisément la conjecture (RIGP/k) pour un corps k algébriquement clos de caractéristique 0. En généralisant la méthode de recollement analytique complexe qui sous-tend la preuve du théorème d'existence de Riemann aux corps complets, D.Harbater a montré la conjecture (RIGP/k) pour k un corps complet non archimédien. De nombreuses variantes de la preuve de ce résultat ont ensuite été données par D.Haran, Q.Liu, F.Pop, H.Volklein *etc.*. On peut distinguer deux types d'approche, le cadre de la géométrie formelle et celui de la géométrie rigide. Pour le cas des réels, P.Dèbes et M.Fried ont obtenu par des méthodes de descente un énoncé aussi précis que le théorème d'existence de Riemann.

1.3.1 G-revêtements p-adiques

L'une des difficultés pour étendre la preuve du théorème d'existence de Riemann à d'autres corps que $\mathbb{C}$ est de trouver une "bonne" catégorie pour remplacer celle des espaces analytiques complexes dans le principe G.A.G.A. et donner un sens à la notion de recollement. Pour les corps valués complets non archimédiens, c'est le rôle que vont jouer la catégories des schémas formels (G.A.G.F.) ou des espaces analytiques rigides (G.A.G.R.). Avant d'énoncer les résultats qui nous seront nécessaires, rappelons les définitions de ces deux catégories :

1.3.1.1 Schémas formels

Soit X un schéma noetherien et $Y \hookrightarrow X$ un sous-schéma fermé défini par un faisceau d'idéaux $\mathcal{I}_Y < \mathcal{O}_X$. On appelle *complétion formelle de X le long de Y* l'espace annelé $(\hat{X}, \mathcal{O}_{\hat{X}})$ où : $\hat{X}$ est l'espace topologique Y et $\mathcal{O}_{\hat{X}}$, le faisceau d'anneaux $\varprojlim_{n\geq 0} \mathcal{O}_X/\mathcal{I}_Y^n$ sur $\hat{X}$. En notant $Y_n \hookrightarrow X$, $n \geq 0$, le sous schéma fermé défini par le faisceau d'idéaux $\mathcal{I}_Y^n < \mathcal{O}_X$, on peut interpréter $(\hat{X}, \mathcal{O}_{\hat{X}})$ comme la limite inductive $\varinjlim_{n\geq 0} Y_n$ dans la catégorie des espaces localement annelés. Intuitivement, $(\hat{X}, \mathcal{O}_{\hat{X}})$ est plus "épais" que chacun des Y_n mais est contenu dans tout voisinage ouvert de Y dans X ; on parle donc du voisinage formel de Y dans X. De même, pour tout faisceau cohérent $\mathcal{F} \in \mathrm{Coh}(X)$ on peut définir la complétion formelle de $\mathcal{F}$ le long de Y par $\hat{\mathcal{F}} = \varprojlim_{n\geq 0} \mathcal{F}/\mathcal{I}_Y^n\mathcal{F}|_Y$. La catégorie des schémas formels noethériens est alors la sous-catégorie pleine de la catégorie des espaces localement annelés dont les objets $(\mathcal{X}, \mathcal{O}_\mathcal{X})$ vérifient : il existe un recouvrement ouvert fini $(U_i)_{1\leq i\leq n}$ de $\mathcal{X}$ tel que $(U_i, \mathcal{O}_\mathcal{X}|_{U_i})$ soit isomorphe à la complétion formelle d'un schéma noethérien X_i le long d'un sous-schéma fermé $Y_i \hookrightarrow X_i$, $1 \leq i \leq n$. Le théorème d'existence de Grothendieck (G.A.G.F.) peut alors s'énoncer en termes de G-revêtements comme suit :

Theorem 1.14 (G.A.G.F., théorème d'existence de Grothendieck) *Pour tout anneau noethérien A complet par rapport à un idéal I et pour tout schéma X/A, propre sur A, notons $Y = X \times_{\mathrm{spec}(A)}$*

spec(A/I). *Pour tout ouverts affines* $U_i < Y$, $i = 1, 2$ *tels que* $Y = U_1 \cup U_2$ *en notant* $U_0 = U_1 \cap U_2$ *et* X_i *la complétion formelle de* X *le long de* U_i *(i.e. la complétion formelle de* $\tilde{U}_i$ *le long de* U_i *où* $\tilde{U}_i < X$ *est un ouvert quelconque de* X *tel que* $\tilde{U}_i \cap Y = U_i$*),* $i = 0, 1, 2$*. Le foncteur naturel de changement de base*

$$\tilde{\mathcal{R}}^{\mathrm{alg}}_{X,G} \to \tilde{\mathcal{R}}^{\mathrm{form}}_{X_1,G} \times_{\tilde{\mathcal{R}}^{\mathrm{form}}_{X_0,G}} \tilde{\mathcal{R}}^{\mathrm{form}}_{X_2,G}$$

est une équivalence de catégories.

1.3.1.2 Espaces analytiques rigides

Soit k un corps valué complet non archimédien, la catégorie des k-espaces analytiques rigides est plus difficile à décrire succintement que celle des schémas formels. Notons $k\{X_1, ..., X_n\}$ la k-algèbre des séries formelles convergentes sur le polydisque unité fermé ; on appelle k-algèbre affinoïde toute k-algèbre quotient d'une telle k-algèbre. Une k-algèbre affinoïde est alors noethérienne, complète, tous ses idéaux sont fermés et le corps résiduel de tout idéal maximal est une extension finie de k. En particulier, on dispose du foncteur bien défini de la catégorie des k-algèbres affinoïdes dans celle des ensembles : $A \to \mathrm{spm}(A)$

$A \xrightarrow{\phi} B \to \mathrm{spm}(B) \xrightarrow{\phi^{-1}()} \mathrm{spm}(A)$

Si A est une k-algèbre affinoïde, on peut considérer les éléments de A comme des fonctions sur spm(A) à valeur dans $\overline{k}$ et en notant $|\cdot|$ l'unique norme de $\overline{k}$ prolongeant celle de k, on peut munir spm(A) d'une topologie en définissant pour tout $M_0 \in$spm(A) une base de voisinages :

$$(U_\epsilon(g_1, ..., g_n, M_0) = \{M \in \mathrm{spm}(A) \mid |g_i(M)| < \epsilon,\ i = 1, ..., n\})_{\substack{\epsilon > 0 \\ g_1,...,g_n \in A \mid g_i(M_0) = 0,\ i=1,...,n}}$$

On appelle alors k-variété affinoïde l'espace localement annelé (spm$(A), A$). Pour obtenir une bonne catégorie (par exemple telle que les morphismes entre deux k-variétés affinoïdes soit rigide *i.e.* de la forme $\phi^{-1}()$) il faut "rigidifier" la sous-catégorie pleine de la catégorie des espaces localement annelés localement isomorphes à des k-variétés affinoïdes ; on obtient ainsi la catégorie des k-espaces analytiques rigides dont les objets sont des espaces localement annelés $(\mathcal{X}, \mathcal{O}_\mathcal{X})$ pour une topologie de Grothendieck et admettant un recouvrement admissible $(U_i)_{i\in I}$ tel que $(U_i, \mathcal{O}_\mathcal{X}|_{U_i})$ soit isomorphe à une k-variété affinoïde. On peut alors, dans ce contexte, énoncer un principe G.A.G.R. en termes de G-revêtements.

1.3.1.3 Enoncés

Pour obtenir des énoncés type (RIGP$/k$) pour un corps k valué complet non archimédien de corps résiduel κ, on procède en deux étapes :
(1) On réalise les groupes cycliques comme G-revêtements de $\mathbb{P}^1_k$ dont la fibre spéciale est un *mock cover* (*i.e.* dont toutes les composantes irréductibles sont isomorphes à $\mathbb{P}^1_\kappa$) dans le cadre formel ou possèdant une fibre totalement k-rationnelle au-dessus d'un k-point non ramifié dans le cadre rigide (*cf.* [H03], [L95], [Des95]). Ces deux conditions assurant la trivialité des G-revêtements que l'on recolle au-dessus de X_0.
(2) Etant donné un groupe fini G, on choisit un système de générateurs $g_1, ..., g_r$ de G et on recolle les G-revêtements cycliques de groupes $< g_1 >$,...,$< g_r >$ de façon ad hoc via G.A.G.F. ou G.A.G.R. (*cf.* [H03], [L95]). On peut même, comme dans [D95], donner un énoncé de construction explicite :

Theorem 1.15 (Harbater) *Soit* G *un groupe fini et* $H_1, H_2 < G$ *deux sous groupes tels que* $G =< H_1, H_2 >$*. Soit* $(f_i : X_i \to \mathbb{P}^1_k, \alpha)$ *un* G*-revêtement défini sur* k *d'invariants* H_i*,* $\mathbf{C}_i = (C_{i,1}, ..., C_{i,r_i})$*,* $\mathbf{t}'_i = (t_{i,1}, ..., t_{i,r_i})$ *et possèdant une fibre totalement* k*-rationnelle au-dessus de* $t_{0,i} \in \mathbb{P}^1(k) \setminus \mathbf{t}_i$*,* $i = 1, 2$*. Alors il existe un* G*-revêtement* $(f : X \to \mathbb{P}^1_k, \alpha)$ *défini sur* k*, d'invariants* G*,* $\mathbf{C} = (C^G_{1,1}, ..., C^G_{1,r_1}, C^G_{2,1}, ..., C^G_{2,r_2})$*,* $\mathbf{t} = (\chi_1(t_{1,1}), ..., \chi_1(t_{1,r_1}), \chi_2(t_{2,1}), ..., \chi_2(t_{2,r_2}))$ *où* $\chi_i \in \mathrm{PSL}_2(k)$*,* $i = 1, 2$ *(et on peut remplacer* k *par n'importe quel sous-corps* k_0 *dense dans* k*).*

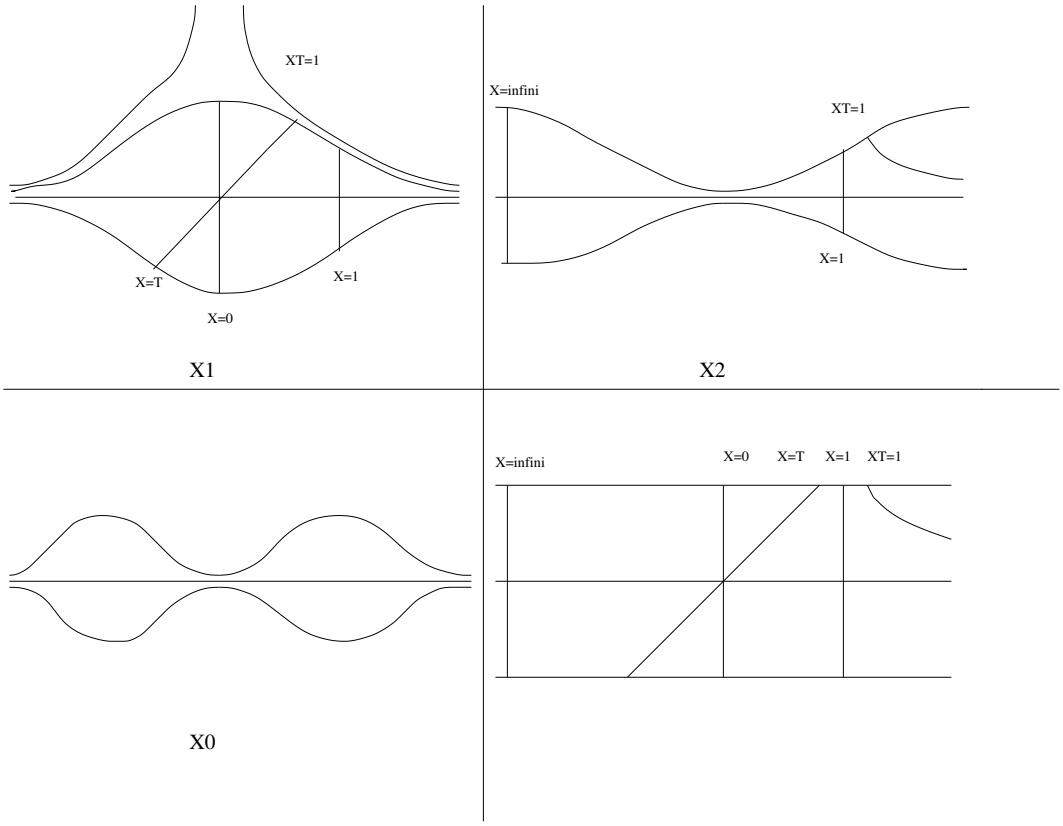


FIG. 1.1 – Recouvrement de $\mathbb{P}^1_{k[[T]]}$ par deux ouverts formels affines : $X_1 = \mathrm{spec}(k[X][[T]])$, $X_2 = \mathrm{spec}(k[X^{-1}][[T]])$ et $X_0 = \mathrm{spec}(k[X, X^{-1}][[T]])$

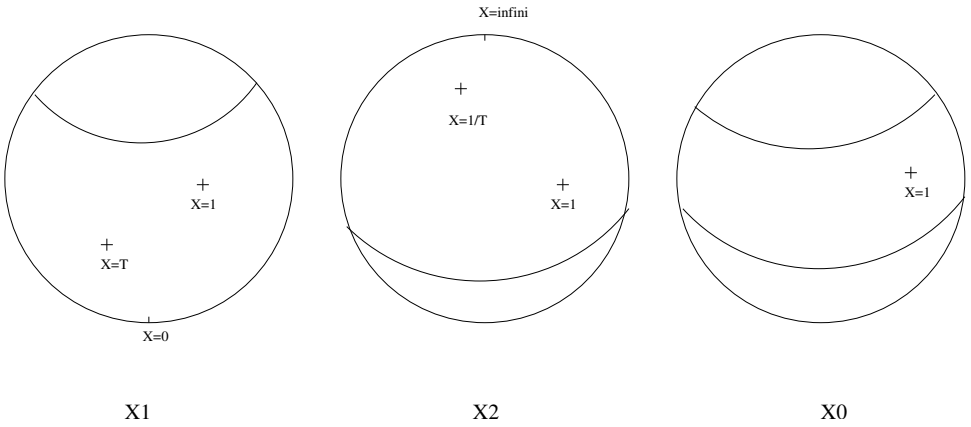


FIG. 1.2 – Recouvrement de $\mathbb{P}^1_{k((T))}$ par deux ouverts admissibles : $X_1 = \{|x| \leq 1\} = \mathrm{spm}(k[X][[T]][1/T])$, $X_2 = \{|x| \geq 1\} = \mathrm{spm}(k[X^{-1}][[T]][1/T])$ et $X_0 = \{|x| = 1\} = \mathrm{spm}(k[X, X^{-1}][[T]][1/T])$

Citons pour terminer un corollaire important concernant les HM G-revêtements [DE03].

Theorem 1.16 (HM G-revêtements sur les corps complets) *Soit G un groupe fini et k un corps valué complet non archimédien de caractéristique 0 et de caractéristique résiduelle p ne divisant pas l'ordre de G. On suppose en outre que k contient toutes les racines $|G|$-ièmes de l'unité. Soit $g_1, ..., g_s \in G$ un système de générateurs de G et $S = S_1 \cup S_2 \subset \mathbb{P}^1_k$ tel que $S_1^s := S_1 \times_k k^s = \{x_1, ..., x_s\}$, $S_2^s := S_2 \times_k k^s = \{y_1, ..., y_s\}$ avec $S_1^s \cap S_2^s = \emptyset$. On note (C) la condition $|a|, |b| \leq 1$ et $|a-b| < 1$ ou $|a|, |b| > 1$ pour $a, b \in k$. Si*

$$(*) \quad x_i, y_i \text{ vérifient (C), } i = 1, ..., s \text{ et } x_1, ..., x_s \text{ vérifient deux à deux "non (C)"}$$

alors il existe des HM G-revêtements définis sur k d'invariants G, $\mathbf{C} = (C_{g_1}^G, C_{g_1}^{G\,-1}, ..., C_{g_s}^G, C_{g_s}^{G\,-1})$, S.

Si on ne suppose plus que k contient toutes les racines $|G|$-ièmes de l'unité, on peut énoncer une variante de ce théorème *cf.* lemme 4.17.

Pour un exposé de synthèse sur les techniques de recollement et leur applications, on renverra à l'article de D. Harbater, [H03].

1.3.2 G-revêtements réels

Soit un groupe fini G, un entier $r \geq 3$ et un r-uplet $\mathbf{C}$ de classes de conjugaison non-triviales de G. Nous nous intéressons dans ce paragraphe aux G-revêtements de corps des modules $\mathbb{R}$ ou définis sur $\mathbb{R}$ d'invariants G, $\mathbf{C}$. Nous supposerons donc toujours que le diviseur des points de branchement est réel, *i.e.* formé de

$$\text{(bp)} \begin{cases} \text{- } r_1 \text{ points de branchement réels } t_1, ..., t_{r_1}, \text{ que l'on supposera ordonnés : } t_1 < ... < t_{r_1}. \\ \text{- } r_2 \text{ paires complexes conjuguées } \{z_i, \overline{z}_i\} \subset \mathbb{P}^1(\mathbb{C}) \backslash \mathbb{P}^1(\mathbb{R}). \text{ On écrira généralement} \\ z_i = t_{r_1+i}, \overline{z}_i = t_{r+1-i}, \ i = 1, ..., r_2 \text{ , que l'on ordonnera, si besoin est, selon leurs parties} \\ \text{réelles et imaginaires.} \end{cases}$$

Définissons les sous-ensembles suivants de $\mathrm{sni}(\mathbf{C})$:
- L'ensemble $\mathrm{sni}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ qui est le sous-ensemble de $\mathrm{sni}(\mathbf{C})$ formé des r-uplets $(g_1, ..., g_r)$ de $\mathrm{sni}(\mathbf{C})$ vérifiant la condition supplémentaire :

$$\text{(4) Il existe } g_0 \in G \text{ tel que } \begin{array}{l} \text{- } g_0(g_1...g_i)g_0^{-1} = (g_1...g_i)^{-1} \text{ pour } i = 1, ..., r_1 - 1 \\ \text{- } g_0 g_{r_1+i} g_0^{-1} = g_{r+1-i}^{-1} \text{ et } g_0 g_{r+1-i} g_0^{-1} = g_{r_1+i}^{-1} \text{ pour } i = 1, ..., r_2 \end{array}$$

- l'ensemble $\mathrm{sni}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$, qui est le sous-ensemble de $\mathrm{sni}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ formé des r-uplets $(g_1, ..., g_r)$ de $\mathrm{sni}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ pour lesquels

$$\text{(4)' dans (4) on peut prendre en outre } g_0 \text{ d'ordre} \leq 2$$

On notera encore $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ et $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ les ensembles quotient correspondants modulo l'action composante par composante de $\mathrm{Inn}(G)$.

On peut maintenant énoncer le résultat principal de [DF94]

Theorem 1.17 (RIGP/$\mathbb{R}$) *Etant donné un diviseur de points de branchement $\mathbf{t} \in \mathcal{U}_r(\mathbb{R})$ ordonné comme dans* (bp)*, il existe un bouquet topologique $\underline{\gamma}$ pour $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ tel que la bijection $BCD_{\underline{\gamma}}$: $(\Psi'_{r,G})^{-1}(\mathbf{t}') \simeq \overline{\mathrm{sni}}(\mathbf{C})$ identifie $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ aux G-revêtements de corps des modules contenu dans $\mathbb{R}$ et $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ aux G-revêtements définis sur $\mathbb{R}$.*

Schéma de preuve. Soit $\mathbf{t} \in \mathcal{U}_r(\mathbb{R})$ ordonné comme dans (bp). On peut trouver un bouquet topologique $\underline{\gamma}$ pour $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ tel que la conjugaison complexe c agisse sur $\underline{\gamma}$ par les formules de Hurwitz [MMa99] :

$$(*) \quad \begin{array}{ll} c.\gamma_i = \gamma_1 \cdots \gamma_{i-1} \gamma_i^{-1} (\gamma_1 \cdots \gamma_{i-1})^{-1} & \text{pour } i = 1, ..., r_1 \\ c.\gamma_{r_1+i} = \gamma_{r+1-i}^{-1} & \text{pour } i = 1, ..., r_2 \end{array}$$

Notons par $\mathcal{C}$ l'opérateur formel qui envoie la ième composante γ_i d'un r-uplet $(\gamma_1, ..., \gamma_r)$ sur le membre de droite des formules (*) (*i.e.* $c.\gamma_i = \gamma_i^{\mathcal{C}}$). Considèrons la bijection $\mathrm{BCD}_{\underline{\gamma}} : (\Psi'_{r,G})^{-1}(\mathbf{t}') \simeq \overline{\mathrm{sni}}(\mathbf{C})$; puisque c est continue, tout G-revêtement (f, α) tel que $\mathrm{BCD}_{\underline{\gamma}}((f, \alpha)) = (g_1, ..., g_r)$ a pour conjugué le G-revêtement $(f, \alpha)^c$ tel que $\mathrm{BCD}_{\underline{\gamma}}((f, \alpha)^c) = (g_1^{\mathcal{C}}, ..., g_r^{\mathcal{C}})$. Cela donne la condition définissant $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$. Pour celle définissant $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$, il suffit de remarquer qu'un G-revêtement (f, α) de corps des modules contenu dans $\mathbb{R}$ est défini sur $\mathbb{R}$ si et seulement si l'épimorphisme $\Phi_{(f,\alpha)} : \pi^{\mathrm{alg}}_{\mathbb{R},\mathbf{t}} \twoheadrightarrow G$ s'étend en un épimorphisme $\Phi_{(f,\alpha),\mathbb{R}} : \pi^{\mathrm{ar}}_{\mathbb{R},\mathbf{t}} \twoheadrightarrow G$ où, par la suite exacte fondamentale, $\pi^{\mathrm{ar}}_{\mathbb{R},\mathbf{t}} \simeq \pi^{\mathrm{alg}}_{\mathbb{R},\mathbf{t}} \rtimes \Gamma_{\mathbb{R}}$ avec l'action de c sur $\pi^{\mathrm{alg}}_{\mathbb{R},\mathbf{t}}$ décrite par les formules (*). □

Remark 1.18 Il existe d'autres façons de définir $\mathrm{sni}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ et $\mathrm{sni}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$, ce que nous ferons parfois dans la suite.

1.4 Deux outils arithmético-géométriques

1.4.1 Principe local-global pour les variétés

Nous utiliserons le principe local-global pour les variétés [Mo89], [GPR97] sous sa forme la plus élémentaire. Soit k un corps global (*i.e.* un corps de nombres ou un corps de fonctions en une variable sur un corps fini) et k^s un cloture séparable de k. Pour tout ensemble fini Σ de places de k on note k^Σ le corps des nombres totalement Σ-adique *i.e.* l'extension maximale de k dans k^s qui est totalement décomposée en chaque place $v \in \Sigma$; par exemple, si $k = \mathbb{Q}$ et $\Sigma = \{+\infty\}$, $k^\Sigma = \mathbb{Q}^{tr}$ est le corps des nombres algébriques totalement réels, de même, si $k = \mathbb{Q}$ et $\Sigma = \{p\}$, $k^\Sigma = \mathbb{Q}^{tp}$ est le corps des nombres algébriques totalement p-adiques. On a alors

Theorem 1.19 (Principe local-global pour les variétés) *Pour toute k^Σ-variété V/k^Σ, lisse et géométriquement irréductible, si pour tout $v \in \Sigma$, $V(k_v) \neq \emptyset$ pour tout plongement $k^\Sigma \hookrightarrow k_v$ (ou si, de façon équivalente, $V^\sigma(k_v) \neq \emptyset$ pour tout $\sigma \in \Gamma_k$) alors $V(k^\Sigma) \neq \emptyset$.*

Le principe local-global généralise en un sens la notion de corps existentiellement clos dans une extension : un corps k_0 est dit existentiellement clos dans une extension régulière $k_0 \hookrightarrow k$ si pour toute k_0-variété V/k_0, lisse et géométriquement irreductible, $V(k) \neq \emptyset$ implique $V(k_0) \neq \emptyset$. Un corps ample ou large par exemple (*i.e.* un corps k tel que pour touter k-variété V/k, lisse et géométriquement irréductible, $V(k) \neq \emptyset$ implique $V(k)$ est Zariski-dense) est existentiellement clos dans $k \hookrightarrow k((T))$, [P96].

Nous appliquerons essentiellement le principe local-global pour les variétés aux variétés de descente.

1.4.2 Variétés de descentes

Les variétés de descente donnent une approche géométrique de l'obstruction corps de module/corps de définition. Les énoncés ci-dessus sont des formes simplifiés des Main Theorems A et B de [DDoMo04].

Theorem 1.20 (Variété de descente pour un G-revêtement) *Etant donné un G-revêtement (f, α) de corps des modules k, il existe une k-variété affine $V(f, \alpha)/k$, lisse et géométriquement irréductible telle que*
(1) Il existe un G-revêtement $(\mathcal{F} : \mathcal{X} \to \mathbb{P}^1_{V(f,\alpha)}, \mathcal{A})$ vérifiant :
(1.1) Pour tout $v \in V(f, \alpha)$, le G-revêtement $v^\star(\mathcal{F}, \mathcal{A})$ est un $k(v)$-modèle de (f, α).
(1.2) Pour toute extension $k \hookrightarrow l$ et pour tout l-modèle (f_l, α_l) de (f, α) il existe $v \in V(f, \alpha)(l)$ tel

que $(f_l, \alpha_l) \sim v^\star(\mathcal{F}, \mathcal{A})$.
(2) Pour toute extension $k \hookrightarrow l$ *telle que* $V(f,\alpha)(l) \neq \emptyset$, $V(f,\alpha)$ *est unirationnelle sur* l.

Autrement dit, montrer qu'un G-revêtement (f, α) est défini sur une extension $k \hookrightarrow l$ de son corps des modules revient à chercher des points l-rationnels sur sa variété de descente $V(f, \alpha)$. On peut globaliser cette construction aux espaces de Hurwitz.

Theorem 1.21 (Variété de descente globale pour un espace de Hurwitz) *Etant donné un groupe fini* G, *un entier* $r \geq 3$, *il existe un* $\mathbb{Q}$*-schéma* $\mathcal{V}/\mathbb{Q}$, *lisse et quasi-projectif et un* G*-revêtement* $(\mathcal{F} : \mathcal{X} \to \mathbb{P}^1_{\mathcal{V}}, \mathcal{A}) \in H_{r,G}(\mathcal{V})$ *tel que :*
(1) $\gamma_{(\mathcal{F},\mathcal{A})} : \mathcal{V} \to \mathcal{H}_{r,G}$ *est lisse à fibres géométriquement irréductibles (où* $\gamma_{(\mathcal{F},\mathcal{A})}$ *est le morphisme structurel i.e. l'image de* $(\mathcal{F}, \mathcal{A})$ *par le morphisme canonique* $H_{r,G}(\mathcal{V}) \to \mathrm{Hom}(\mathcal{V}, \mathcal{H}_{r,G})$*).*
(2) Pour tout corps k *de caractéristique* 0 *et pour tout* k*-*G*-revêtement* $(f, \alpha) \in H_{r,G}(k)$, *il existe* $v \in \mathcal{V}(k)$ *tel que* $(f, \alpha) \sim v^\star(\mathcal{F}, \mathcal{A})$. *En particulier, l'ensemble* $\gamma_{(\mathcal{F},\mathcal{A})}(\mathcal{V}(k)) =: \mathcal{H}_{r,G}(k)^{noob}$ *est le lieu de* k*-non obstruction de* $\mathcal{H}_{r,G}$ *i.e., l'ensemble des* k*-points de* $\mathcal{H}_{r,G}$ *correspondant à des* G*-revêtements définis sur* k.

On a un énoncé similaire pour $\mathcal{H}'_{r,G}$ (resp. $\mathcal{H}_{r,G}(\mathbf{C})$ en remplaçant $\mathbb{Q}$ par $\mathbb{Q}_{\mathbf{C}}$, $\mathcal{H}'_{r,G}(\mathbf{C})$, en remplaçant $\mathbb{Q}$ par $\mathbb{Q}'_{\mathbf{C}}$.

Chapitre 2

Présentation du travail

Sommaire

introduction

Etant donné un corps k et un groupe - fini ou profini - G, considèrons les énoncés suivants :

(RIGP/k/G) Il existe une extension galoisienne $K/k(T)$ régulière sur k (i.e. telle que k soit algébriquement clos dans K) de groupe de Galois G.

(IGP/k/G) Il existe une extension galoisienne K/k de groupe de Galois G.

Quand k est un corps hilbertien (par exemple un corps de nombres) et G un groupe fini on a l'implication

$$(\text{RIGP}/k/G) \quad \Rightarrow \quad (\text{IGP}/k/G)$$

Le cadre général de ce travail est le problème de Galois inverse régulier, *i.e.* l'étude de l'énoncé (RIGP/k/G) pour tout corps k et pour tout groupe - fini ou profini - G.

Dans le cas des groupes finis, on peut distinguer deux types d'énoncés :

- Les énoncés valables pour tout groupe fini :

(RIGP/k/$\cdot$) est vrai pour
- $k = \overline{k}$ corps algébriquement clos de caractéristique 0.
- $k = \mathbb{R}$.
- k corps valué hensélien.
- k corps ample[1].

Les preuves actuelles de ces résultats sont toutes basées sur un principe G.A.G.(A., F., R.) (*cf.* chapitre 1). Le théorème d'existence de Riemann et le théorème de descente de Grothendieck donne un description complète des G-revêtements sur un corps k algébriquement clos de caractéristique 0 et la continuité de la conjugaison complexe permet d'obtenir un résultat du même type pour $k = \mathbb{R}$. Dans le cas des corps valués complets non archimédiens, on ne dispose plus de la notion de groupe fondamental topologique et donc plus non plus d'un énoncé du type 1.3 décrivant entièrement le groupe fondamental

algébrique de la droite projective privée d'un certain nombre de points. En outre, l'équivalence entre G-revêtements ramifiés de la droite projective et G-revêtements étales de la droite projective privée d'un certain nombre de points n'est plus toujours vérifiée. On a cependant un analogue partiel du théorème d'existence de Riemann :

Theorem 2.1 (1/2 théorème d'existence de Riemann, Pop [P94]) *Soit k un corps valué hensélien de rang 1, de caractéristique résiduelle p et $S \subset \mathbb{P}^1_k$ un ensemble v-ajusté en paires (i.e. S est la réunion disjointe de deux sous-ensembles fermés $S = S_1 \cup S_2$ tels que $S_i^s := S_i \times_k k^s = \{x_{i,1}, ..., x_{i,s}\}$, $i = 1, 2$ avec $|x_{1,i} - x_{2,i}| < |x_{1,i} - x_{1,j}||p|^{1/(p-1)}$, $1 \leq i \neq j \leq s$). Alors, la suite exacte courte fondamentale*

$$1 \to \pi^{\mathrm{alg}}_{k,S} \to \pi^{\mathrm{ar}}_{k,S} \to \Gamma_k \to 1$$

a pour quotient la suite exacte courte

$$1 \to \Pi \to \Pi \rtimes \Gamma_k \to \Gamma_k \to 1$$

Où Π est le produit libre de s copies de $\hat{\mathbb{Z}}$ si $p = 0$ ou de $\hat{\mathbb{Z}}/\mathbb{Z}_p$ sinon et $\sigma \in \Gamma_k$ agit sur les générateurs $(\gamma_1, ..., \gamma_r)$ de Π par $\sigma \cdot (\gamma_1, ..., \gamma_r) = (\gamma^{\chi(\sigma)}_{\pi(\sigma)(1)}, ..., \gamma^{\chi(\sigma)}_{\pi(\sigma)(r)})$ avec, comme d'habitude, $\chi : \Gamma_k \to \hat{\mathbb{Z}}^\star$ le caractère cyclotomique de k et $\pi : \Gamma_k \to \mathcal{S}_s$ la permutation induite par l'action de Γ_k sur S_1^s.

Les résultats sur les corps amples sont encore plus partiels. Ils s'obtiennent en construisant d'abord un G-revêtement $(f : X \to \mathbb{P}^1_{k((T))}, \alpha)$ de groupe G défini sur $k((T))$ qui, en fait, est défini sur une k-courbe projective C/k géométriquement irréductible possèdant un $k((T))$-point donc un sous-ensemble Zariski-dense de k-points ; on applique ensuite le théorème de Bertini-Noether et l'hypothèse ample pour montrer qu'il existe un ouvert non vide U de C dont dont la spécialisation $(f : X_u \to \mathbb{P}^1_k, \alpha)$ en tout point k-rationnel u de U est encore un G-revêtement de groupe G défini sur k. Alternativement, pour les corps amples de caractéristique 0, on peut utiliser une $\mathbb{Q}$-composante géométriquement irréductible d'un espace de Hurwitz associé à G et possèdant des $k((T))$-points correspondant à des G-revêtements définis sur $k((T))$ (*cf.* le théorème de Conway & Parker de [FV91] :*Pour tout groupe fini G, si $\mathbf{C} = (C_1, ..., C_n)$ est une énumération de toutes les classes de conjugaison non triviales de G, il existe un entier $r(G) \geq 1$ tel que pour tout $r \geq r(G)$ $\mathcal{H}_{2rn,G}(\mathbf{C}^r)$ soit géométriquement irréductible (et définie sur $\mathbb{Q}$).*) ; la variété de descente correspondante, qui est aussi géométriquement irréductible défini sur $\mathbb{Q}$ possède des $k((T))$-points, donc aussi des k-points.

L'absence de preuves purement algébriques des précédent résultats a jusqu'à présent interdit leur généralisation aux corps "maigres" comme $\mathbb{Q}^{ab}$ ou les corps de nombres. On ne dispose dans ce cas que

- D'énoncés valables pour certains groupes finis :

(RIGP/$\mathbb{Q}$/G) est vrai pour	G groupe commutatif. $G = G_1 \rtimes G_2$ produit semi-direct de deux groupes G_1, G_2 vérifiant (RIGP/$\mathbb{Q}$/G_i), $i = 1, 2$. tous les groupes sporadiques sauf M_{23}. *etc.*

On renverra par exemple à [MMa99] pour un exposé complet sur ce sujet. Ces types de résultats sont obtenus par des méthodes ad hoc comme la rigidité ou les méthodes de genre 0, qui, toutes deux, peuvent se ramener à la recherche de points $\mathbb{Q}$-rationnels sur les espaces de Hurwitz. Quand le centre $Z(G)$ n'est pas un facteur direct de G, les points $\mathbb{Q}$-rationnel d'un espace de Hurwitz ne correspondent qu'à des G-revêtements de corps des modules $\mathbb{Q}$; se pose alors le problème de l'obstruction corps des modules/corps de définition dont l'étude intervient à plusieurs endroits de cette thèse.

Pour les groupes profinis métrisables, de nouvelles obstructions apparaissent, notamment le rôle essentiel des racines de l'unité. Le Branch cycle argument contredit par exemple (RIGP/k/$\mathbb{Z}_p$) pour

tout corps k tel que $\lim_{n\to+\infty}[k(\zeta_{p^n}):k]=+\infty$ (ici, ζ_{p^n} désigne une racine primitive p^n-ième de l'unité) bien que (RIGP/$\mathbb{Q}/\mathbb{Z}/p^n\mathbb{Z}$) soit vrai pour tout $n\geq 0$. Inversement, (RIGP/$\mathbb{Q}$/GL$_n(\mathbb{Z}_p)$) a récemment été prouvé en utilisant l'algorithme de Katz pour la rigidité. L'extension des résultats du cadre fini au cadre profini est donc loin d'être immédiate et systématique. On peut cependant citer quelques énoncés positifs : (RIGP/k/G) est vrai pour

$k=\overline{k}$ corps algébriquement clos de caractéristique 0 et $G=\hat{F}_\omega$.

(1) $k=\mathbb{R}$ et $G=\hat{F}_\omega$.

(2) k corps valué hensélien de caractéristique résiduelle 0 contenant toutes les racines de l'unité et $G=\hat{F}_\omega$.

(3) k corps valué hensélien de caractéristique résiduelle $p>0$ contenant toutes les racines de l'unité et $G=\hat{F}_\omega^{(p')}$.

(4) k corps ample et $G=\lim_{\leftarrow n\geq 0} G_n$ pour un système projectif complet d'extensions scindées ($G_{n+1}\twoheadrightarrow G_n$)$_{n\geq 0}$.

où $\hat{F}_\omega$ désigne le groupe prolibre á un nombre dénombrable de générateurs et $\hat{F}_\omega^{(p')}$ sont quotient maximal d'ordre premier à p. On peut définir trois types de méthodes pour aborder ce problème :

- des méthodes "négatives" comme le Branch cycle argument ou l'argument de M. Fried dans la preuve du théorème 6.1 de [BF02].

- Le passage à la limite dans un système projectif d'ensembles finis : Etant donné un système projectif complet $(p_n:G_{n+1}\twoheadrightarrow G_n)_{n\geq 0}$ de groupes finis, on se fixe pour tout $n\geq 0$, $\mathbf{t}_n=\{t_{n,1},...,t_{n,r_n}\}\in\mathcal{U}_{r_n}$ et $\mathbf{C}_n=(C_{n,1},...,C_{n,r_n})\in\mathcal{C}_{r_n}(G_n)$ tels que $p_n(C_{n+1,i})=C_{i,n}$, $i=1,...,r_n$, $p_n(C_{n+1,i})=\{1\}$, $i=r_n+1,...,r_{n+1}$ et $t_{n+1,i}=t_{n,i}$, $i=1,...,r_n$. On montre ensuite que l'ensemble $E_n(k)$ des G-revêtements d'invariants G_n, $\mathbf{C}_n$, $\mathbf{t}_n$ définis sur k est non vide ; ce qui donne un système projectif d'ensembles finis non vides $(E_{n+1}(k)\to E_n(k))_{n\geq 0}$ dont tout élément de la limite projective $\lim_{\leftarrow n\geq 0} E_n(k)$ convient. C'est la méthode utilisée par P. Dèbes et B. Deschamps [DDes04] pour traiter les cas (1), (2), (3) ci-dessus et celle qui, combinée à la rigidité, donne par exemple (RIGP/$\mathbb{Q}(\mu_{p^\infty}(1))/\mathbb{Z}_p$), (RIGP/$\mathbb{Q}(\mu_{p^\infty}(1))/D_{2p^\infty}$), (RIGP/$\mathbb{Q}$/GL$_n(\mathbb{Z}_p)$) *etc.*

- La résolution en chaines de problèmes de plongements réguliers : Etant donné un système projectif complet $(p_n:G_{n+1}\twoheadrightarrow G_n)_{n\geq 0}$ de groupes finis, on suppose que l'on sait construire un G-revêtement (f_0,α_0) défini sur k correspondant à un épimorphisme $\phi_0:\Gamma_{k(X)}\twoheadrightarrow G_0$ tel que $k(X)^{\ker(\phi_0)}\cap\overline{k}=k$ et on essaye de construire un G-revêtement (f_1,α_1) défini sur k de quotient (f_0,α_0) autrement dit de construire un épimorphisme $\phi_1:\Gamma_{k(X)}\twoheadrightarrow G_1$ tel que $\phi_0=p_0\circ\phi_1$ et $k(X)^{\ker(\phi_1)}\cap\overline{k}=k$ puis on itère. C'est la méthode utilisée par F. Pop [P96] pour prouver le cas (4) ci-dessus en résolvant d'abord inductivement les problèmes de plongement sur $k((T))$ par recollement puis en spécialisant.

Pour reprendre la terminologie de [DDes04], on dira qu'un corps k est régulièrement Ψ-libre si (RIGP/$k/\hat{F}_\omega$) est vrai ou, de façon équivalente, si (RIGP/k/G) est vrai pour tout groupe profini métrisable. L'une des lignes directrices de cette thèse était l'étude de la Ψ-liberté régulière des corps amples et, dans un premier temps, de $\mathbb{Q}^{tr}$. D'après (1), (2) ci-dessus $\mathbb{R}$ et $\mathbb{Q}^{ab}((T))$, par exemple, sont régulièrement Ψ-libres par contre A. Tamagawa a prouvé que $\mathbb{Q}_p$ ne l'était pas, [DDes04], proposition 1.10. Cela illustre encore une fois la difficulté d'étendre les résultats du cadre fini au cadre profini. La Ψ-liberté régulière est une propriété plus faible que l'ω-liberté régulière (tout problème de plongement régulier fini admet une solution régulière propre) ; la méthode de passage à la limite dans un système projectif d'ensembles finis semble donc la plus naturelle. Elle impose cependant, étant donné un groupe profini métrisable $G=\lim_{\leftarrow n\geq 0} G_n$, de savoir réaliser à priori tous les groupes finis $(G_n)_{n\geq 0}$ avec un diviseur de points de branchement $\mathbf{t}_n$ fixé. C'est un cas particulier du problème (RIGP/k/G/div) qui consiste à réaliser un groupe fini G régulièrement sur k avec une condition div sur le diviseur de

points de branchement fixée à priori (par exemple, k_0-div : être k_0-rationnel ou k_0-pts : être constitué de points k_0-rationnels si $k_0 < k$ est un sous corps de k, *etc*). Résoudre (RIGP$/k/$div) est une condition cruciale pour appliquer la plupart des critères de descente ou recoller les G-revêtements. De plus, l'énoncé (RIGP$/k_0/G$) implique l'énoncé (RIGP$/k/G/k_0$-div), pour toute extension de corps k/k_0 ; les vérifications de (RIGP$/k/G/\mathbb{Q}$-div) (resp. (RIGP$/k/G/\mathbb{Q}^{ab}$-div)) où k est un corps de caractéristique 0 (resp. un corps de caractéristique 0 contenant toutes les racines de l'unité) et G un groupe fini constituent donc autant de tests pour l'étude du problème de Galois inverse régulier sur $\mathbb{Q}$ ou $\mathbb{Q}^{ab}$. On ne sait cependant apporter de réponses satisfaisantes à ce problème que pour les corps algébriquement clos de caractéristique 0, $\mathbb{R}$ et les corps valués henséliens. Dans le cas des corps k amples, les données sur le diviseur de point de branchement du G-revêtement sur $k((T))$ sont perdues dans l'étape de spécialisation ; c'est aussi ce qui se passe quand on applique le principe local-global pour les corps Σ-adiques.

(RIGP$/k/G/$div) est finalement le problème qui sous-tend les différents chapitres de cette thèse, par ailleurs relativement indépendants. Au chapitre 3, on donne par exemple un critère combinatoire pour résoudre (RIGP$/\mathbb{Q}^{tr}/\cdot/\mathbb{Q}$-div). Au chapitre 4, on s'intéresse à la condition ($r_1/r/\mathbb{Q}$-div) définie par : le diviseur de points de branchement $\mathbf{t} \in \mathcal{U}_r(\overline{\mathbb{Q}})$ s'écrit comme réunion disjointe $\mathbf{t} = \mathbf{t}_1 \cup \mathbf{t}_2$ avec $\mathbf{t}_2 \in \mathcal{U}_{r-r_1}(\mathbb{Q})$ et on explique comment associer à un groupe fini G une constante $c(G)$ pour laquelle (RIGP$/\mathbb{Q}^{\Sigma}_{|G|}/\cdot/(c(G)/r/\mathbb{Q}$-div)) est vrai pour une infinité de r et pour tout ensemble fini Σ de places de $\mathbb{Q}_{|G|} := \mathbb{Q}(\mathrm{e}^{2\pi i/|G|})$ ne divisant pas $|G|$ (par exemle, si G est un groupe simple possèdant un uplet g-complet de longueur $l(G)$, on peut prendre $c(G) = 2l(G) - 3$). Le chapitre 5 étudie (RIGP$/k/G$) pour les groupes profinis G extension d'un groupe fini G_0 par un groupe pronilpotent projecctif de rang fini P et k un corps de nombres ou un corps fini de caractéristique ne divisant ni $|G_0|$ ni p si P est un pro-p groupe ; l'un des corollaires que l'on obtient est que, pour de tels groupes, en notant Q-bad la condition "avoir mauvaise réduction modulo Q", (RIGP$/k_Q/G/Q$-bad) équivaut à (RIGP$/k_Q/G$) . Le chapitre 6 énonce deux résultats techniques sur les courbes de Hurwitz standards (*i.e.* obtenues en fixant tous les points de branchement sauf un), à savoir une formule générale pour en calculer le genre et une méthode de genre 0 quand $r = 4$. Le chapitre 5 enfin, utilise plutôt des méthodes "négatives" pour montrer que (RIGP$/k/G$) est faux pour un groupe profini G extension d'un groupe fini G_0 par un pro-p groupe libre P de rang fini. Des résultats sur l'obstruction corps des modules/corps de définition apparaissent aussi naturellement en plusieurs endroits des chapitres 3 et 5.

La suite de ce chapitre décrit en détails les résultats et - quand c'est possible - les idées clef des preuves des chapitres 3, 4, 5, 6.

2.1 Chapitre 3 : Counting real Galois covers of the projective line

L'objet de cet article est d'étendre les méthodes combinatoires utilisées pour évaluer $|\mathrm{sni}(\mathbf{C})|$ au calcul de $|\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)|$ et $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$. Cela nous permet de donner des versions effectives de critères de descente (de $\overline{\mathbb{Q}}$ à $\mathbb{Q}^{tr}$ ou de $\mathbb{Q}^{tr}$ à $\mathbb{Q}$) et des informations sur l'obstruction corps des modules/corps de définition.

Rappelons d'abord l'énoncé classique qui sert de base au critère de rigidité :

Proposition 2.2 (Rigidité) *Soit G un groupe fini, $\mathbf{C} = (C_1, ..., C_r) \in \mathcal{C}_r(G)$ et $\mathbf{t} = \{t_1, ..., t_r\} \in \mathcal{U}_r(\mathbb{Q})$ tel que la représentation $\pi : \Gamma_{\mathbb{Q}} \to \mathcal{S}_r$ induite par l'action naturelle de $\Gamma_{\mathbb{Q}}$ sur $\mathbf{t}' = (t_1, ..., t_r)$ vérifie pour tout $\sigma \in \Gamma_{\mathbb{Q}}$ $C_i^{\chi(\sigma)} = C_{\pi(\sigma)}$. Alors les G-revêtements d'invariants G, $\mathbf{C}$, $\mathbf{t}'$ ont pour corps des modules une extension de degré $\leq |\overline{\mathrm{sni}}(\mathbf{C})|$ de $\mathbb{Q}^2$.*

[2] En fait, on peut toujours construire $\mathbf{t}$ ainsi. En effet, si $|G| = n$, avec $\Gamma := \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$,

$$\begin{array}{ccc} \Gamma \times \{C_1, ..., C_r\} & \to & \{C_1, ..., C_r\} \\ (\sigma, C) & \to & \sigma(C) = C^{\chi(\sigma)} \end{array}$$

Quand $|\overline{\text{sni}}(\mathbf{C})| = 1$, on parle de configuration rigide. L'une des difficultés de cette méthode est le calcul de $|\text{sni}(\mathbf{C})|$. Au chapitre VII de [S92], J.-P. Serre montre que

$$|\Sigma(\mathbf{C})| = \frac{|C_1|\cdots|C_r|}{|G|}\sum_{\chi\in\text{Irr(G)}}\frac{\chi(C_1)\cdots\chi(C_r)}{\chi(1)^{r-2}}$$

où $\Sigma(\mathbf{C})$ est l'ensemble défini comme $\text{sni}(\mathbf{C})$ mais sans la condition d'engendrement (1) de la définition de $\text{sni}(\mathbf{C})$. En particulier, lorsque $\Sigma(\mathbf{C}) = \text{sni}(\mathbf{C})$, on obtient directement $|\overline{\text{sni}}(\mathbf{C})| = \frac{|\Sigma(\mathbf{C})|}{[G:Z(G)]}$. Sinon, on peut exploiter les sous-groupes maximaux de G pour déterminer inductivement $|\overline{\text{sni}}(\mathbf{C})|$. Cette formule - qui ne fait intervenir que la table des caractères de G *i.e.* une donnée facilement accessible - s'est révélée être un outil puissant pour la détection des configurations rigides ; la plupart des groupes sporadiques par exemple ont ainsi été réalisés régulièrement sur $\mathbb{Q}$ (*cf.* [MMa99] pour une investigation systématique de cette méthode).

Les deux critères de descente suivants peuvent être considérés comme des variantes du critère de rigidité classique :

Proposition 2.3 (Descente de $\overline{\mathbb{Q}}$ à $\mathbb{Q}^{tr}$) *Soit G un groupe fini et $\mathbf{C} = (C_1, ..., C_r) \in \mathcal{C}_r(G)$. Pour tout $\mathbf{t} \in \mathcal{U}_r(\mathbb{Q})$ en configuration (r_1, r_2), si :*
- pour tout $m \geq 1$ premier à $|G|$, $|\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)| = |\overline{\text{sni}}(\mathbf{C})|$ alors tous les G-revêtements d'invariants G, $\mathbf{C}$, $\mathbf{t}$ ont leur corps des modules contenu dans $\mathbb{Q}^{tr}$.
- pour tout $m \geq 1$ premier à $|G|$, $|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)| = |\overline{\text{sni}}(\mathbf{C})|$ alors tous les G-revêtements d'invariants G, $\mathbf{C}$, $\mathbf{t}$ sont définis sur $\mathbb{Q}^{tr}$.

Proposition 2.4 (Descente de $\mathbb{Q}^{tr}$ à $\mathbb{Q}$) *Soit G un groupe fini et $\mathbf{C} = (C_1, ..., C_r) \in \mathcal{C}_r(G)$ et $\mathbf{t} = \{t_1, ..., t_r\} \in \mathcal{U}_r(\mathbb{Q})$ en configuration (r_1, r_2) tel que $C_i^{\chi(\sigma)} = C_{\pi(\sigma)}$, $\sigma \in \Gamma_{\mathbb{Q}}$. S'il existe un G-revêtement (f, α) d'invariants G, $\mathbf{C}$, $\mathbf{t}$ et*
- de corps des modules contenu dans $\mathbb{Q}^{tr}$, alors le corps des modules de (f, α) est contenu dans une extension de $\mathbb{Q}$ de degré $\leq |\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)|$.
- défini sur $\mathbb{Q}^{tr}$ alors (f, α) est défini sur une extension de $\mathbb{Q}$ de degré $\leq |\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$.

La proposition 2.3 donne donc un critère pour étudier (RIGP/$\mathbb{Q}^{tr}$/$\mathbb{Q}$-div) en utilisant $|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$ et la proposition 3.18 illustrera le rôle joué par (RIGP/$\mathbb{Q}^{tr}$/$\mathbb{Q}$-div) pour descendre de $\mathbb{Q}^{tr}$ à des extensions de degré fini de $\mathbb{Q}$ (évidemment, le gain de la proposition 3.18 par rapport à la proposition 2.2 est d'obtenir une meilleure majoration du degré des extensions de $\mathbb{Q}$!). Ces deux propositions nous ont donc semblé fournir des raisons suffisantes pour chercher un analogue de la formule de Serre : c'est là le résultat central de cet article. Dans ce qui suit, $\Sigma^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ (resp. $\Sigma^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$) désigne l'ensemble défini comme $\text{sni}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ (resp. $\text{sni}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$) mais sans la relation d'engendrement (1).

Theorem 2.5 *Soit G un groupe fini et $\mathbf{C} = (C_1, ..., C_r) \in \mathcal{C}_r(G)$.*
(1) Si $\Sigma^{\mathbb{R}}(\mathbf{C}; r, 0) \neq \emptyset$ alors $|\Sigma^{\mathbb{R}}(\mathbf{C}; r, 0)| = \mathbf{n}^{\mathbb{R}}(\mathbf{C}; r, 0)$ avec :

$$\mathbf{n}^{\mathbb{R}}(\mathbf{C}; r, 0) = \frac{|G|^r}{|C_1|\cdots|C_r|}\sum_{\underline{\chi}\in\text{Irr}(G)^r}\chi_1(C_1)\cdots\chi_r(C_r)\mathbf{I}_{\underline{\chi}}$$

définit une action de groupe. En notant Γ_1 le stabilisateur de C_1 et $\sigma_1, ..., \sigma_{r_1}$ un système de représentants de Γ/Γ_1, quitte à renuméroter, on peut supposer que $\sigma_i(C_1) = C_i$, $i = 1, ..., r_1$. Soit alors t_1 un élément primitif de $k_1 = \mathbb{Q}(\zeta_n)^{S_1}/\mathbb{Q}$ et $t_i = \sigma_i(t_1)$ le point de branchement associé à C_i, $i = 1, ..., r_1$. On vérifie immédiatement que $(C_1, ..., C_{r_1})$, $(t_1, ..., t_{r_1})$ ainsi définis vérifient les relations cherchées et on itère le procédé sur $(C_{r_1+1}, ..., C_r)$

(2) Si $\Sigma^{mod,\mathbb{R}}(\mathbf{C};r,0)\neq\emptyset$ *alors* $|\Sigma^{mod,\mathbb{R}}(\mathbf{C};r,0)|=\mathbf{n}^{mod,\mathbb{R}}(\mathbf{C};r,0)$ *avec :*

$$\mathbf{n}^{mod,\mathbb{R}}(\mathbf{C};r,0)=\frac{|G|^r}{|C_1|\cdots|C_r|}\sum_{\underline{\chi}\in\mathrm{Irr}(G)^r}\chi_1(C_1)\cdots\chi_r(C_r)\mathbf{I}_{\underline{\chi}}^{mod}$$

Les $\mathbf{I}_{\underline{\chi}}$ *(resp.* $\mathbf{I}_{\underline{\chi}}^{mod}$*) sont des termes définis à partir des involutions de* G *(resp. des involutions de* G *modulo modulo une certaine relation d'équivalence faisant intervenir le centre* $Z(G)$*) et nous renvoyons au théorème 3.2 et au commentaire 3.2.2.5 pour leur définition.*

Theorem 2.6 *Soit* G *un groupe fini et* $\mathbf{C}=(C_1,C_1^{-1}...,C_s,C_s^{-1})\in\mathcal{C}_{2s}(G)$ *un* $2s$*-uplet symétrique.*
(1) $|\Sigma^{\mathbb{R}}(\mathbf{C};0,s)|\leq\mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s)$ *avec égalité si* $\Sigma^{\mathbb{R}}(\mathbf{C};0,s)=\mathrm{sni}^{\mathbb{R}}(\mathbf{C};0,s)$ *et :*

$$\mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s)=\frac{|C_1|\cdots|C_s|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(C_1)\cdots\chi(C_s)}{\chi(1)^{s-1}}\mathbf{A}_\chi$$

(2) $|\Sigma^{mod,\mathbb{R}}(\mathbf{C};0,s)|\leq\mathbf{n}^{mod,\mathbb{R}}(\mathbf{C};0,s)$ *avec égalité si* $\Sigma^{mod,\mathbb{R}}(\mathbf{C};0,s)=\mathrm{sni}^{mod,\mathbb{R}}(\mathbf{C};0,s)$ *et :*

$$\mathbf{n}^{mod,\mathbb{R}}(\mathbf{C};0,s)=\frac{|C_1|\cdots|C_s|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(C_1)\cdots\chi(C_s)}{\chi(1)^{s-1}}\mathbf{A}_\chi^{mod}$$

Les $\mathbf{A}_\chi$ *(resp.* $\mathbf{A}_\chi^{mod}$ *) sont des termes définis à partir des involutions de* G *(resp. des involutions de* G *modulo une certaine relation d'équivalence faisant intervenir le centre* $Z(G)$*) et nous renvoyons au théorème 3.4 et au commentaire 3.2.2.5 pour leur définition*

En appliquant le théorème 2.6 et la proposition 2.3, on obtient par exemple

Corollary 2.7 *Pour tout* $a\geq 2$*, toute extension galoisienne* $K/\overline{\mathbb{Q}}(T)$ *de groupe le groupe prodihédral* $D_{2a\infty}=\mathbb{Z}_a\rtimes\mathbb{Z}/2\mathbb{Z}$*, d'invariant canonique de l'inertie* (I,I,A,A) *où* I *est une classe d'involutions non triviales et* A *la classe d'un générateur de* $\mathbb{Z}_a$*, de points de branchement* $(z_1,\overline{z}_1,z_2,\overline{z}_2)$ *avec* $\{z_i,\overline{z}_i\}\in\mathcal{U}_2(\mathbb{Q})$*,* $i=1,2$ *est définie sur* $\mathbb{Q}^{tr}$*.*

Ce qui, à notre connaissance, est la seule réalisation régulière d'un groupe profini sur $\mathbb{Q}^{tr}$ par une autre méthode que la rigidité.

Les théorèmes 2.5 et 2.6 permettent aussi de rendre effectif l'évaluation de

$$\Delta^{mod,\mathbb{R}}(\mathbf{C};r_1,r_2)=|\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C};r_1,r_2)|-|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};r_1,r_2)|$$

offrant ainsi une nouvelle approche du problème corps des modules/corps de définition. Par exemple, pour $G=\mathbb{H}_8$ et $\mathbf{C}$ un uplet formé de a copies de la classe $\{\pm i\}$, b copies de la classe $\{\pm j\}$ et c copies de $\{\pm k\}$ (et $a,b\geq 1$ ou $b,c\geq 1$ ou $a\geq 1$) on obtient :

$$\begin{array}{lcl}\mathbf{n}^{mod,\mathbb{R}}(\mathbf{C};0,a+b+c) & = & 2^{a+b+c-1}\times(5+(-1)^{b+c}+(-1)^{a+c}+(-1)^{a+b})\\ \mathbf{n}^{\mathbb{R}}(\mathbf{C};0,a+b+c) & = & 2^{a+b+c}\end{array}$$

donc $\Delta^{mod,\mathbb{R}}(\mathbf{C};0,a+b+c)=2^{a+b+c-3}(3+(-1)^{b+c}+(-1)^{a+c}+(-1)^{a+b})$. En particulier, avec $a=b=1$, $c=0$, $\mathbf{t}'=(\sqrt{-1},1+\sqrt{-1},1-\sqrt{-1},-\sqrt{-1})$, on obtient deux G-revêtements d'invariants $\mathbb{H}_8$, $\mathbf{C}$, $\mathbf{t}'$; l'un - disons (f_1,α_1) - défini sur $\mathbb{R}$ et l'autre - (f_2,α_2) - de corps des modules contenu dans $\mathbb{R}$ mais non défini sur $\mathbb{R}$. En utilisant ces informations, on montre alors que (f_1,α_1) est en fait défini sur $\mathbb{Q}$ et que $(f_2\times_{\overline{\mathbb{Q}}}\overline{\mathbb{Q}_2},\alpha_2)$ a pour corps des modules $\mathbb{Q}_2$ mais n'est pas défini sur $\mathbb{Q}_2$; c'est un nouvel exemple de G-revêtement de corps des modules p-adique mais non défini sur son corps des modules (*cf.* [W02] pour $p>5$ et $G=\tilde{\mathcal{A}}_5$, l'extension centrale universelle de $\mathcal{A}_5$ et, pour le cas des revêtements purs, [CoRo04]).

Enfin, la formule explicite de $\Delta^{mod,\mathbb{R}}(\mathbf{C};0,s)$ permet d'énoncer une condition suffisante facilement vérifiable pour qu'un groupe fini G admette des G-revêtements non définis sur leur corps des modules :

Corollary 2.8 *Soit G un groupe fini. Il existe des G-revêtements d'invariants G, $\mathbf{t}$ où $\mathbf{t}$ est un diviseur réel en configuration $(0,s)$ de corps des modules réel mais non définis sur $\mathbb{R}$ ssi $Z(G)$ contient un élément qui est un carré dans G mais pas dans $Z(G)$.*

Cela permet en particulier d'exhiber de nombreuses familles de G-revêtements non définis sur les corps des modules et dans lesquelles le groupe G peut être pris arbitrairement grand (D_{2n} avec $4|n$, $\mathrm{GL}_n(p^m)$ avec $n \geq 2$, $m \geq 1$, $p \geq 3$ premier, tous les groupes finis G tels que $\mathrm{Inv}(G) \subset Z(G)$ et $2|[G : Z(G)]$ comme par exemple T_{4n} avec $n \geq 2$, $\mathrm{SL}_2(p^m)$ avec $m \geq 1$, $p \geq 3$ premier, *etc.*).

Signalons enfin que nous obtenons des énoncés similaires aux théorèmes 2.5 et 2.6 pour les revêtements purs ; nous donnons leur preuve à la fin du chapitre 3. Nous donnons aussi, dans certains cas, une borne inférieure du nombre de G-revêtements définis sur les corps p-adiques qui utilise le 1/2 Théorème d'existence de Riemann.

2.2 Chapitre 4 : Harbater-Mumford subvarieties of moduli spaces of covers

Les méthodes du chapitre 3, s'inspirant de la rigidité, étaient essentiellement combinatoires ; celles du chapitre 4 sont plus géométriques et utilisent l'arithmétique des espaces de Hurwitz pour résoudre (RIGP/k/(n/r/$\mathbb{Q}$-div)).

Si, par exemple, G est un groupe fini contenant un couple g-complet (A,B) de classes de conjugaison telles que $G =< A >=< B >$ (par exemple, si G est une extension de Frattini finie d'un des groupes suivants : M_{11}, M_{23}, J_2, J_3, $Sz(8)$, $L_2(p)$ pour p premier tel que $p \equiv 3[\mathrm{mod}4]$, $\mathcal{A}_p$ pour p premier ≥ 5 *etc.*). Alors, en notant $e(G)$ l'exposant de G et $k := \mathbb{Q}(\mathrm{e}^{\frac{2\pi i}{e(G)}})$, $\mathbf{C}_s := ((A,A^{-1}),(B,B^{-1})^s)$, $r_s := 2s+2$, on montre que pour s suffisamment grand la variété de Harbater-Mumford $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)$ est géométriquement irréductible (définie sur k) et que, pour tout $\mathbf{t}'_2 \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$, la courbe $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_2}$ obtenue en spécialisant tous les points de branchement sauf le premier est encore géométriquement irréductible (définie sur $k(\mathbf{t}'_2)$). En outre - quittes à remplacer $[B]^s$ par un uplet "rationalisé" $\phi(B^s)$ - pour tout ensemble fini Σ de places de k de caractéristique résiduelle première à l'ordre de G, on peut choisir $\mathbf{t}'_\Sigma =: \mathbf{t}'_2 \in \mathcal{U}^{r_s-1}(\mathbb{Q})$ de sorte que $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_2}(k^\Sigma)^{noob} \neq \emptyset$ (où $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_2}$ est l'image de $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_2}$ via le morphisme Σ_{r_s}). En termes de G-revêtements on obtient donc qu'il existe des G-revêtements (f,α) de groupe G, définis sur k^Σ et avec un diviseur de ramification de la forme $\mathbf{t}_f = \mathbf{t}_{f,1} + \mathbf{t}_\Sigma$ où $|\mathbf{t}_{f,1}| = 1$ et $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-1}(\mathbb{Q})$. Dans le cas général, on peut associer à G une constante $r(G)$ telle que les résultats ci-dessus restent vrais avec $\mathbf{t}'_2 \in \mathcal{U}^{r_s-r(G)}(\overline{\mathbb{Q}})$; au lie de courbes, on obtient donc des sous-variétés fermées géométriquement irréductibles de dimension $r(G)$. (par exemple, si G est un groupe fini simple non abélien, on peut prendre $r(G) = 2l(G) - 1$ où $l(G)$ est la longueur minimale d'un uplet g-complet de classes de conjugaisons de G). Ce sont ces sous-variétés fermées que l'on appelle sous-variétés de Harbater-Mumford. La constante $r(G)$ peut s'interpréter comme une "mesure générique" du nombre de points de branchement qu'il faut laisser varier pour réaliser G sur k^Σ.

Sous certaines hypothèses, notre construction est compatible avec les extensions de Frattini. Par exemple, avec les notations ci-dessus, si A, B sont en outre des p'-classes de conjugaison pour un premier p divisant l'ordre de G alors $(\mathcal{H}'^{HM}_{r_s,p^{k+1}\tilde{G}}(\mathbf{C}_{s,k+1}) \to \mathcal{H}'^{HM}_{r_s,p^k\tilde{G}}(\mathbf{C}_{s,k}))_{k\geq 0}$ est une tour de variétés de Harbater-Mumford géométriquement irréductibles (définies sur k) et pour tout $\mathbf{t}'_2 \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$, $(\mathcal{H}'^{HM}_{r_s,p^{k+1}\tilde{G}}(\mathbf{C}_{s,k+1})_{\mathbf{t}'_2} \to \mathcal{H}'^{HM}_{r_s,p^k\tilde{G}}(\mathbf{C}_{s,k})_{\mathbf{t}'_2})_{k\geq 0}$ est une tour de courbes géométriquement irréductibles (définies sur $k(\mathbf{t}'_2)$). Là encore - quittes à remplacer $[B]^s$ par un uplet "rationalisé" $\phi(B^s)$ - pour tout ensemble fini Σ de places de k de caractéristique résiduelle première à l'ordre de G, on peut choisir $\mathbf{t}'_\Sigma =: \mathbf{t}'_2 \in \mathcal{U}^{r_s-1}(\mathbb{Q})$ de sorte que (i) $\varprojlim_{k\geq 0} \mathcal{H}^{HM}_{r_s,p^k\tilde{G}}(\mathbf{C}_{s,k})_{\mathbf{t}'_\Sigma}(k_P)^{noob} \neq \emptyset$, $P \in \Sigma$ et (ii) $\mathcal{H}^{HM}_{r_s,p^k\tilde{G}}(\mathbf{C}_{s,k})_{\mathbf{t}'_\Sigma}(k^\Sigma)^{noob} \neq \emptyset$. En termes de G-revêtements on obtient donc que pour tout $k \geq 0$ il existe des G-revêtements

(f_k, α_k) de groupe ${}^k_p\tilde{G}$, définis sur k^Σ et avec un diviseur de ramification de la forme $\mathbf{t}_{f_k} = \mathbf{t}_{f_k,1} + \mathbf{t}_\Sigma$ où $|\mathbf{t}_{f_k,1}| = 1$ et $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-1}(\mathbb{Q})$.

La preuve de ces résultats se décompose en plusieurs étapes. On se fixe dans ce qui suit un groupe fini G et on note $k := \mathbb{Q}(e^{\frac{2\pi i}{e(G)}})$.

– Corps de définition de $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_2}$: Dans un premier temps, il faut trouver des composantes géométriquement irréductibles d'espaces de Hurwitz "dessymétrisés" associés à G de corps de définition aisément calculables. Le théorème de Conway & Parker ne s'applique qu'aux espaces de Hurwitz "symétrisés" mais le théorème 3.21 de [F95a] et le corollaire 1.12 suggèrent que les variétés de Harbater-Mumford peuvent jouer un rôle analogue. En particulier, pour tout $2s$-uplet symétrique $\mathbf{C} = (C_1, C_1^{-1}, ..., C_s, C_s^{-1}) \in \mathcal{C}_{2s}(G)$, $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})$ est défini sur $\mathbb{Q}'_{\mathbf{C}}$ donc pour tout $\mathbf{t}'_2 \in \mathcal{U}^{2s-r}$, $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_2}$ est défini sur $\mathbb{Q}'_{\mathbf{C}}(\mathbf{t_2}')$ (par exemple, si toutes les classes de conjugaison C_i sont rationnelles, $i = 1, ..., s$ et si $\mathbf{t}'_2 \in \mathcal{U}^{2s-r}(\mathbb{Q})$ alors $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_2}$ est défini sur $\mathbb{Q}$).

– Condition pour que $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_2}$ soit géométriquement irréductible : C'est le résultat qui remplace le théorème de Conway & Parker dans la preuve du (RIGP/k) pour k corps ample de caractéristique 0 et c'est là qu'apparait la constante $r(G)$.

1/ On reformule d'abord le problème en termes d'actions de groupes. Etant donné $\mathbf{t}' = (\mathbf{t}'_1, \mathbf{t}'_2) \in \mathcal{U}^{2s}(\mathbb{C})$ (où $\mathbf{t}'_1 \in \mathcal{U}^r(\mathbb{C})$ et $\mathbf{t}'_2 \in \mathcal{U}^{2s-r}(\mathbb{C})$), tout bouquet topologique $\underline{\gamma}$ pour $\mathbb{P}^1(\mathbf{C}) \setminus \mathbf{t}$ basé en $t_0 \notin \mathbf{t}$ définit une bijection $\mathrm{BCD}_{\underline{\gamma}} : \mathcal{H}'^{HM}_{2s,G}(\mathbf{C}) \simeq \coprod_{1\leq i\leq n} O_i$ où $O_1, ..., O_n$ sont les orbites de $\overline{\mathrm{sni}}(\mathbf{C})/SH_{2s}$ d'intersection non vide avec l'ensemble $\overline{\mathrm{hm}}(\mathbf{C})$ des HM-représentants de $\overline{\mathrm{sni}}(\mathbf{C})$ (*i.e.* les éléments $\mathbf{g} \in \overline{\mathrm{sni}}(\mathbf{C})$ de la forme $\mathbf{g} = (g_1, g_1^{-1}, ..., g_s, g_s^{-1}) =: [g_1, ..., g_s]$). Notons $\Pi_{r,2s}$ le sous-groupe de SH_{2s} engendré par les éléments $A_{i,j}$, $1 \leq i < r$, $i < j \leq 2s$. On montre alors qu'on a un isomorphisme de suites exactes courtes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1^{\mathrm{top}}(\mathcal{U}^{2s}_{\mathbf{t}'_2}, \mathbf{t}'_1) & \longrightarrow & \pi_1^{\mathrm{top}}(\mathcal{U}^{2s}, \mathbf{t}') & \longrightarrow & \pi_1^{\mathrm{top}}(\mathcal{U}^r, \mathbf{t}'_1) & \longrightarrow & 1 \\ & & \simeq\downarrow & & \simeq\downarrow & & \simeq\downarrow & & \\ 1 & \longrightarrow & \Pi_{r,2s} & \longrightarrow & SH_{2s} & \longrightarrow & SH_{2s-r} & \longrightarrow & 1 \end{array}$$

ce qui permet de décrire de façon combinatoire le revêtement $(\psi'_{2s,G})_{\mathbf{t}'_2} : \mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_2} \to \mathcal{U}^{2s}_{\mathbf{t}'_2}$: les composantes géométriquement irréductibles de $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_2}$ sont en correspondance bijective avec les orbites de $\coprod_{1\leq i\leq n} O_i/\Pi_{r,2s}$. On obtient donc : $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})$ est géométriquement irréductible ssi il n'y a qu'une seule orbite $O^{HM}(\mathbf{C}) \in \overline{\mathrm{sni}}(\mathbf{C})/SH_{2s}$ de HM-représentants et $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_2}$ reste géométriquement irréductible ssi $\Pi_{r,2s}$ agit transitivement sur $O^{HM}(\mathbf{C})$.

2/ On peut maintenant énoncer une forme purement combinatoire de notre résultat.

Notations : Pour tout m-uplet $\mathbf{a} = (a_1, ..., a_m) \in G^m$ et pour tout uplet $(E_1, ..., E_n)$ de sous-ensembles de G, on note $< \mathbf{a}^{<E_1,...,E_n>} >$ le sous-groupe de G engendré par les éléments $a_1^{e_1} \cdots a_m^{e_m}$ avec $e_1, ..., e_m \in < E_1, ..., E_n >$. Pour tout m-uplet $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$, on note $[\mathbf{A}] = (A_1, A_1^{-1}, ..., A_m, A_m^{-1})$ et $[\mathbf{A}]^s$ le $2ms$-uplet obtenu en répétant s fois le $2m$-uplet $[\mathbf{A}]$.

Theorem 2.9 *Soit* $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$, $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$ *deux uplets. Considèrons les hypothèses suivantes :*
(**H**1)=(***H*1.0**)+(***H*1.1**)+(***H*1.2**)** *avec*
(**H**1.0) *Il existe* $\mathbf{a} \in \mathbf{A}$ *tel que* $G =< \mathbf{a}, \mathbf{B} >$.
(**H**1.1) $< \mathbf{a}^{<\mathbf{b}>} >$ *agit transitivement sur* B_i *pour tout* $\mathbf{a} \in \mathbf{A}$, $\mathbf{b} \in \mathbf{B}$, $i = 1, ..., n$.

(**H**1.2) $< \mathbf{a}_i^{<\mathbf{B}>} >$ *agit transitivement sur* A_i *pour tout* $\mathbf{a}_i = (a_1, ..., a_{i-1}) \in A_1 \times \cdots \times A_{i-1}$, $i = 2, ..., m$.
(**H**2) *Il existe* $b_i \in B_i$, $b_j \in B_j$ *tels que* $b_i b_j = b_j b_i$, $1 \leq i \neq j \leq n$.
Alors
(**C**1) *Si* **A**, **B** *vérifient* (**H**1) *alors pour* s *suffisamment grand et en posant* $\mathbf{C}_s = ([\mathbf{A}], [\mathbf{B}]^s)$, *tous les HM-représentants sont dans une seule orbite* $O^{HM}_{2m-1}(\mathbf{C}_s) \in \overline{\text{sni}}(\mathbf{C})/SH_{2(m+sn)}$.
(**C**2) *Si, de plus,* **B** *vérifie* (**H**2) *alors* $\Pi_{2m-1,2(m+sn)}$ *agit transitivement sur la* $SH_{2(m+sn)}$*-orbite des HM-représentants* $O^{HM}_{2m-1}(\mathbf{C}_s) \in \overline{\text{sni}}(\mathbf{C}_s)/SH_{2(m+sn)}$.

Remark 2.10 On peut remplacer (**H**1.1),(**H**1.2) par les conditions plus fortes mais plus faciles à vérifier :
($\mathbf{H}^+$1.1) $< \mathbf{a}^{<\mathbf{b}>} >= G$ pour tout $\mathbf{a} \in \mathbf{A}$, $\mathbf{b} \in \mathbf{B}$
($\mathbf{H}^+$1.2) $< \mathbf{a}_i^{<\mathbf{B}>} >= G$ pour tout $\mathbf{a}_i = (a_1, ..., a_{i-1}) \in A_1 \times \cdots \times A_{i-1}$, $i = 2, ..., m$.
Cela permet d'obtenir par exemple un corollaire facilement manipulable comme :
Corollary 2.11 *Si* G *contient deux uplets* $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$ *et* $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$ *tels que*

(i) $G =< A_1 >=< \mathbf{B} >$.
(ii) $(\mathbf{A}, \mathbf{B}) \in \mathcal{C}_{m+n}(G)$ *est g-complet.*
(iii) *Il existe* $b_i \in B_i$, $b_j \in B_j$ *tels que* $b_i b_j = b_j b_i$, $1 \leq i \neq j \leq n$.

Alors, pour s *suffisamment grand, en écrivant* $\mathbf{C}_s := ([\mathbf{A}], [\mathbf{B}]^s)$, *il y a une unique* $SH_{2(m+sn)}$ *HM-orbite* $O^{HM}(\mathbf{C}_s) \in \overline{\text{sni}}(\mathbf{C}_s)/SH_{2(m+sn)}$ *et* $\Pi_{2m-1,2(m+sn)}$ *agit transitivement sur cette orbite.*
Par exemple, si G est un groupe fini et $(C_1, ..., C_t) \in \mathcal{C}_t(G)$ un t-uplet g-complet tel que $G =< C_1 >=< C_t >$, on peut prendre $\mathbf{A} = (C_1, ..., C_{t-1})$ et $\mathbf{B} = (C_t)$. On peut de façon générale définir $r(G)$ comme le minimum des $2m - 1$ sur l'ensemble des uplets **A**, **B** vérifiant les hypothèses du théorème 2.9

La preuve de ce théorème est technique ; elle se schématise comme suit :
(1) On montre d'abord que pour s suffisamment grand tous les HM-représentants sont dans une même $\Pi_{1,2m-1}$-orbite $O^{HM}_{2m-1}(\mathbf{C}_s) \in \overline{\text{sni}}(\mathbf{C}_s)/\Pi_{1,2m-1}$.
(2) On montre ensuite que pour tout $1 \leq i < j \leq 2(m + ns)$ il existe $g_{i,j} \in O^{HM}_{2m-1}(\mathbf{C}_s)$ tel que $A_{i,j} \cdot g_{i,j} = g_{i,j}$.
(3) On conlut en utilisant le fait que $\Pi_{1,2m-1}$ est distingué dans SH_{r_s} donc que les $A_{i,j}$ permutent les orbites de $\overline{\text{sni}}(\mathbf{C}_s)/\Pi_{1,2m-1}$.
Nous renvoyons à la section 4.3 pour les détails techniques.

– Application du principe local-global : On conserve les notations du théorème 2.9.

1/ Pour tout ensemble fini Σ de places de k, les techniques de recollement p-adique (formelles ou rigides) permettent, pour tout $P \in \Sigma$, de construire des G-revêtement définis sur k_P et d'invariants G, $\mathbf{C}_s$, $(\mathbf{t}'_{1,\Sigma}, \mathbf{t}'_{2,\Sigma})$. Il n'est pas évident à priori que ces G-revêtements sont des HM-G-revêtements. Si les caractéristiques résiduelles des places de k sont premières à l'ordre de G, le théorème 1.16 permet de construire $(\mathbf{t}'_{1,\Sigma}, \mathbf{t}'_{2,\Sigma})$ avec $\mathbf{t}'_{2,\Sigma} \in \mathcal{U}^{r_s-(2m-1)}(k)$ de sorte que les G-revêtements obtenus soient bien HM. Dans le cas général, le problème est encore ouvert (à cause de la mauvaise réduction des expaces de Hurwitz en ces places). En outre, les conditions de congruences (*) imposées à $(\mathbf{t}'_{1,\Sigma}, \mathbf{t}'_{2,\Sigma})$ imposent de grossir le corps k pour les réaliser. Pour palier ce problème *i.e.* obtenir des HM-G-revêtements qui sont encore définis sur k_P, $P \in \Sigma$ et des variétées définies sur k, il faut remplacer $[\mathbf{B}]^s$ par un uplet "rationalisé" $\text{Rat}_{\underline{m}}(\mathbf{B}^s)$ et travailler dans l'image symétrisée $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C})_{\mathbf{t}'_\Sigma}$ de $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C})_{\mathbf{t}'_\Sigma}$. Nous renvoyons à la section 4.4.2 pour les détails.

2/ D'après le théorème 2.9, $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C})_{\mathbf{t}'_\Sigma}$ est géométriquement irréductible définie sur $\mathbb{Q}_{|G|}$ donc la variété de descente globale associée $\mathcal{D}^{HM}_{r_s,G}(\mathbf{C})_{\mathbf{t}'_\Sigma}$ est aussi lisse géométriquement irréductible défini sur k. De plus, d'après le point 1/, $\mathcal{D}^{HM}_{r_s,G}(\mathbf{C})_{\mathbf{t}'_\Sigma}(k_P)^{noob} \neq \emptyset$, $P \in \Sigma$ donc en appliquant le

principe local-global à $\mathcal{D}^{HM}_{r_s,G}(\mathbf{C})_{\mathbf{t}'_\Sigma}$, on obtient $\mathcal{D}^{HM}_{r_s,G}(\mathbf{C})_{\mathbf{t}'_\Sigma}(k^\Sigma)^{noob} \neq \emptyset$ ou, de façon équivalente, que $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C})_{\mathbf{t}'_\Sigma}(k^\Sigma)^{noob} \neq \emptyset$.

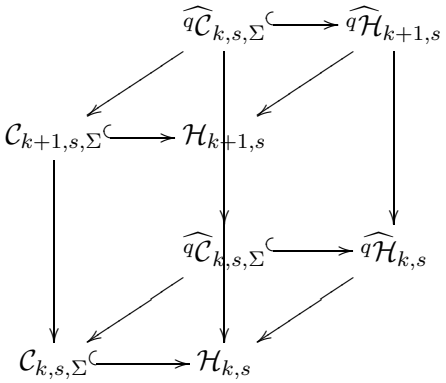
– Compatibilité avec les extensions de Frattini : Elle résulte de la proposition suivante, démontrée au paragraphe 4.3.

Proposition 2.12 *Pour tout groupe fini G vérifiant les hypothèses* (**H**1.0), (**H**$^+$1.1), (**H**$^+$1.2) *avec* $\mathbf{A} = (A_1, ..., A_m)$, $(B_1, ..., B_n)$, *pour s suffisamment grand* $\mathbf{C}_s := ([\mathbf{A}], [\mathbf{B}]^s)$ *vérifie* (**C**1) *et* (**C**3) *si les B_i, $i = 1, ..., n$ sont des p'-classes de conjugaison pour un nombre premier p ne divisant pas l'ordre de $|G|$ et si* **B** *vérifie* (**H**2) *alors pour tout p revêtement de Frattini fini $\tilde{G} \twoheadrightarrow G$, il existe* $\tilde{\mathbf{A}} \in \mathcal{C}_m(\tilde{G})$, $\tilde{\mathbf{B}} \in \mathcal{C}_n(\tilde{G})$ *relevant* **A**, **B** *et tels que le uplet* $([\tilde{\mathbf{A}}], [\tilde{\mathbf{B}}]^s)$ *vérifie* (**C**2).
(**C**4) *Si $n = 1$ alors pour tout revêtement de Frattini fini $\tilde{G} \twoheadrightarrow G$, pour tout* $\tilde{\mathbf{A}} \in \mathcal{C}_m(\tilde{G})$, $\tilde{\mathbf{B}} \in \mathcal{C}_n(\tilde{G})$ *relevant* **A**, *le uplet* **B**, $([\tilde{\mathbf{A}}], [\tilde{\mathbf{B}}]^s)$ *vérifie* (**C**2).

On se fixe un groupe fini G vérifiant les hypothèses (**H**1.0), (**H**$^+$1.1), (**H**$^+$1.2) avec $\mathbf{A} = (A_1, ..., A_m)$, $(B_1, ..., B_n)$. Pour tout ensemble fini Σ de places de k de caractéristique résiduelle première à l'ordre de G,

- Dans le cas où (**C**3) est vérifiée, on peut considérer la tour $(\mathcal{H}^{HM}_{r_s,{}^{k+1}_p\tilde{G}}(\mathbf{C}_{s,k+1})_{\mathbf{t}'_\Sigma} \to \mathcal{H}^{HM}_{r_s,{}^{k}_p\tilde{G}}(\mathbf{C}_{s,k})_{\mathbf{t}'_\Sigma})_{k\geq 0}$ de HM-sous-variétés géométriquement irréductibles définies sur k ; elle vérifie les propriétés (i) et (ii) introduites au début de cette section.

- Dans le cas où G est aussi q-parfait pour un nombre premier $q \neq p$ divisant l'ordre de G, Schur-Zassenhauss implique qu'il existe un unique système projectif $(\widehat{{}^q\mathbf{C}_{s,k}})_{k\geq 0}$ de r_s-uplets symétriques $\widehat{{}^q\mathbf{C}}_{s,k} \in \mathcal{C}_{r_s}(\widehat{{}^q({}^k_p\tilde{G})})$ relevant $\mathbf{C}_{s,k} \in \mathcal{C}_{r_s}({}^k_p\tilde{G})$ dans la q-extension centrale universelle $\widehat{{}^q({}^k_p\tilde{G})}$ de ${}^k_p\tilde{G}$ avec la propriété que les éléments des classes de conjugaison de $\widehat{{}^q\mathbf{C}}_{s,k}$ est même ordre que ceux des classes de conjugaison de $\mathbf{C}_{s,k}$. En notant $\mathcal{H}_{s,k} := \mathcal{H}^{HM}_{r_s,{}^k_p\tilde{G}}(\mathbf{C}_{s,k})$, $\widehat{{}^q\mathcal{H}}_{s,k} := \mathcal{H}^{HM}_{r_s,\widehat{{}^q({}^k_p\tilde{G})}}(\widehat{{}^q\mathbf{C}}_{s,k})$, $\mathcal{C}_{s,k,\Sigma} := \mathcal{H}^{HM}_{r_s,{}^k_p\tilde{G}}(\mathbf{C}_{s,k})_{\mathbf{t}'_\Sigma}$ et $\widehat{{}^q\mathcal{C}}_{s,k,\Sigma} := \mathcal{H}^{HM}_{r_s,\widehat{{}^q({}^k_p\tilde{G})}}(\widehat{{}^q\mathbf{C}}_{s,k})_{\mathbf{t}'_\Sigma}$, $k \geq 0$ on obtient le diagramme défini sur k :



dont la partie de gauche porte des (doubles) systèmes projectifs de points k_P-rationnels pour tout $P \in \Sigma$ et vérifie $\widehat{{}^q\mathcal{C}}_{s,k,\Sigma}(K^\Sigma)^{noob} \neq \emptyset$, $k \geq 0$.

On peut itérer ou varier (par exemple si G est parfait, considérer les extensions centrales universelles *etc*) ce procédé. Cela montre en particulier que des propriétés structurelles fortes sont conservées le long de certaines tours modulaires (et tours centrales associées comme $(\widehat{{}^q\mathcal{H}}_{s,k+1} \to \widehat{{}^q\mathcal{H}}_{s,k})_{k\geq 0}$) et souligne la difficulté des conjectures de Fried sur la disparition des points rationnels sur les tours modulaires au-delà d'un certain niveau.

Nous n'avons esquissé ci-dessus la preuve que dans le cas où le corps de base est $\mathbb{Q}(e^{\frac{2\pi i}{e(G)}})$. On peut généraliser cela au cas où le corps de base est $\mathbb{Q}$ (quitte à augmenter $r(G)$). On explique aussi au paragraphe **??** ce qui se passe quand on essaye d'appliquer directement le procédé décrit ci-dessus aux corps amples ou quand l'ensemble fini Σ est remplacé par un ensemble infini ; les résultats obtenus sont alors beaucoup plus faibles.

Terminons par citer un exemple où le fait d'avoir tous les points de branchement fixés sauf un permet de réaliser régulièrement un groupe profini sur $\mathbb{Q}^{tr}$: notons $D_{2a} =< u, v | u^a = v^2 = 1, vuv = u^{-1} >$ le groupe dihédral d'ordre $2a$. En prenant $\mathbf{A} = (I)$, où I est une classe d'involutions et $\mathbf{B} = (\{u, u^{-1}\})$, le groupe D_{2a} avec les uplets $\mathbf{A}$ et $\mathbf{B}$ vérifie les hypothèses (**H**1.0), (**H**$^+$1.1), (**H**$^+$1.2) et (**H**2) donc pour s suffisamment grand il existe des G-revêtements $(\tilde{f}_1, \tilde{\alpha}_1)$ définis sur $\mathbb{Q}^{tr}$ d'invariants D_{2a}, $([\mathbf{A}], [\mathbf{B}]^s)$, $\tilde{\mathbf{t}}' = (t_1, 0, i, -i, 1+i, 1-i, ..., s-1+i, s-1-i)$, où $t_1 \in \mathbb{Q}^{tr}$. Puis en observant que tout G-revêtement défini sur $\mathbb{R}$ et d'invariants D_{2a}, $([\mathbf{A}], [\mathbf{B}]^s)^m$ (avec $(m, 2a) = 1$), $\mathbf{t}'$ en configuration $(2, s-1)$ se relève en des G-revêtements d'invariants D_{2a^n}, $([\mathbf{A}], [\mathbf{B}]^s)^m$, $\mathbf{t}'$ tous définis sur $\mathbb{R}$, on conclut que tout système projectif de G-revêtements $(f_n, \alpha_n)_{n\geq 1}$ d'invariants D_{2a^n}, $([\mathbf{A}], [\mathbf{B}]^s)$, $\tilde{\mathbf{t}}'$ avec $(f_1, \alpha_1) = (\tilde{f}_1, \tilde{\alpha}_1)$ est en fait un système projectif de G-revêtements définis sur $\mathbb{Q}^{tr}$.

2.3 Chapitre 5 : Rational points on towers of Hurwitz spaces

Cet article a pour objet l'étude du (RIGP/G/k) pour k un corps de nombre et G un groupe profini extension d'un groupe fini G_0 par un groupe pronilpotent projectif de rang fini P (Cela inclut en particulier $\mathbb{Z}_p$, D_{2p^∞}, tout p-revêtement de Frattini universel d'un groupe fini *etc.*) ainsi que sa généralisation en terme de systèmes projectifs de points k-rationnels sur les tours d'espaces de Hurwitz associées à G.

Commençons par décrire un procédé général "d'abélianisation" qui permet de se ramener au cas où P est un pro-p groupe libre abélien de rang fini et, ainsi, d'appliquer les techniques de [F95b] pour les groupes prodihédraux.

La série de Frattini d'un pro-p groupe P est la famille de sous groupes caractéristiques définie inductivement par

$$P_0 := P,\ P_1 := P^p[P,P],\ ...,\ P_{n+1} := P_n^p[P_n, P_n],\ ...etc.$$

Si G est un groupe profini extension d'un groupe fini G_0 par un pro-p groupe libre de rang fini P, posons $G_n := G/P_n$, $n \geq 0$; on a alors $G = \varprojlim_{n\geq 0} G_n$ ce qui nous conduit à étudier les réalisation régulières des G_n. Celles-ci sont liées aux réalisations régulières des $\overline{G}_n := G/P^{ab}/(P^{ab})_n$, $n \geq 0$ via le diagramme commutatif de tours d'espaces de Hurwitz

$$\begin{array}{ccc} \mathcal{H}_{r_{n+1}, G_{n+1}}(\mathbf{C}_{n+1}) & \twoheadrightarrow & \mathcal{H}_{r_{n+1}, \overline{G}_{n+1}}(\overline{\mathbf{C}}_{n+1}) \\ \downarrow & & \downarrow \\ \mathcal{H}_{r_n, G_n}(\mathbf{C}_n) & \twoheadrightarrow & \mathcal{H}_{r_n, \overline{G}_n}(\overline{\mathbf{C}}_n) \end{array}$$

(où, si $\mathbf{C}$ est un uplet quelconque de classes de conjugaison de G, $\mathbf{C}_n$ (resp. $\overline{\mathbf{C}}_n$) est l'image de $\mathbf{C}$ via la projection canonique $G \twoheadrightarrow G_n$ (resp. $G \twoheadrightarrow G/P^{ab} \twoheadrightarrow \overline{G}_n$)). Tout G-revêtement $f_n : X_n \to \mathbb{P}^1_k$ d'invariants G_n, $\mathbf{C}_n$ induit un G-revêtement $\overline{f}_n : \overline{X}_n \to \mathbb{P}^1_k$ d'invariants $\overline{G}_n$, $\overline{\mathbf{C}}_n$. En outre le quotient modulo P/P_n de f_n et le quotient modulo $P^{ab}/(P^{ab})_n$ de $\overline{f}_n$ sont identiques ; c'est un G-revêtement $f_0 : X_0 \to \mathbb{P}^1_k$ d'invariants G_0, $\mathbf{C}_0$.

Si on suppose de plus que $\mathbf{C}$ n'est formé que d'un nombre fini de classes de conjugaison d'éléments d'ordre fini, les revêtements $\overline{X}_n \to X_0$ sont étales de groupe $P^{ab}/(P^{ab})_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^r$ (où r est le rang de P). Or, si f_n est défini sur k, il en est de même $\overline{X}_n \to X_0$ et, quitte à prendre une extension finie

k_0/k telle que $X_0(k_0) \neq \emptyset$, $\overline{X}_n \times_k k_0 \to X_0 \times_k k_0$ induit un unique diagramme cartésien sur k_0

$$\begin{array}{ccc} X_n \times_k k_0 & \longrightarrow & A_n \\ \downarrow & \square & \downarrow \\ X_0 \times_k k_0 & \longrightarrow & \mathrm{Jac}(X_0 \times_k k_0) \end{array}$$

où A_n *est une* k_0*-variété abélienne isogène à* $\mathrm{Jac}(X_0 \times_k k_0)$ *et possèdant un point de torsion* k_0*-rationnel d'ordre* p^n. Ce résultat interviendra à plusieurs reprises dans la suite.

Le résultat principal que nous y démontrons est le suivant :

Theorem 2.13 *Un groupe profini* G *extension d'un groupe fini* G_0 *par un groupe pronilpotent projectif* P *de rang fini ne peut être groupe de Galois d'une extension galoisienne* $K/\overline{\mathbb{Q}}(T)$ *de corps des module un corps de nombres ou un corps fini de caractéristique* $q \neq p$ *si* P *est un pro-*p *groupe.*

Géométriquement, ce théorème signifie qu'il n'existe pas de système projectifs de points k-rationnels (avec k un corps de nombres) sur les tours de Hurwitz $(\mathcal{H}_{G_{n+1},\mathbf{C}_{n+1}} \to \mathcal{H}_{G_n,\mathbf{C}_n})_{n\geq 0}$ induites par les systèmes projectifs de groupes finis (et de uplets de classes de conjugaison) $(G_{n+1} \to G_n)_{n\geq 0}$ tels que $G = \varprojlim G_n$.

La preuve de ce résultat nous a conduit a developper différentes techniques de géométrie arithmétique profinie. On se ramène d'abord au cas où P est un pro-p groupe libre de rang fini. On peut ensuite décomposer la preuve en deux grandes étapes.

La première consiste à généraliser l'obstruction cohomologique cdm/cdd usuelle à des systèmes projectifs de G-revêtements[3]. Cette *obstruction profinie* nous permet de donner des critères simples sur un groupe profini quelconque G pour que toute extension galoisienne $K/\overline{\mathbb{Q}}(T)$ de groupe de Galois G et de corps des modules un corps de nombres k soit définie sur une extension finie de k. Plus précisément, dans notre situation, ils deviennent

Proposition 2.14 *Si l'une des trois conditions suivantes est vérifiée*

(1) $Z(G)$ *est facteur direct de* G.
(2) $[G : Z(G)]$ *est fini.*
(3) $Z(G) \cap P_{n_0} = \{1\}$ *pour un* $n_0 \geq 0$.

Alors toute extension galoisienne $K/\overline{k}(T)$ *de groupe* G *et de corps des modules* k *peut être définie sur une extension finie* k_0/k. *De plus,* k_0/k *peut être choisie comme suit :* $k = k_0$ *en (1),* $[k_0 : k] \leq [G : Z(G)]$ *en (2) et* $[k_0 : k] \leq |G_{n_0}|$ *en (3).*

La vérification de ses critères utilise essentiellement trois ingredients : la classification des groupes pro-cycliques, la théorie du multiplieur de Schur et les propriétés des centralisateurs des produits libres. Il est à noter que lorsque $\mathrm{rang}(P) \geq 2$ ou lorsque G est le p-revêtement de Frattini universel d'un groupe fini p-parfait G_0, on a toujours $Z(G) \cap P = \{1\}$.

La deuxième étape est donc de montrer qu'il n'existe pas de réalisation régulière de G sur un corps de nombres. On utilise pour cela le *procédé d'abélianisation* qui, essentiellement, réduit le problème au cas où P est un pro-p groupe abélien libre de rang fini. Il faut ensuite distinguer les cas où tous les groupes d'inertie sont d'ordre fini (contradiction du nombre de points de la réduction (modulo certaines places) de la jacobienne de la courbe du premier G-revêtement des systèmes projectifs considérés) et

[3]La difficulté, dans le cas profini n'est pas seulement de pouvoir réaliser régulièrement chaque quotient fini de G mais de réaliser ces quotients finis *de façon compatible.*

le cas où au moins l'un des groupes d'inertie est d'ordre infini (contradiction de l'action galoisienne sur les générateurs distingués de l'inertie).

Dans le cas des corps finis, il est naturel de se demander ce qui se passe pour les caractéristiques manquantes du théorème 2.13. En utilisant des résultats sur les problèmes de plongement en caractéristiques positives [MMa99], chap. IV, on obtient l'énoncé suivant

Theorem 2.15 *Soit G un groupe fini, p un premier divisant $|G|$ et ${}_p\tilde{G}$ le p-revêtement de Frattini universel de G alors toute réalisation régulière de G sur un corps fini F de caractéristique p induit une réalisation régulière de ${}_p\tilde{G}$ sur F*

qui montre en particulier que les hypothèses sur la carcatéristiques sont loin d'être liées à la méthode !

On donne ensuite quelques applications des précédents résultats aux (RIGP/G/k) et (IGP/G/k). Le théorème 2.13 combiné au théorème de Beckmann [Be89] et à un argument de [S89] permet par exemple de montrer

Proposition 2.16 *Il existe une extension algébrique $k/\mathbb{Q}$ où seules un nombre fini de places se ramifient et telle que (*IGP*$/G/k$) est vrai.*

Des arguments de réduction modulo $\mathcal{Q}$ mettent par ailleurs en évidence l'importance des propriété arithmétiques du diviseur de ramification. Par exemple, si l'on considère la tour d'espaces de Hurwitz $(\mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r_n,G_n}(\mathbf{C}_n))_{n\geq 0}$ et que pour, tout nombre premier q, on définit $X_r^0(q) \subset \mathcal{U}_r(\overline{\mathbb{Q}})$ comme le sous-ensemble de tous les diviseurs $\mathbf{t} \in \mathcal{U}_r(\overline{\mathbb{Q}})$ ayant bonne réduction modulo q et, étant donné un corps de nombres k, $X_r(k,q)$ comme la $\mathrm{PGL}_2(k)$-orbite de $X_r^0(q)$. Alors, en notant $\mathcal{H}_{n,q}(k) := \mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(k) \cap (\Psi_{r_n,G_n})^{-1}(X_r(k,q))$ le sous-ensemble de $\mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(k)$ correspondant aux $\overline{\mathbb{Q}}$ G-revêtements d'invariants G_n, $\mathbf{C}_n$, de corps des modules k et de diviseur de pooints de branchement dans $X_r(k,q)$, on obtient

Proposition 2.17 *Pour tout nombre premier q ne divisant pas $|G|$ et pour tout entier $d \geq 1$ il existe $n(q,d,\mathbf{C}) \geq 0$ tel que*

$$(\star) \quad \bigcup_{[k:\mathbb{Q}]\leq d} \mathcal{H}_{n,q}(k) = \emptyset, \quad n \geq n(q,d,\mathbf{C})$$

La dernière partie de ce travail est consacrée à la conjecture de Fried qui généralise aux tours modulaires le théorème de Merel pour la tour des courbes modulaires. A savoir,

Conjecture 2.18 *Si G_0 est un groupe fini p-parfait, alors, pour tout entier $r \geq 3$, pour tout r-uplet $\mathbf{C}_0$ de p'-classes de conjugaison de G_0 et tout entier $d \geq 1$ il existe $n(d, g_{\mathbf{C}_0}) \geq 0$ tel que*

$$\bigcup_{[k:\mathbb{Q}]\leq d} \mathcal{H}_{r,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)(k) = \emptyset, \text{ for each } n \geq n(d, g_{\mathbf{C}_0})$$

(où $g_{\mathbf{C}_0}$ est le genre de la courbe X_0 associée à un G-revêtement $f_0 : X_0 \to \mathbb{P}^1$ d'invariants canoniques de l'inertie $\mathbf{C}_0$).

En réexploitant les techniques précedemment développés on donne des bornes effectives "partielles" pour le rang $n(d, g_{\mathbf{C}_0})$. Plus précisément, si l'on définit $n(q,d,\mathbf{C}_0)^{noob}$ comme dans la proposition 2.17 mais en ne considèrant que les lieux de non obstruction, on obtient

$$n(q,d,\mathbf{C})^{noob} \leq \frac{\ln(\mathcal{N}(g_{\mathbf{C}_0}, q^{d|G_0|/o(\mathbf{C}_0)}))}{\ln(p)}$$

avec $\mathcal{N}(g,n) = n + 2g(\sqrt{n} - 1) + 2^g$.

Enfin, en combinant à nouveau la procédure d'abélianisation et un argument cohomologique (qui fait intervenir de façon essentielle le fait que $Z(G) \cap P = \{1\}$ on montre que la conjecture de Fried est une conséquence de la *strong torsion conjecture pour les variétés abéliennes*.

2.4 Chapitre 6 : Standard Hurwitz curves

Le dernier chapitre de cette thèse est consacré aux courbes de Hurwitz standard *i.e.* les courbes définies par des diagrammes cartésiens

$$\begin{array}{ccc} \mathcal{H}'_{r,G}(\mathbf{C}) & \longleftarrow & \mathcal{H}'_{r,G}(\mathbf{C})_{\mathbf{t}} \\ {\scriptstyle \Psi'_{r,G}}\downarrow & \square & \downarrow \\ \mathcal{U}^r & \longleftarrow & \mathcal{U}^r_{\mathbf{t}} \simeq \mathbb{P}^1 \setminus \mathbf{t} \end{array}$$

où $\mathbf{t} = (t_2, ..., t_r) \in \mathcal{U}^{r-1}$. Il se compose de deux parties distinctes.

Dans la première partie, on démontre une généralisation à un entier $r \geq 4$ quelconque de la formule du genre pour $r = 4$ donnée dans [DF94], §4 : *Etant donné un groupe fini G et un 4-uplet $\mathbf{C} \in \mathcal{C}_4(G)$, pour toute $\Pi_{1,4}$-orbite $O \in \overline{\text{sni}}(\mathbf{C})/\Pi_{1,4}$, les composantes géométriquement irréductibles des courbes de Hurwitz standard correspondantes ont pour genre*

$$g_O = 1 - |0| + \frac{1}{2} \sum_{2 \leq i \leq 4} \sum_{\mathbf{g} \in 0} \frac{i_{1,i}(\mathbf{g}) - 1}{i_{1,i}(\mathbf{g})}$$

avec

$$\begin{array}{rcl} i_{1,2}(\mathbf{g}) & = & | < g_1 g_2 > / < g_1 g_2 > \cap Z(g_1, g_2) Z(g_3)| \\ i_{1,3}(\mathbf{g}) & = & | < g_4 g_2 > / < g_4 g_2 > \cap Z(g_4, g_2) Z(g_3)| \\ i_{1,4}(\mathbf{g}) & = & | < g_4 g_1 > / < g_4 g_1 > \cap Z(g_4, g_1) Z(g_3)| \end{array}$$

Soit maintenant un entier $r \geq 4$, un r-uplet $\mathbf{C} \in \mathcal{C}_r(G)$ et une $\Pi_{1,r}$-orbite $O \in \overline{\text{sni}}(\mathbf{C})/\Pi_{1,r}$. Pour tout $\mathbf{g} \in O$ posons

$$\left.\begin{array}{l} Z_i(\mathbf{g}) = \bigcap\limits_{2 \leq i \neq j \leq r} \text{Cen}_G(g_j)\text{Cen}_G(g_1) \\ \alpha_i(\mathbf{g}) = g_1 \cdots g_{i-1} \end{array}\right\}, \ i = 2, ..., r$$

Le genre des composantes géométriquement irréductibles des courbes de Hurwitz standard correspondantes est alors donné par

Proposition 2.19

$$g_O = 1 + \frac{(r-3)l_O}{2} - \frac{1}{2} \sum_{2 \leq i \leq r} \sum_{\mathbf{g} \in U} \frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 > |}{| < g_i^{\alpha_i} g_1 > |}.$$

Cette formule permet de manipuler le genre de façon plus générale que la formule de Riemann-Hurwitz "brute" et, notamment, d'en donner des bornes inférieures quand $\mathbf{C}$ vérifie certains types d'hypothèses.

La deuxième partie décrit une méthode de genre 0 pour les courbes de Hurwitz standard quand $r = 4$ (ou les courbes de Hurwitz réduites) basée sur le principe de Hasse et non sur l'existence de diviseurs de degré impair - comme les méthodes de genre 0 usuelles - pour montrer l'existence de points rationnels. Donnons en les différentes étapes et résultats qu'elle met en jeux. Soit G un groupe fini et $\mathbf{C} = (C_1, C_1^{-1}, C_2, C_2^{-1}) \in \mathcal{C}_4(G)$ un 4-uplet symétrique.

(1) On recherche d'abord des composantes géométriquement irréductibles de $\mathcal{H}'_{r,G}(\mathbf{C})_{\mathbf{t}}$ définie sur $\mathbb{Q}'_{\mathbf{C}}$ de genre 0. Pour cela, on cherche $O \in \overline{\text{sni}}(\mathbf{C})/\Pi_{1,r}$ telle que

- $g_O = 0$
- L'une des trois propriétés suivantes est vérifiée :

(i) $O = \overline{\text{sni}}(\mathbf{C})$

(ii) $|\overline{\text{sni}}(\mathbf{C})| - |O| < |\overline{\text{hm}}(\mathbf{C})|$

(iii) Il n'y a qu'une seule HM-orbite $O^{HM}(\mathbf{C}) \in \overline{\text{sni}}(\mathbf{C})/SH_4$ et $O = O^{HM}(\mathbf{C})$.

Pour prouver que l'orbite correspondant à O est définie sur $\mathbb{Q}'_{\mathbf{C}}$, on utilise, dans le cas (ii) le fait qu'elle

est isolée (*i.e.* toutes les autres orbites sont de cardinal $< |O|$) et dans le cas (iii), le théorème 1.12.

(2) On vérifie ensuite la condition de Hasse *i.e.* $\mathcal{H}'_{r,G}(\mathbf{C})_{\mathbf{t}\ O}(\mathbb{Q}'_{\mathbf{C}\ P}) \neq \emptyset$ pour toutes places P de $\mathbb{Q}'_{\mathbf{C}}$ sauf éventuellement une. Dans les cas (i) et (ii), cette condition est toujours vérifiée ; dans le cas (iii), elle l'est toujours si G est un p-groupe. Dans le cas (i), cela se voit en utilisant le théorème 1.15, dans le cas (ii), cela résulte du fait que $|\overline{\mathrm{hm}}(\mathbf{C})|$ est borne inférieure du nombre de G-revêtements définis sur $\mathbb{Q}'_{\mathbf{C}\ P}$ sous réserve que les points de branchement soient bien choisis (ce qui est un corollaire du 1/2 théorème d'existence de Riemann) et, dans le cas (iii), de l'application du théorème 1.16 d'où, en particulier, la restriction aux p-groupes.

Deuxième partie

Chapitre 3

Counting real Galois covers of the projective line

Il s'agit de la version longue de l'article [C04b] à paraître au P.J.M. Outre les résultats de [C04b], on y trouve la preuve intégrale du théorème 3.5 (§3.3.3), le developpement de l'exemple 3.4.1.1 (§3.4.1.2), le traitement complet de la réalisation régulière des groupes prodihédraux D_{2a^∞} sur $\mathbb{Q}^{tr}$ ainsi que quelques compléments sur la descente de $\overline{\mathbb{Q}}$ à $\mathbb{Q}^{tr}$ et l'obstruction corps des modules/ corps de définition. On donne finalement un analogue des théorèmes 3.2 et 3.4 pour les revêtements purs (§3.7) et, dans certains cas, une borme inférieure du nombre de G-revêtements d'invariants fixés définis sur les p-adiques.

Sommaire

Introduction

By Riemann's Existence Theorem there is a bijective correspondence between isomorphism classes of Galois covers $f : X \to \mathbb{P}^1_{\mathbb{C}}$ of the projective line with Galois group G and branch points $t_1, ..., t_r \in \mathbb{P}^1(\mathbb{C})$ and r-tuples $(g_1, ..., g_r) \in G$ of generators of G satisfying the relation $g_1 \cdots g_r = 1$. Fixing a r-tuple $\mathbf{C} = (C_1, ..., C_r)$ of conjugacy classes of G, we say f is of type $\mathbf{C}$ if the corresponding r-tuple $(g_1, ..., g_r) \in G$ has the extra property that there exists a permutation σ such that $g_i \in C_{\sigma(i)}$, for $i = 1, ..., r$.

An important and well-known formula proved by Serre in [S98] chap.7 computes the number of r-tuples $(g_1, ..., g_r) \in G$ with $g_i \in C_i$ for $i = 1, ..., r$ and such that $g_1 \cdots g_r = 1$. In many cases, this formula can be used to compute the number of isomorphism classes of G-covers of $\mathbb{P}^1$ of type $\mathbf{C}$, with branch points $t_1, ..., t_r \in \mathbb{P}^1(\mathbb{C})$. This formula proved to be particularly powerful in the classical rigid situation and, for instance, led to the realization over $\mathbb{Q}$ of many sporadic groups (see [MMa99] chap II for a systematic investigation of this method).

In this paper we consider the refined problem of counting the number of those G-covers of $\mathbb{P}^1$ with fixed branch locus and for which the field of the real numbers $\mathbb{R}$ is a field of definition. We also consider the related problem of how many G-covers have their field of moduli contained in $\mathbb{R}$. For these two questions P. Dèbes and M. Fried showed in [DF94] there is also a group theoretic characterization : the r-tuples $(g_1, ..., g_r) \in G$ should verify some additional conditions, involving the involutions of G (see §3.1).

Our results are the following. First, generalizing Serre's formula, and using Dèbes and Fried's results, we give a general formula for the number of r-tuples $(g_1, ..., g_r) \in G$ corresponding to G-covers $f : X \to \mathbb{P}^1$ with given branch locus and which are defined over $\mathbb{R}$. In the general situation, this formula is more complicated than the one given by Serre. In order to simplify it and make it effective, we consider two special cases separately, where the branch locus consists either only of real points or only of pairs of complex conjugate points. We give then several applications. On the one hand, we deal with the existence of G-covers which are not defined over their field of moduli. Some criteria are already known to guarantee that the field of moduli is a field of definition, for instance when $Z(G)$ is a direct summand of G (see [CoH85] prop.2.8). Most of these results rely on a cohomological approach (see for instance [D95], [DDo97] or [W02]) ; ours is different and leads to criteria - one of them being an easy-to-check group theoretic condition - for G-covers not to be defined over their field of moduli. Applying these criteria, we exhibit infinite families of groups for which one can always find such G-covers. We also give a criterion for profinite groups. On the other hand we explain how to use our computations to descend from $\mathbb{C}$ to the field $\mathbb{Q}^{tr}$ of all totally real algebraic numbers. It is known (cf [DF94] Theorem 5.7) that each finite group is the Galois group of a regular extension of $\mathbb{Q}^{tr}(X)$ but the proof of this result does not show this can be done with a branch point divisor $\mathbf{t}$ defined over $\mathbb{Q}$. Our method - when it works - enables us to choose $\mathbf{t}$ this way. It also provides regular regular realizations of the profinite dihedral groups D_{2n^∞} over $\mathbb{Q}^{tr}(X)$ with rational branch point divisor. This is, we believe, the first non trivial regular realizations of profinite groups over $\mathbb{Q}^{tr}(X)$ (Recall that D_{2n^∞} can not be realized regularly over $\mathbb{Q}(X)$ [F04]). We conclude by considering the case of the Mathieu group M_{11}.

The paper is organized as follow. In §1 we introduce the main tools. In §2 we state the results and make some comments. §3 is devoted to the proofs, §4 to the first application, §5 to the second one. In §6 we give the Mathieu group. In appendix A, we give the statements and proofs for mere covers. We also give in appendix B the character tables which are used in our examples.

I wish to thank P. Dèbes for encouraging me to write this paper and making many helpful suggestions.

3.1 Preliminaries

Notations :For a finite group G, denote :
- the set of all inner automorphisms of G by Int(G).
- the set of all elements of order ≤ 2 in G by Inv(G).
- the set of all the irreducible complex characters of G by Irr(G) and the trivial character of G by χ_1.
- for all $g \in G$ the centralizer of g in G by $\mathrm{Cen}_G(g)$.

Recall a G-cover with group G is a pair (f, α) where $f : X \to \mathbb{P}^1$ is a Galois cover with group G and $\alpha : \mathrm{Aut}(f) \to G$ is a group isomorphism. One can attach to each G-cover of $\mathbb{P}^1_{\mathbb{C}}$ the three following invariants : the monodromy group G, the branch point set $\mathbf{t} = \{t_1, ..., t_r\} \subset \mathbb{P}^1(\mathbb{C})$ (that we sometimes view as a divisor $(t_1) + ... + (t_r)$ on $\mathbb{P}^1$) and for each $t \in \mathbf{t}$ the *associated inertia canonical conjugacy class* C_t . To summarize this, we will sometimes say the considered G-cover has *ramification type* $[G, \mathbf{C}, \mathbf{t}]$ (see [V99] definition 2.12 p.37). Adopting the topological point of view, let us recall what these invariants correspond to : given $\mathbf{t} = \{t_1, ..., t_r\}$ introduce a *topological bouquet* $\underline{\gamma}$ of $\mathbb{P}^1_{\mathbb{C}} \backslash \mathbf{t}$, that is an r-tuple of homotopy classes of loops $\gamma_1, ..., \gamma_r$ based at some point $t_0 \notin \mathbf{t}$ such that
- $\gamma_1, ..., \gamma_r$ generate the topological fundamental group $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C})\backslash \mathbf{t}, t_0)$ with the single relation $\gamma_1 ... \gamma_r = 1$.
- γ_i is a loop revolving once, counterclockwise, about t_i, $i = 1, ..., r$.

Now, considering a G-cover $f : X \to \mathbb{P}^1_{\mathbb{C}}$, the monodromy action defines a permutation representation $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C})\backslash \mathbf{t}, t_0) \to \mathrm{Per}(f^{-1}(t_0))$. The image group G of this representation is the monodromy group (or, equivalently the Galois group) of f and the conjugacy class C_{t_i} of the image of γ_i in G is the inertia canonical class corresponding to t_i, $i = 1, ..., r$.

For any integer $r \geq 3$ let $\mathcal{U}^r \subset (\mathbb{P}^1_{\mathbb{C}})^r$ be the subset of $(\mathbb{P}^1_{\mathbb{C}})^r$ consisting of all r-tuples $\mathbf{t}' = (t_1, ..., t_r) \in (\mathbb{P}^1_{\mathbb{C}})^r$ such that $t_i \neq t_j$ for $1 \leq i \neq j \leq r$, let $\mathcal{U}_r = \mathcal{U}^r / S_r$ be the quotient space of $\mathcal{U}^r$ by the natural action of the symmetric group S_r and $\pi_r : \mathcal{U}_r \to \mathcal{U}^r / S_r$ the canonical projection. Given a finite group G let $\psi_{r,G} : \mathcal{H}_{r,G} \to \mathcal{U}_r$ be the coarse moduli space (fine assuming $Z(G) = \{1\}$) for the category of G-covers of $\mathbb{P}^1_{\mathbb{C}}$ with group G and r branch points, where $\psi_{r,G}$ is the application which to a given isomorphism class of G-covers associates its branch point set. For any r-tuple $\mathbf{C} = (C_1, ..., C_r)$ of non trivial conjugacy classes in G let $\mathcal{H}_{r,G}(\mathbf{C})$ be the corresponding *Hurwitz space* [FV91], that is the union of irreducible components of $\mathcal{H}_{r,G}$ parametrizing the isomorphism classes of G-covers with ramification type $[G, \mathbf{C}, \mathbf{t}]$. A point $\mathbf{h} = (h, (t_1, ..., t_r))$ of the fiber product $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$ then corresponds to a G-cover given with an ordering of its branch points, which allows us to define a monodromy application :

$$\begin{array}{rccc} \mathrm{M}: & \mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r & \to & \{C_1, ..., C_r\}^r \\ & (h, (t_1, ..., t_r)) & \to & (C_{t_1}, ..., C_{t_r}) \end{array}$$

This application, being continuous, is constant on each connected component of $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$. So, $M^{-1}(\mathbf{C})$ is a union of connected components of $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$; we will denote this variety by $\mathcal{H}'_{r,G}(\mathbf{C})$. We have a cartesian square :

$$\begin{array}{ccc} \mathcal{H}'_{r,G}(\mathbf{C}) & \xrightarrow{\Pi_r} & \mathcal{H}_{r,G}(\mathbf{C}) \\ \downarrow{\scriptstyle \psi'_{r,G}} & \square & \downarrow{\scriptstyle \psi_{r,G}} \\ \mathcal{U}^r & \xrightarrow{\pi_r} & \mathcal{U}_r \end{array}$$

We will freely use the general theory of Hurwitz spaces (see for instance [FV91] and [V99]), and only recall here the description of the fibers of $\psi_{r,G}$ and $\psi'_{r,G}$ in terms of *Nielsen classes* $\mathrm{ni}(\mathbf{C})$ and *straight*

Nielsen classes $\mathrm{sni}(\mathbf{C})$ respectively, where :

$$\mathrm{ni}(\mathbf{C}) = \left\{ (g_1,...,g_r) \in G^r \;\middle|\; \begin{array}{l} (1)\ G =< g_1,...,g_r > \\ (2)\ g_1 \cdots g_r = 1 \\ (3)\ g_i \in C_{\sigma(i)},\ i = 1,...,r \text{ for some } \sigma \in S_r \end{array} \right\}$$

and $\mathrm{sni}(\mathbf{C})$ is the set defined as $\mathrm{ni}(\mathbf{C})$, but replacing (3) by

$$(3)'\ g_i \in C_i \text{ for } i = 1,...,r.$$

We use the notations $\overline{\mathrm{ni}}(\mathbf{C})$ and $\overline{\mathrm{sni}}(\mathbf{C})$ for the corresponding quotient sets modulo the componentwise action of $\mathrm{Int}(G)$.

Given $\mathbf{t} \in \mathcal{U}_r$, it is classical that $(\psi_{r,G})^{-1}(\mathbf{t})$ is in bijection with $\overline{\mathrm{ni}}(\mathbf{C})$. Furthermore, if we choose an ordering of the branch points $\mathbf{t}' = (t_1,...,t_r)$ in $\mathbf{t}$, $\overline{\mathrm{sni}}(\mathbf{C})$ is in bijection with $(\psi'_{r,G})^{-1}(\mathbf{t}')$. The correspondence is given by the monodromy action. We will sometimes say abusively that *a G-cover with branch point set $\mathbf{t} \in \mathcal{U}_r(\mathbb{C})$ is in $\overline{\mathrm{ni}}(\mathbf{C})$* when its isomorphism class has ramification type $[G, \mathbf{C}, \mathbf{t}]$ or that, *if an ordering $\mathbf{t}' = (t_1,...,t_r) \in \mathcal{U}^r(\mathbb{C})$ is given, a G-cover is in $\overline{\mathrm{sni}}(\mathbf{C})$* when C_i is the inertia canonical class associated with t_i for $i = 1,...,r$.

Since we are interested in G-covers defined over $\mathbb{R}$, we will always suppose the branch point divisor is real, that is consists of

$$(\mathrm{bp}) \left\{ \begin{array}{l} \text{- } r_1 \text{ real branch points } t_1,...,t_{r_1}, \text{ which we assume to be ordered : } t_1 < ... < t_{r_1}. \\ \text{- } r_2 \text{ complex conjugated pairs } \{z_i, \overline{z}_i\} \subset \mathbb{P}^1(\mathbb{C}) \backslash \mathbb{P}^1(\mathbb{R}). \text{ We will generally write} \\ z_i = t_{r_1+i},\ \overline{z}_i = t_{r+1-i},\ i = 1,...,r_2. \text{ We may also, if needed, order them} \\ \text{according to their real and imaginary parts.} \end{array} \right.$$

We now introduce the two following subsets of $\mathrm{sni}(\mathbf{C})$, which play an important part in the sequel :

– the set $\mathrm{sni}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$, which is the subset of $\mathrm{sni}(\mathbf{C})$ consisting of those $(g_1,...,g_r)$ in $\mathrm{sni}(\mathbf{C})$ verifying the additional condition :

(4) there exists $g_0 \in G$ such that
- $g_0(g_1...g_i)g_0^{-1} = (g_1...g_i)^{-1}$ for $i = 1,...,r_1 - 1$
- $g_0 g_{r_1+i} g_0^{-1} = g_{r+1-i}^{-1}$ and $g_0 g_{r+1-i} g_0^{-1} = g_{r_1+i}^{-1}$ for $i = 1,...,r_2$

– the set $\mathrm{sni}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$, which is the subset of $\mathrm{sni}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ consisting of those $(g_1,...,g_r)$ in) for which

(4)' in addition to (4) g_0 can be taken in $\mathrm{Inv}(G)$.

As above we write $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ and $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ for the corresponding quotient sets modulo the action of $\mathrm{Inn}(G)$. We have the following relation :

$$|\mathrm{sni}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)| = |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|[G : Z(G)]$$

We will also need the "Σ-versions", $\Sigma^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ and $\Sigma^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ of) and) which are defined by conditions (2), (3)', (4) and (2), (3)', (4)' respectively (that is we drop the generating condition (1)). It readily follows from the definitions that

$$|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)| = \frac{|\mathrm{sni}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|}{[G : Z(G)]} \leq \frac{|\Sigma^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|}{[G : Z(G)]}$$

So, computing the cardinality of the "Σ-versions", which is easier, gives an upper bound for $|)|$ and $|)|$. Moreover, in lots of situations $) = \Sigma^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ and $) = \Sigma^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ (see comment 3.2.2.3).

One of the main results of [DF94] is that, given $\mathbf{t} \in \mathcal{U}_r(\mathbb{R})$ ordered as is (bp), there exists an identification $(\Psi'_{r,G})^{-1}(\mathbf{t}') \simeq \overline{\text{sni}}(\mathbf{C})$ as recalled above such that $\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ is exactly the set of those G-covers in $\overline{\text{sni}}(\mathbf{C})$ with field of moduli contained in $\mathbb{R}$ and $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ the one of those G-covers in $\overline{\text{sni}}(\mathbf{C})$ which are defined over $\mathbb{R}$.

A complete proof of this statement can be found in [DF94]. We only recall here the main ideas. Let $\mathbf{t} \in \mathcal{U}_r(\mathbb{R})$ be a real branch point divisor ordered as in (bp). The first step consists in describing the action of complex conjugation c on the fundamental group $\pi_1^{\text{top}}(\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t}, t_0)$ of $\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t}$, which we denote by π^{top}. One can find $\Gamma_1, ..., \Gamma_r \in \pi^{\text{top}}$ which generate π^{top} with the single relation $\Gamma_1 ... \Gamma_r = 1$ and complex conjugation c acts on π^{top} by Hurwitz's formulas (see for instance [MMa99]) :

$$(*) \quad \begin{array}{ll} c.\Gamma_i = \Gamma_1 ... \Gamma_{i-1} \Gamma_i^{-1} (\Gamma_1 ... \Gamma_{i-1})^{-1} & \text{for } i = 1, ..., r_1 \\ c.\Gamma_{r_1+i} = \Gamma_{r+1-i}^{-1} & \text{for } i = 1, ..., r_2 \end{array}$$

We will denote by $\mathcal{C}$ the formal operator which maps each component Γ_i of an r-tuple $(\Gamma_1, ..., \Gamma_r)$ to the right hand side term of the formulas (*) (that is $c.\Gamma_i = \Gamma_i^{\mathcal{C}}$, $i = 1, ..., r$). Let $\Omega/\mathbb{C}(X)$ be the maximal algebraic extension of $\mathbb{C}(X)$ unramified outside $\mathbf{t}$; $\Omega/\mathbb{C}(X)$ is Galois with group $\text{Gal}(\Omega|\mathbb{C}(X)) =: \pi^{\text{alg}}$. And, by Riemann's Existence Theorem we get an isomorphism $\widehat{\pi^{\text{top}}} \xrightarrow{\sim} \pi^{\text{alg}}$, where $\widehat{\pi^{\text{top}}}$ is the profinite completion of π^{top} [S98].

The second step is an if and only if condition for the "descent from $\mathbb{C}$ to $\mathbb{R}$" : As the branch point divisor is real, $\Omega/\mathbb{R}(X)$ is Galois with group $\text{Gal}(\Omega|\mathbb{R}(X)) =: \pi_{\mathbb{R}}$. Furthermore, since $\mathbb{P}^1$ has real points, the short exact sequence (**) below splits and $\pi_{\mathbb{R}} \simeq \pi^{\text{alg}} \rtimes \mathbb{Z}/2\mathbb{Z}$. Now, if $K/\mathbb{C}(X)$ is the function field extension of an algebraic G-cover $f : X \to \mathbb{P}^1$ and $\psi : \pi^{alg} \to G$ is the corresponding epimorphism, f can be defined over $\mathbb{R}$ (so f is in)) if and only if there exists a map $\tilde{\psi}$ such that the following diagram commutes :

$$(**) \quad \begin{array}{ccccccccc} 1 & \longrightarrow & \pi^{\text{alg}} & \longrightarrow & \pi_{\mathbb{R}} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 1 \\ & & \psi \downarrow & \swarrow_{\exists \tilde{\psi}} & & & & & \\ & & G & & & & & & \end{array}$$

For all $\psi \in \text{Hom}(\pi^{\text{alg}}, G)$, write $g_i = \psi(\Gamma_i)$ i=1,...,r. Then, ψ extends to $\tilde{\psi} \in \text{Hom}(\pi^{\text{alg}} \rtimes \mathbb{Z}/2\mathbb{Z}, G)$ if and only if there exists $g_0 \in \text{Inv}(G)$ for which $g_0 g_i g_0 = g_i^{\mathcal{C}}$, $i = 1, ..., r$ (see [DF94] ; lemma 3.3). This provides the condition in the definition of).

Furthermore, if $f : X \to \mathbb{P}^1_{\mathbb{C}}$ corresponds to $(g_1, ..., g_r) \in \text{sni}(\mathbf{C})$, $f^c : X^c \to \mathbb{P}^1_{\mathbb{C}}$ corresponds to $(g_1^{\mathcal{C}}, ..., g_r^{\mathcal{C}}) \in \text{Sni}(\mathbf{C}^{\mathcal{C}}, G)$. So the set of all isomorphism classes of G-covers with field of moduli contained in $\mathbb{R}$ and branch points $\mathbf{t}'$ in $\overline{\text{sni}}(\mathbf{C})$ corresponds to $\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$. The extra condition $g_0^2 = 1$ that appears in) comes from Weil's cocycle condition [We].

Remark 3.1 If we fix $\mathbf{t} \in \mathcal{U}_r(\mathbb{R})$, the real points in the fiber $(\psi_{r,G})^{-1}(\mathbf{t})$ correspond to G-covers which have their field of moduli contained in $\mathbb{R}$. So, when working with moduli spaces, it is no longer posssible to distinguish between the G-covers defined over $\mathbb{R}$ and those which only have their field of moduli contained in $\mathbb{R}$. Some information is lost.

3.2 Statements and comments

3.2.1 Statements

Our main results are estimates of the cardinality of $|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$. What we actually compute is not $|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$ but $|\Sigma^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$, which is an upper bound for $|)|$. In the sequel, we will always assume $\Sigma^{\mathbb{R}}(\mathbf{C}; r_1, r_2) \neq \emptyset$.

We distinguish between the three following situations, depending on the branch points configuration :

- *General configuration* (R-C) : $r_1, r_2 \geq 0$.

and the two special cases :

- *Real configuration* (R) : $r_2 = 0$.
- *Complex pairs configuration* (C) : $r_1 = 0$.

Though (R) and (C) are only special cases of (R-C), it is easier to compute $|\Sigma^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$ in those two situations and the formulas obtained are much simpler than in the general case.

To make the formulas more legible, we will write :
- Z_i for the order of the centralizer of any element in the conjugacy class C_i.
- $\underline{\chi} \in \mathrm{Irr}(G)^r$ for any r-tuple $(\chi_1, ..., \chi_r) \in \mathrm{Irr}(G)^r$.
- $\underline{u} \in \mathrm{Inv}(G)^r$ for any r-tuple $(u_0, ..., u_{r-1}) \in \mathrm{Inv}(G)^r$.

We also fix $g_1, ..., g_r \in G$ with $g_i \in C_i$, $i = 1, ..., r$.

3.2.1.1 Statement of theorem 3.2 (configuration (R))

For all $\underline{\chi} \in \mathrm{Irr}(G)^r$ we set :

$$\mathbf{I}_{\underline{\chi}} = \sum_{\underline{u} \in \mathrm{Inv}(G)^r/G\cdot} \chi_1(u_0u_1)\chi_2(u_1u_2)\cdots\chi_r(u_{r-1}u_0)$$

where $\mathrm{Inv}(G)^r/G\cdot$ is the quotient set of the equivalence relation on $\mathrm{Inv}(G)^r$ which identifies two r-tuples $\underline{u}, \underline{u}' \in \mathrm{Inv}(G)^r$ if $(u_0, ..., u_{r-1}) = g.(u'_0, ..., u'_{r-1})$ for some $g \in G$. We also write :

$$\mathbf{n}^{\mathbb{R}}(\mathbf{C}; r, 0) = \frac{1}{Z_1 \cdots Z_r} \sum_{\underline{\chi} \in \mathrm{Irr}(G)^r} \chi_1(g_1)\cdots\chi_r(g_r)\, \mathbf{I}_{\underline{\chi}}$$

Theorem 3.2 (Real branch points) *We have*

$$|\Sigma^{\mathbb{R}}(\mathbf{C}; r, 0)| = \mathbf{n}^{\mathbb{R}}(\mathbf{C}; r, 0)$$

Remark 3.3 This formula can be improved to give exactly $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r, 0)|$

$$|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r, 0)| = \frac{|Z(G)|}{|G| Z_1 \cdots Z_r} \sum_{\underline{\chi} \in \mathrm{Irr}(G)^r} \chi_1(g_1)\cdots\chi_r(g_r)\, \mathbf{I}^*_{\underline{\chi}}$$

where $\mathbf{I}^*_{\underline{\chi}}$ is defined as $\mathbf{I}_{\underline{\chi}}$ with the only difference that the summation domain is the subset of $\mathrm{Inv}(G)^r/G\cdot$ of those r-tuples of representatives $\underline{u} \in \mathrm{Inv}(G)^r/G\cdot$ such that $G =< u_0u_1, ..., u_{r-2}u_{r-1} >$. This condition does not depend on the representive $\underline{u}$ since, if $g \cdot \underline{u} \in \mathrm{Inv}(G)^r$ for some $g \in G$ then $gu_igu_{i+1} = (gu_i)^{-1}gu_{i+1} = u_iu_{i+1},\ i = 0, ..., r-2$.

3.2.1.2 Statement of theorem 3.4 (configuration (C))

For any $\chi \in \mathrm{Irr}(G)$ and for any $g_0 \in G$ we denote the number of occurences of the trivial representation in the decomposition of $\chi|_{\mathrm{Cen}_G(g_0)}$ into a direct sum of irreducible linear representations by $\frac{\alpha_{\chi,g_0}}{|\mathrm{Cen}_G(g_0)|}$, that is (see [S98]) :

$$\alpha_{\chi,g_0} = \sum_{u \in \mathrm{Cen}_G(g_0)} \chi(u)$$

We also set :

$$\mathbf{A}_{\chi} = \sum_{g_0 \in \mathrm{Inv}(G)/Z(G)\cdot} \alpha_{\chi,g_0}$$

where $\mathrm{Inv}(G)/Z(G)\cdot$ is defined as $\mathrm{Inv}(G)^r/G\cdot$ above and :

$$\mathbf{n}^{\mathbb{R}}(\mathbf{C}; 0, s) = \frac{|C_1|\cdots|C_s|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1)\cdots\chi(g_s)}{\chi(1)^{s-1}}\, \mathbf{A}_{\chi}$$

Theorem 3.4 (Complex conjugate branch points) *We have*

$$|\Sigma^{\mathbb{R}}(\mathbf{C};0,s)| \leq \mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s)$$

with equality if $\Sigma^{\mathbb{R}}(\mathbf{C};0,s) = \mathrm{Sni}^{\mathbb{R}}(\mathbf{C};0,s)$

3.2.1.3 Statement of theorem 3.5 (configuration (R-C))

Our formula for the general case is more complicated. We set, for $r_1, r_2 > 0$ [1] :

$$\mathbf{n}_0^{\mathbb{R}}(\mathbf{C};r_1,r_2) = \sum_{\underline{\chi},\alpha,\beta,\underline{u}} \frac{\alpha(g_{r_1})\prod_{i=1}^{r_2}\beta(g_{r_1+i})}{\beta(1)^{r_2-1}} \prod_{i=1}^{r_1-1}(\chi_i(g_i)\chi_i(u_{i-1}u_i)) \sum_{x\in G}\alpha(u_{r_1-1}x^{-1}u_0x)\beta(x)$$

where the first summation is taken over all $\underline{\chi} \in \mathrm{Irr}(G)^{r_1-1}$, all $\alpha,\beta \in \mathrm{Irr}(G)$, all $\underline{u} \in \mathrm{Inv}(G)^{r_1}/\sim$ and $\sim$ is an equivalence relation on $\mathrm{Inv}(G)^{r_1}$ which we will define in 3.3.3. We also write

$$\mathbf{n}^{\mathbb{R}}(\mathbf{C};r_1,r_2) = \frac{|C_{r_1+1}|\cdots|C_{r_1+r_2}|}{|G|Z_1\cdots Z_{r_1}}\,\mathbf{n}_0^{\mathbb{R}}(\mathbf{C};r_1,r_2)$$

Theorem 3.5 (Real and complex conjugate branch points) *We have*

$$|\Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)| \leq \mathbf{n}^{\mathbb{R}}(\mathbf{C};r_1,r_2)$$

3.2.2 Comments

3.2.2.1

For a fixed $\mathbf{t} \in \mathcal{U}_r(\mathbb{R})$, the invariants of G and $\mathbf{C}$ on which the number of real G-covers in $\mathrm{sni}(\mathbf{C})$ depends clearly appear in Theorems 3.2, 3.4 and 3.5. Compared with Serre's formula for the basic rigidity criterion, one can notice the important part played by the involutions of G.

3.2.2.2

From a practical point of view, the terms depending on involutions make formulas in configurations (R) and (R-C) complicated for direct computations. On the contrary, $\mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s)$ is easy to compute once the character table of G and the centralizers of its involutions are known. When $\mathrm{Sni}^{\mathbb{R}}(\mathbf{C};0,s)$ is properly contained in $\Sigma^{\mathbb{R}}(\mathbf{C};0,s)$, $\mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s)$ only gives an upper bound for $|\Sigma^{\mathbb{R}}(\mathbf{C};0,s)|$, but we explain in the next comment how this difficulty can be handled.

3.2.2.3

One can proceed as in the classical rigidity context, generalizing the method given by Serre in [S98] to evaluate $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};r_1,r_2)|$ from $|\Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)|$:

1. Evaluate $|\Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)|$ by $\mathbf{n}^{\mathbb{R}}(\mathbf{C};r_1,r_2)$, using the character table of G.
2. Compute $|\Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)| - |\mathrm{sni}^{\mathbb{R}}(\mathbf{C};r_1,r_2)|$, by finding r-tuples $(g_1,...,g_r) = \underline{g}$ in $\Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)$ which do not generate G (to do this, try to find r-tuples the entries of which are contained in a maximal subgroup of G). But we are to be careful : when a r-tuple $\underline{g} \in \Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)-)$ has been found, the following should be done,
   – In situation (R) : $\underline{g}$ has to be counted once as in the classical rigidity method.

[1] For $r_2 = 0$ or $r_1 = 0$, the formulas are the ones given in 3.2 and 3.4

- In situation (C) : an extra difficuly arises from the computation of $\mathbf{A}_\chi$. One has to compute $\mathrm{Cen}_G(< g_1, ..., g_{2s} >)$ and notice that $\underline{g}$ corresponds to one single class of $\mathrm{Inv}(G)/\mathrm{Cen}_G(< g_1, ..., g_{2s} >)\cdot$. If this class can be written has the union of n classes of $\mathrm{Inv}(G)/Z(G)\cdot$, $\underline{g}$ has to be counted n times.
- Situation (R-C) has to be dealt with as situation (C).

The best situation is obviously when $\Sigma^{\mathbb{R}}(\mathbf{C}; r_1, r_2) =)$. This occurs for instance when each non trivial conjugacy class of G appears at least once in $\mathbf{C}$ or, more generally when $\mathbf{C}$ is *g-complete* [F95a], that is for any $g_i \in C_i$, $i = 1, ..., r$, we have $G =< g_1, ..., g_r >$. Then theorem 3.4 directly provides $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$. Moreover, if $\Sigma(\mathbf{C}, G) = \mathrm{sni}(\mathbf{C})$, one can also compute $|\overline{\mathrm{sni}}(\mathbf{C})|$ with Serre's formula [S98] and consequently the proportion of G-covers defined over $\mathbb{R}$: $|\overline{\mathrm{sni}}(\mathbf{C})|/|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$.

3.2.2.4

As in the rigidity context $|\overline{\mathrm{sni}}(\mathbf{C})|$ and $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$ provide some information about the field of moduli of the associated G-covers. For instance, the condition $|\overline{\mathrm{sni}}(\mathbf{C}; r_1, r_2)| = |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$ (under some technical assumptions) leads to G-covers defined over $\mathbb{Q}^{tr}$ (see 3.5.2 for some applications of this). Similarly, when $\overline{\mathrm{sni}}(\mathbf{C})$ contains a G-cover f defined over $\mathbb{Q}^{tr}$ and satisfying some other technical conditions, $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$ is an upper bound for the degree of a field extension $K/\mathbb{Q}$ over which f is defined :

Theorem 3.6 *[D95] Th. 4.1 For any $f \in \overline{\mathrm{sni}}(\mathbf{C})$, if*

1. $Z(G) =< 1 >$
2. *$\mathbb{Q}$-rationality condition :*
   - *configuration (R) : for all $n \geq 1$ such as $|G| \wedge n = 1$ $\forall 1 \leq i \leq r$ $C_i^n = C_i$*
   - *configuration (C) : for all $n \geq 1$ such as $|G| \wedge n = 1$ $\exists \tau \in < \{(i, 2r+1-i)\}_{1 \leq i \leq r} >$; $\forall 1 \leq i \leq 2r$ $C_i^n = C_{\tau(i)}$*
   - *configuration (R-C) : for all $n \geq 1$; $|G| \wedge n = 1$ $\forall 1 \leq i \leq r_1$ $C_i^n = C_i$ and there is $\tau \in < \{(r_1 + i, r_1 + 2r_2 + 1 - i)\}_{1 \leq i \leq r_2} >$ such as $\forall 1 \leq i \leq 2r_2$ $C_{r_1+i}^n = C_{\tau(r_1+i)}$*
3. *the G-cover f is defined over $\mathbb{Q}^{tr}$*
4. $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)| = 1$

then the G-cover f is defined over $\mathbb{Q}$.
If only conditions (1) to (3) are fulfilled, $|sni^{\mathbb{R}}(\mathbf{C}; r_1, r_2)|$ gives however an upper bound for the degree of the field if definition of f over $\mathbb{Q}$.

3.2.2.5

As in theorems 3.2, 3.4 and 3.5, one can give formulas for G-covers with field of moduli contained in $\mathbb{R}$. They can be proved exactly as the ones for G-covers defined over $\mathbb{R}$, using in the proofs, instead of condition (4), the equivalent one

(4)" there exists $g_0 \in G$ such that $g_0^2 \in Z(G)$ and
- $(g_0 g_1 ... g_i)^2 = g_0^2$ for $i = 1, ..., r_1 - 1$
- $g_0 g_{r_1+i} g_0^{-1} = g_{r+1-i}^{-1}$ for $i = 1, ..., r_2$

We write $Z(G)^{\frac{1}{2}} = \{g \in G | g^2 \in Z(G)\}$. We only state the results for configuration (R) and (C) :

1. *Configuration (R)* : Set $E_{r,G} = \{\underline{u} \in G^r \mid \exists g_0 \in Z(G)^{\frac{1}{2}} \ ; \ u_i^2 = g_0^2 \text{ for } i = 0, ..., r-1\}/G\cdot$ and

$$\begin{cases} \mathbf{I}_{\underline{\chi}}^{mod} = \sum_{\underline{u} \in E_{r,G}} \chi_1(u_0 u_1^{-1}) \chi_2(u_1 u_2^{-1}) \cdots \chi_r(u_{r-1} u_0^{-1}) \quad \text{for any } \underline{\chi} \in \mathrm{Irr}(G)^r \\ \mathbf{n}^{mod,\mathbb{R}}(\mathbf{C}; r, 0) = \dfrac{1}{Z_1 ... Z_r} \sum_{\underline{\chi} \in \mathrm{Irr}(G)^r} \chi_1(g_1) ... \chi_r(g_r) \, \mathbf{I}_{\underline{\chi}}^{mod} \end{cases}$$

   Then we get : $|\Sigma^{mod,\mathbb{R}}(\mathbf{C}; r, 0)| = \mathbf{n}^{mod,\mathbb{R}}(\mathbf{C}; r, 0)$.

2. *Configuration (C)* :Set

$$\begin{cases} \mathbf{A}_{\chi}^{mod} = \sum_{g_0 \in Z(G)^{\frac{1}{2}}/Z(G)\cdot} \alpha_{\chi, g_0} \quad \text{for any } \chi \in Irr(G) \\ \mathbf{n}^{mod,\mathbb{R}}(\mathbf{C}; 0, s) = \frac{|C_1| ... |C_s|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) ... \chi(g_s)}{\chi(1)^{s-1}} \mathbf{A}_{\chi}^{mod} \end{cases}$$

   Then we get : $|\Sigma^{mod,\mathbb{R}}(\mathbf{C}; 0, s)| \leq \mathbf{n}^{mod,\mathbb{R}}(\mathbf{C}; 0, s)$ with equality if $\Sigma^{mod,\mathbb{R}}(\mathbf{C}; 0, s) = \mathrm{Sni}^{mod,\mathbb{R}}(\mathbf{C}; 0, s)$.

As recalled in the introduction, one already has criteria to say when the field of moduli is the field of definition, for instance when $Z(G)$ is a direct submand of G (c.f. [CoH85] prop.2.8). Let us give an alternative proof of the weaker following result :

> For any finite group G such as $Z(G)$ is a direct submand of G, any G-cover with group G is defined over $\mathbb{R}$ if and only if its field of moduli is contained in $\mathbb{R}$.

So, suppose $G \simeq Z(G) \times H$, with $g_i = (z_i, h_i)$ we have $Z_i = |Z(G)| Z_{i,H}$ (where we set $|C_H(h_i)| = Z_{i,H}$) and $|C_i| = |\mathrm{Int}(H).h_i|$ for $i = 1, ..., r$ and we get :

1. Configuration (R) :
   $E_{r,G} \simeq E_{r,Z(G)} \times E_{r,H}$. But, as $Z(H) = \{1\}$ we have $E_{r,H} = \mathrm{Inv}(H)^r/H\cdot$. Likewise, as $Z(G)$ is abelian,

$$\begin{aligned} E_{r,Z(G)} &= \{(\zeta_0, ..., \zeta_{r-1}) \in Z(G)^r | \zeta_0^2 = ... = \zeta_{r-1}^2\}/Z(G)\cdot \\ &= \{(\zeta_0, ..., \zeta_{r-1}) \in Z(G)^r | \zeta_0^2 = ... = \zeta_{r-1}^2\}/Z(G)\cdot \\ &= \{(zu_0, ..., zu_{r-1}) | z \in Z(G), \ (u_0, ..., u_{r-1}) \in \mathrm{Inv}(Z(G))^r\}/Z(G)\cdot \\ &\simeq \mathrm{Inv}(Z(G))/Z(G)\cdot \end{aligned}$$

   so $E_{r,G} \simeq \mathrm{Inv}(Z(G))/Z(G)\cdot \times \mathrm{Inv}(H)^r/H\cdot \simeq \mathrm{Inv}(G)^r/G\cdot$ which provides $\mathbf{I}_{\underline{\chi}}^{\mathbf{mod}} = \mathbf{I}_{\underline{\chi}}$ for any $\underline{\chi} \in \mathrm{Irr}(G)^r$ and, as a result, $\mathbf{n}^{mod,\mathbb{R}}(\mathbf{C}; r, 0) = \mathbf{n}^{\mathbb{R}}(\mathbf{C}; r, 0)$ becomes :

2. Configuration (C) :
   $Z(G)^{\frac{1}{2}} = Z(G) \times \mathrm{Inv}(H)$ so $Z(G)^{\frac{1}{2}}/Z(G)\cdot . \simeq \mathrm{Inv}(H)$ and for all $\chi^Z \in \mathrm{Irr}(Z(G))$, for all $\chi^H \in \mathrm{Irr}(H)$, with $\chi = \chi^Z \otimes \chi^H$

$$\begin{aligned} A_{\chi}^{mod} &= \sum_{h_0 \in \mathrm{Inv}(H)} \sum_{(z,u) \in Z(G) \times \mathrm{Cen}_H(h_0)} \chi^Z(z) \chi^H(u) \\ &= \underbrace{\sum_{z \in Z(G)} \chi^Z(z)}_{= <\chi^Z, \chi_1^Z>} \sum_{h_0 \in \mathrm{Inv}(H)} \sum_{u \in \mathrm{Cen}_H(h_0)} \chi^H(u) \\ &= |Z(G)| A_{\chi^H} \text{ if } \chi^Z = \chi_1^Z, \ 0 \text{ otherwise} \end{aligned}$$

So

$$\mathbf{n}^{mod,\,\mathbb{R}}(\underline{C};0,s)=\frac{|C_1|...|C_s|}{|H|}\sum_{\chi\in\mathrm{Irr}(H)}\frac{\chi(h_1)...\chi(h_s)}{\chi(1)^{s-1}}A_\chi$$

and once again the above argument applied to $\mathbf{n}^{\mathbb{R}}(\underline{C};0,s)$ gives $\mathbf{n}^{\mathbb{R}}(\underline{C};0,s)=\mathbf{n}^{mod\,\mathbb{R}}(\underline{C};0,s)$.

In fact, given a G-cover f with field of moduli k_m, there is a cohomological obstruction $\omega(f)\in \mathrm{H}^2(k_m,Z(G))$ (where $Z(G)$ acts on k_m trivially) for the field of moduli to be a field of definition (see for instance [W02]). $\omega(f)$ is functorial in k_m and in particular, $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C};r_1,r_2)=sni^{\mathbb{R}}(\mathbf{C};r_1,r_2)$ if and only if for all f in $\overline{\mathrm{sni}}(\mathbf{C})$ $\omega(f)|_{\mathbb{R}}=0$.

3.3 Proofs

We give the proofs of theorems 3.2 and 3.4 in details ; for theorem 3.5, we just explain the main changes, in particular we give the description of $\Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)$ we use so as to explain the definition of $\sim$.

Following Serre's method, we are going to compute $|\Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)|$ using the function

$$\epsilon=\frac{1}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)\chi$$

which is 1 on 1_G and 0 elsewhere.

First, we prove the following technical lemma, which we will use in the sequel.

Lemma 3.7 *Given a finite group G, for any irreducible character $\chi\in\mathrm{Irr}(G)$ and for any $g_1,...,g_n,u,v\in G$ we have :*

$$\sum_{(\gamma_1,...,\gamma_n)\in G}\chi(ug_1^{\gamma_1}\cdots g_n^{\gamma_n}v)=\frac{|G|^n\prod_{i=1}^n\chi(g_i)}{\chi(1)^n}\chi(uv)$$

Proof. Let $R:G\to\mathrm{GL}(V)$ be a linear irreducible representation of G with character χ. Then

$$\sum_{\underline{\gamma}\in G}R(ug_1^{\gamma_1}\cdots g_n^{\gamma_n}v)=R(u)\left(\sum_{\gamma_1\in G}R(g_1^{\gamma_1})\cdots\sum_{\gamma_n\in G}R(g_n^{\gamma_n})\right)R(v)$$

But for any $g,h\in G$

$$\sum_{\gamma\in G}R(g^\gamma)R(h)=\sum_{\gamma\in G}R(g^\gamma h)=\sum_{\gamma\in G}R(hg^{h^{-1}\gamma})=R(h)\sum_{\gamma\in G}R(g^{h^{-1}\gamma})=R(h)\sum_{\gamma\in G}R(g^\gamma)$$

So, according to Schur's lemma (cf. for instance [S98] proposition 4 chap.2) :

$$\sum_{\gamma\in G}R(g^\gamma)=\lambda\mathrm{Id}_V\text{ with }\lambda=\frac{1}{\dim V}\mathrm{Tr}(\sum_{\gamma\in G}R(g^\gamma))=\frac{|G|}{\chi(1)}\chi(g)$$

Consequently we get

$$\sum_{\gamma_1\in G}R(g_1^{\gamma_1})\cdots\sum_{\gamma_n\in G}R(g_n^{\gamma_n})=\frac{|G|^n\prod_{i=1}^n\chi(g_i)}{\chi(1)^n}\mathrm{Id}_V$$

so,

$$\sum_{\gamma\in G}R(ug_1^{\gamma_1}\cdots g_n^{\gamma_n}v)=\frac{|G|^n\prod_{i=1}^n\chi(g_i)}{\chi(1)^n}R(uv)$$

And, taking traces yields the formula in lemma 4.10. □

3.3.1 Real branch points

We first note that conditions (2) and (4)' in the definition of $\Sigma^{\mathbb{R}}(\mathbf{C}; r, 0)$ are equivalent to

$$(*)\ \exists g_0 \in G \text{ such that } (g_0 g_1 \cdots g_i)^2 = 1,\ i = 1, ..., r-1 \text{ and } g_1 \cdots g_r = 1$$

which in turn is equivalent to

$$(**)\ g_1 = u_0 u_1, ..., g_{r-1} = u_{r-2} u_{r-1} \text{ and } g_r = u_{r-1} u_0 \text{ for some } (u_0, ..., u_{r-1}) \in \mathrm{Inv}(G)^r$$

(just take $u_i = g_0 \cdots g_i$, $i = 0, ..., r-1$). In the the rest of the paragraph we will use the r-cycle $c = (0, ..., r-1) \in S_r$ to shorten the formulas. For instance (**) can be re-written $g_{i+1} = u_i u_{c(i)}$, $i = 0, ..., r-1$

Now, fix $g_1, ..., g_r \in G$ with $g_i \in C_i$, $i = 1, ..., r$ and consider the set $E_{\underline{g}}$ of those r-tuples $\underline{\gamma} = (\gamma_1, ..., \gamma_r) \in G^r$ such that $g_{i+1}^{\gamma_{i+1}} = u_i u_{c(i)}$, $i = 0, ..., r-1$ for some $(u_0, ..., u_{r-1}) \in \mathrm{Inv}(G)^r$. The correspondence $\underline{\gamma} \to (g_1^{\gamma_1}, ..., g_r^{\gamma_r})$ provides a surjective map $E_{\underline{g}} \to \Sigma^{\mathbb{R}}(\mathbf{C}; r, 0)$. Note then that two distinct r-tuples $\underline{\gamma}, \underline{\gamma}' \in G^r$ have the same image if and only if $\gamma_i^{-1}\gamma_i' \in \mathrm{Cen}_G(g_i)$, $i = 1, ..., r$. Consequently

$$|\Sigma^{\mathbb{R}}(\mathbf{C}; r, 0)| = \frac{|E_{\underline{g}}|}{Z_1 \cdots Z_r}$$

which reduces the problem to computing $|E_{\underline{g}}|$.

We proceed this way : for each $(\gamma_1, ..., \gamma_r) \in G^r$, we check for every r-tuple $(u_0, ...u_{r-1}) \in \mathrm{Inv}(G)^r$ whether $g_{i+1}^{\gamma_{i+1}} = u_i u_{c(i)}$, $i = 0, ..., r-1$, that is whether

$$\prod_{i=0}^{r-1} \epsilon(u_i g_{i+1}^{\gamma_{i+1}} u_{c(i)}) = 1$$

However, we should take into account that for a given $\underline{\gamma} \in G^r$, distinct r-tuples $\underline{u}, \underline{u}' \in \mathrm{Inv}(G)^r$ can satisfy $g_{i+1}^{\gamma_{i+1}} = u_i u_{c(i)}$, $i = 0, ..., r-1$; this is equivalent to the condition $u_0 u_0' = u_1 u_1' = ... = u_{r-1} u_{r-1}'$, which can also be written $G \cdot (u_0, ..., u_{r-1}) = G \cdot (u_0', ..., u_{r-1}')$, where G acts on G^r by left translation. This defines the equivalence relation $G\cdot$ on $\mathrm{Inv}(G)^r$ which appears in the statement of Theorem 3.2.

Putting these remarks together we get :

$$\begin{aligned} |E_{\underline{g}}| = \sum_{\substack{\underline{\gamma} \in G^r \\ \underline{u} \in \mathrm{Inv}(G)^r/G\cdot}} \prod_{i=0}^{r-1} \epsilon(u_i g_{i+1}^{\gamma_{i+1}} u_{c(i)}) &= \sum_{\underline{u} \in \mathrm{Inv}(G)^r/G\cdot} \left(\sum_{\underline{\gamma} \in G} \prod_{i=0}^{r-1} \epsilon(u_i g_{i+1}^{\gamma_{i+1}} u_{c(i)}) \right) \\ &= \sum_{\underline{u} \in \mathrm{Inv}(G)^r/G\cdot} \left(\prod_{i=0}^{r-1} \sum_{\gamma \in G} \epsilon(u_i g_{i+1}^{\gamma} u_{c(i)}) \right) \end{aligned}$$

Using the formula $\epsilon = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$ and lemma 4.10 we obtain, for $i = 0, ..., r-1$ and $\underline{u} \in \mathrm{Inv}(G)^r$:

$$\begin{aligned} \sum_{\gamma \in G} \epsilon(u_i g_{i+1}^{\gamma} u_{c(i)}) &= \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \sum_{\gamma \in G} \chi(u_i g_{i+1}^{\gamma} u_{c(i)}) \\ &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(g_{i+1}) \chi(u_i u_{c(i)}) \end{aligned}$$

Substituting this back in the previous formula leads to the announced result. Note the generating condition $G =< u_0 u_1, ..., u_{r-2} u_{r-1} >$ can be taken into account to get $\mathrm{Sni}^{\mathbb{R}}(\mathbf{C}; r, 0)$: the only change is then that, in the sums above, the r-tuples $\underline{u}$ should run over the subset of $\mathrm{Inv}(G)^r/G\cdot$ of those r-tuples $\underline{u}$ of representatives satisfying this extra generating condition.This yields remark 3.3.

□

3.3.2 Complex conjugate branch points :

This time note that conditions (2) and (4)' in the definition of $\Sigma^{\mathbb{R}}(\mathbf{C};0,s)$ are equivalent to

(*) there exists $g_0 \in \mathrm{Inv}(G)$ such that $g_0\ g_i\ g_0\ g_{2s+1-i} = 1,\ i = 1,...,s$ and $g_1 \cdots g_{2s} = 1$

which in turn is equivalent to

(**) there exists $g_0 \in \mathrm{Inv}(G)$ such that $g_0\ g_i\ g_0\ g_{2s+1-i} = 1,\ i = 1,...,s$ and $[g_1 \cdots g_s, g_0] = 1$
(where we write $[u,v]$ for the commutator $uvu^{-1}v^{-1}$ of $u,v \in G$).

As above, fix $g_1,...,g_{2s} \in G$ with $g_i \in C_i,\ i = 1,...,2s$ and consider the set $E_{\underline{g}}$ of those $2s$-tuples $\underline{\gamma} = (\gamma_1,...,\gamma_{2s}) \in G^r$ such that $g_0\ g_i^{\gamma_i}\ g_0\ g_{2s+1-i}^{\gamma_{2s+1-i}} = 1$ for $i = 1,...,s$ and $[g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0] = 1$ (or, equivalently $g_1^{\gamma_1} \cdots g_s^{\gamma_s} \in \mathrm{Cen}_G(g_0)$) for some $g_0 \in \mathrm{Inv}(G)$. Again, the correspondence $\underline{\gamma} \to (g_1^{\gamma_1},...,g_{2s}^{\gamma_{2s}})$ provides a surjective map $E_{\underline{g}} \to \Sigma^{\mathbb{R}}(\mathbf{C};0,s)$ and two distinct $2s$-tuples $\underline{\gamma},\underline{\gamma}' \in G^r$ have the same image if and only if $\gamma_i^{-1}\gamma_i' \in \mathrm{Cen}_G(g_i)$ for $i = 1,...,2s$. Consequently

$$|\Sigma^{\mathbb{R}}(\mathbf{C};0,s)| = \frac{|E_{\underline{g}}|}{Z_1 \cdots Z_{2s}}$$

which reduces the problem to computing $|E_{\underline{g}}|$.

We proceed this way : for each $(\gamma_1,...,\gamma_{2s}) \in G^{2s}$, we check for every $g_0 \in \mathrm{Inv}(G)$ whether $g_0\ g_i^{\gamma_i}\ g_0\ g_{2s+1-i}^{\gamma_{2s+1-i}} = 1,\ i = 1,...,2s$ and $[g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0] = 1$, that is whether

$$\epsilon([g_1^{\gamma_1}...g_s^{\gamma_s}, g_0]) \prod_{i=1}^{s} \epsilon(g_0 g_i^{\gamma_i} g_0 g_{2s+1-i}^{\gamma_{2s+1-i}}) = 1$$

As in 3.3.1 note that for a given $\underline{\gamma} \in G^r$, distinct involutions $g_0, g_0' \in \mathrm{Inv}(G)$ can satisfy condition (**). This is equivalent to the condition $g_0 g_0' \in \mathrm{Cen}_G(g_1^{\gamma_1},...,g_s^{\gamma_s})$ or $\mathrm{Cen}_G(g_1^{\gamma_1},...,g_s^{\gamma_s}).g_0 = \mathrm{Cen}_G(g_1^{\gamma_1},...,g_s^{\gamma_s}).g_0'$. And, as $Z(G) < \mathrm{Cen}_G(g_1^{\gamma_1},...,g_s^{\gamma_s})$, the preceeding equivalent conditions are implied by $Z(G) \cdot g_0 = Z(G) \cdot g_0'$ (see remark 3.8), where $\mathrm{Cen}_G(g_1^{\gamma_1},...,g_s^{\gamma_s})$ and $Z(G)$ act on G by left translation. Here again this gives the equivalence relation $Z(G)\cdot$ on $\mathrm{Inv}(G)$ which appears in the statement of theorem 3.4.

Putting these remarks together we get :

$$\begin{aligned}
|E_{\underline{g}}| &\leq \sum_{\substack{\underline{\gamma} \in G^{2s} \\ g_0 \in \mathrm{Inv}(G)/Z(G)\cdot}} \epsilon([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0]) \prod_{i=1}^{s} \epsilon(g_0\ g_i^{\gamma_i}\ g_0\ g_{2s+1-i}^{\gamma_{2s+1-i}}) \\
&\leq \sum_{\substack{(\gamma_1,...,\gamma_s) \in G \\ g_0 \in \mathrm{Inv}(G)/Z(G)\cdot}} \epsilon([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0]) \sum_{(\gamma_{s+1},...,\gamma_{2s}) \in G} \prod_{i=1}^{s} \epsilon(g_0\ g_i^{\gamma_i}\ g_0\ g_{2s+1-i}^{\gamma_{2s+1-i}}) \\
&\leq \sum_{\substack{(\gamma_1,...,\gamma_s) \in G \\ g_0 \in \mathrm{Inv}(G)/Z(G)\cdot}} \epsilon([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0]) \prod_{i=1}^{s} \sum_{\gamma \in G} \epsilon(g_0\ g_i^{\gamma_i}\ g_0\ g_{2s+1-i}^{\gamma})
\end{aligned}$$

As before lemma 4.10 combined with the formula defining ϵ gives :

$$\begin{aligned}
\prod_{i=1}^{s} \sum_{\gamma \in G} \epsilon(g_0 g_i^{\gamma_i} g_0 g_{2s+1-i}^{\gamma}) &= \prod_{i=1}^{s} \sum_{\chi \in \mathrm{Irr}(G)} \chi(g_0 g_i^{\gamma_i} g_0)\chi(g_{2s+1-i}) \\
&= \prod_{i=1}^{s} \sum_{\chi \in \mathrm{Irr}(G)} \chi(g_i)\chi(g_{2s+1-i})
\end{aligned}$$

Hence we have now :

$$|E_{\underline{g}}| \leq \left(\sum_{\substack{(\gamma_1,...,\gamma_s)\in G \\ g_0 \in \mathrm{Inv}(G)/Z(G).}} \epsilon([g_1^{\gamma_1}\cdots g_s^{\gamma_s}, g_0]) \right) \left(\prod_{i=1}^{s} \sum_{\chi\in\mathrm{Irr}(G)} \chi(g_i)\chi(g_{2s+1-i}) \right)$$

Noting that, for all $g_0 \in \mathrm{Inv}(G)$, $[u,v]=1$ if and only if $u \in \mathrm{Cen}_G(v)$

$$\begin{aligned} \sum_{(\gamma_1,...,\gamma_s)\in G} \epsilon([g_1^{\gamma_1}\cdots g_s^{\gamma_s}, g_0]) &= \sum_{u\in\mathrm{Cen}_G(g_0)} \sum_{(\gamma_1,...,\gamma_s)\in G} \epsilon(g_1^{\gamma_1}\cdots g_s^{\gamma_s}u) \\ &= \sum_{u\in\mathrm{Cen}_G(g_0)} \frac{1}{|G|} \sum_{\chi\in\mathrm{Irr}(G)} \chi(1) \sum_{(\gamma_1,...,\gamma_s)\in G} \chi(g_1^{\gamma_1}\cdots g_s^{\gamma_s}u) \end{aligned}$$

So, using lemma 4.10 again,

$$\begin{aligned} \sum_{(\gamma_1,...,\gamma_s)\in G} \epsilon([g_1^{\gamma_1}\cdots g_s^{\gamma_s}, g_0]) &= |G|^{s-1} \sum_{u\in\mathrm{Cen}_G(g_0)} \sum_{\chi\in\mathrm{Irr}(G)} \frac{\prod_{i=1}^{s}\chi(g_i)}{\chi(1)^{s-1}}\chi(u) \\ &= |G|^{s-1} \sum_{\chi\in\mathrm{Irr}(G)} \frac{\prod_{i=1}^{s}\chi(g_i)}{\chi(1)^{s-1}} \sum_{u\in\mathrm{Cen}_G(g_0)} \chi(u) \end{aligned}$$

We recognize here $\alpha_{\chi,g_0} = \sum_{u\in\mathrm{Cen}_G(g_0)}\chi(u)$. Finally, we get :

$$|E_{\underline{g}}| \leq |G|^{s-1} \left(\prod_{i=1}^{s} \sum_{\chi\in\mathrm{Irr}(G)} \chi(g_i)\chi(g_{2s+1-i}) \right) \left(\sum_{\chi\in\mathrm{Irr}(G)} \frac{\prod_{i=1}^{s}\chi(g_i)}{\chi(1)^{s-1}} \mathbf{A}_\chi \right)$$

To end the proof, just recall that we have assumed $|\Sigma^{\mathbb{R}}(\mathbf{C};0,s)| \neq \emptyset$, this implies in particular that $C_i = C_{2s+i-1}^{-1}$ for $i=1,...,s$, so $Z_i = Z_{2s+1-i}$ and $\chi(g_i)\chi(g_{2s+1-i}) = |\chi(g_i)|^2$ whence

$$\sum_{\chi\in\mathrm{Irr}(G)} \chi(g_i)\chi(g_{2s+1-i}) = \sum_{\chi\in\mathrm{Irr}(G)} |\chi(g_i)|^2 = Z_i$$

for $i=1,...,s$, which leads to the announced result.

□

Remark 3.8 We only get an upper bound for $|\Sigma^{\mathbb{R}}(\mathbf{C};0,s)|$ because of the inclusions, which may be proper, $Z(G) < \mathrm{Cen}_G(g_1^{\gamma_1},...,g_s^{\gamma_s})$. But if $\Sigma^{\mathbb{R}}(\mathbf{C};0,s) = \mathrm{Sni}^{\mathbb{R}}(\mathbf{C};0,s)$, these inclusions become equalities and $|\Sigma^{\mathbb{R}}(\mathbf{C};0,s)| = |\mathrm{Sni}^{\mathbb{R}}(\mathbf{C};0,s)|$.

3.3.3 Real and complex conjugate branch points

The method consists in rewriting conditions (2) and (4)' as in the two preceeding sections but replacing conditions $g_1\cdots g_{r_1}=1$ and $g_{r_1+1}\cdots g_{r_1+2r_2}=1$ by the weaker one $g_1\cdots g_{r_1}g_{r_1+1}\cdots g_{r_1+2r_2}=1$. So, in the general situation conditions (2) and (4)' are equivalent to

$$(*) \text{ there exists } g_0 \in \mathrm{Inv}(G) \text{ such that } \begin{cases} g_1\cdots g_r = 1 \\ (g_0g_1\cdots g_i)^2 = 1,\ i=1,...,r_1-1 \\ g_0\ g_{r_1+i}\ g_0\ g_{r+1-i} = 1,\ i=1,...,r_2 \end{cases}$$

which in turn is equivalent to

$$(**) \text{ there exists } (u_0,...,u_{r_1-1}) \in \mathrm{Inv}(G)^{r_1} \text{ such that } \begin{cases} u_0u_{r_1-1}g_{r_1}[g_{r_1+1}\cdots g_{r_1+r_2}, u_0] = 1 \\ g_{i+1} = u_iu_{i+1},\ i=0,...,r_1-2 \\ u_0\ g_{r_1+i}\ u_0\ g_{r+1-i} = 1,\ i=1,...,r_2 \end{cases}$$

$(***)$ there exists $(u_0,...,u_{r_1-1}) \in \mathrm{Inv}(G)^{r_1}$ such that

$$\begin{array}{l}\exists x \in G \text{ such that } g_{r_1+1}\cdots g_{r_1+r_2} = x \text{ and } u_{r_1-1}\ g_{r_1}\ x\ u_0\ x^{-1} = 1\\ g_{i+1} = u_i u_{i+1},\ i = 0,...,r_1-2\\ u_0\ g_{r_1+i}\ u_0\ g_{r_1+2r_2+1-i} = 1,\ i = 1,...,r_2\end{array}$$

We still fix $g_1,...,g_r \in G$ with $g_i \in C_i$, $i = 1,...,r$ and consider the set $E_{\underline{g},r_1,r_2}$ of those r-tuples $\underline{\gamma} = (\gamma_1,...,\gamma_r) \in G^r$ such that $u_0 u_{r_1-1} g_{r_1}^{\gamma_{r_1}} [g_{r_1+1}^{\gamma_{r_1+1}}\cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}}, u_0] = 1$ and $g_{i+1}^{\gamma_{i+1}} = u_i u_{i+1}$ for $i = 0,...,r_1-2$, $u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r+1-i}^{\gamma_{r+1-i}} = 1$, $i = 1,...,r_2$. As above

$$|\Sigma^{\mathbb{R}}(\mathbf{C};0,s)| = \frac{|E_{\underline{g},r_1,r_2}|}{Z_1\cdots Z_r}$$

which once again reduces the problem to computing $|E_{\underline{g},r_1,r_2}|$. That is, for each $\underline{\gamma} = (\gamma_1,...,\gamma_r) \in G^r$, we check for every $\underline{u} = (u_0,...,u_{r_1-1}) \in \mathrm{Inv}(G)^{r_1}$ whether $g_{i+1}^{\gamma_{i+1}} = u_i u_{i+1}$, $i = 0,...,r_1-2$, $u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r_1+2r_2+1-i}^{\gamma_{r_1+r_2+1-i}} = 1$, $i = 1,...,r_2$ and $u_0 u_{r_1-1} g_{r_1}^{\gamma_{r_1}} [g_{r_1+1}^{\gamma_{r_1+1}}\cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}}, u_0] = 1$, that is whether

$$\prod_{i=0}^{r_1-1} \epsilon(u_i g_{i+1}^{\gamma_{i+1}} u_{i+1}) \prod_{i=1}^{r_2} \epsilon(u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r+1-i}^{\gamma_{r+1-i}}) \epsilon(u_0 u_{r_1-1} g_{r_1}^{\gamma_{r_1}} [g_{r_1+1}^{\gamma_{r_1+1}}\cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}}, u_0]) = 1$$

Now, the introduction of $\sim$ derives from the usual remarks about counting exactly one time each element $\underline{\gamma} \in E_{\underline{g},r_1,r_2}$:
- for all $(\gamma_1,...,\gamma_{r_1-1}) \in G^{r_1-1}$, $\underline{u},\underline{u}' \in \mathrm{Inv}(G)^{r_1}$, the condition

$$u_i g_{i+1}^{\gamma_{i+1}} u_{i+1} = 1 = u_i' g_{i+1}^{\gamma_{i+1}} u_{i+1}',\ i = 0,...,r_1-1$$

is equivalent to $u_0 u_0' = u_1 u_1' = ... = u_{r_1-1} u_{r_1-1}'$ which can also be written $G.(u_0,...u_{r_1-1}) = G.(u_0',...u_{r_1-1}')$, where G acts on G^{r_1} by left translation.
- for all $(\gamma_{r_1+1},...,\gamma_r) \in G^{2r_2}$, $u_0, u_0' \in \mathrm{Inv}(G)$ the condition

$$u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 = (g_{r+1-i}^{\gamma_{r+1-i}})^{-1} = u_0' g_{r_1+i}^{\gamma_{r_1+i}} u_0',\ i = 1,...,r_2$$

is equivalent to

$$u_0 u_0') \in \mathrm{Cen}_G(g_{r_1+1}^{\gamma_{r_1+1}},...,g_{r_1+r_2}^{\gamma_{r_1+r_2}})$$

that is $\mathrm{Cen}_G(g_{r_1+1}^{\gamma_{r_1+1}},...,g_{r_1+r_2}^{\gamma_{r_1+r_2}})\cdot u_0 = \mathrm{Cen}_G(g_{r_1+1}^{\gamma_{r_1+1}},...,g_{r_1+r_2}^{\gamma_{r_1+r_2}})\cdot u_0'$ which is implied by

$$N\cdot u_0 = N\cdot u_0'$$

where $N = \mathrm{Cen}_G(C_{r_1+1},...,C_{r_1+r_2})$ is the centralizer of the subgroup generated by the conjugacy classes of $g_{r_1+1},...,g_{r_1+r_2}$ and both $\mathrm{Cen}_G(g_{r_1+1}^{\gamma_{r_1+1}},...,g_{r_1+r_2}^{\gamma_{r_1+r_2}})$ and N act on G by left translation.

Hence, for all $\underline{\gamma} = (\gamma_1,...,\gamma_{r_1-1}) \in G^{r_1-1}$ let $\sim_{\underline{\gamma}}$ the relation defined on $\mathrm{Inv}(G)^{r_1}$, by :
for all $\underline{u},\underline{u}' \in \mathrm{Inv}(G)^{r_1}$,

$$\begin{array}{rcl}\underline{u} \sim_{\underline{\gamma}} \underline{u}' & \iff & \mathrm{Cen}_G(g_{r_1+1}^{\gamma_{r_1+1}},...,g_{r_1+r_2}^{\gamma_{r_1+r_2}})\cdot u_0 = \mathrm{Cen}_G(g_{r_1+1}^{\gamma_{r_1+1}},...,g_{r_1+r_2}^{\gamma_{r_1+r_2}})\cdot u_0'\\ & & \text{and } G\cdot(u_0,...,u_{r_1-1}) = G\cdot(u_0',...,u_{r_1-1}')\end{array}$$

and write $\sim$ for the relation one gets replacing $\mathrm{Cen}_G(g_{r_1+1}^{\gamma_{r_1+1}},...,g_{r_1+r_2}^{\gamma_{r_1+r_2}})$ by $\mathrm{Cen}_G(N)$ in the definition above. These relations are equivalence relations on $\mathrm{Inv}(G)^{r_1}$ and we obtain formula $\mathbf{n}^{\mathbb{R}}(\mathbf{C};r_1,r_2)$ in theorem 3.5 by summing on the equivalence classes $\mathrm{Inv}(G)^{r_1}/\sim$.

Remark 3.9 When for all $\underline{\gamma} = (\gamma_1, ..., \gamma_{r_1-1}) \in G$, $N = \mathrm{Cen}_G(g_{r_1+1}^{\gamma_{r_1+1}}, ..., g_{r_1+r_2}^{\gamma_{r_1+r_2}})$, the inequality in Theorem 3.5 becomes an equality

$$\begin{aligned}
|E_{\underline{g},r_1,r_2}| &= \sum_{\substack{\underline{\gamma}\in G^r \\ \underline{u}\in \mathrm{Inv}(G)^r/\sim_{\underline{\gamma}}}} \prod_{i=1}^{r_1-1} \epsilon(u_i g_i^{\gamma_i} u_{i+1}) \prod_{i=1}^{r_2} \epsilon(u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r_1+2r_2+1-i}^{\gamma_{r_1+2r_2+1-i}}) \\
&\quad \times \epsilon(u_0 u_{r_1-1} g_{r_1}^{\gamma_{r_1}} [g_{r_1+1}^{\gamma_{r_1+1}} \cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}}, u_0]) \\
&\leq \sum_{\substack{\underline{\gamma}\in G^r \\ \underline{u}\in \mathrm{Inv}(G)^r/\sim}} \prod_{i=1}^{r_1-1} \epsilon(u_i g_i^{\gamma_i} u_{i+1}) \prod_{i=1}^{r_2} \epsilon(u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r_1+2r_2+1-i}^{\gamma_{r_1+2r_2+1-i}}) \\
&\quad \times \epsilon(u_0 u_{r_1-1} g_{r_1}^{\gamma_{r_1}} [g_{r_1+1}^{\gamma_{r_1+1}} \cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}}, u_0])
\end{aligned}$$

First we reorder the sum to isolate terms that can be computed separately :

$$\begin{aligned}
|E_{\underline{g},r_1,r_2}| &\leq \sum_{\underline{u}\in \mathrm{Inv}(G)^{r_1}/\sim} \sum_{\gamma_{r_1},...,\gamma_{r_1+r_2}\in G} \sum_{\gamma_{r_1+r_2+1},...,\gamma_{r_1+2r_2}\in G} \prod_{i=1}^{r_2} \epsilon(u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r_1+2r_2+1-i}^{\gamma_{r_1+2r_2+1-i}}) \\
&\quad \times \epsilon(u_0 u_{r_1-1} g_{r_1}^{\gamma_{r_1}} [g_{r_1+1}^{\gamma_{r_1+1}} \cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}}, u_0]) \sum_{(\gamma_1,...,\gamma_{r_1-1})\in G} \prod_{1\leq i\leq r_1-1} \epsilon(u_i g_i^{\gamma_i} u_{i+1}) \\
&\leq \sum_{\underline{u}\in \mathrm{Inv}(G)^{r_1}/\sim} \sum_{\gamma_{r_1+1},...,\gamma_{r_1+r_2}} \sum_{\gamma_{r_1}\in G} \epsilon(u_0 u_{r_1-1} g_{r_1}^{\gamma_{r_1}} [g_{r_1+1}^{\gamma_{r_1+1}} \cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}}, u_0]) \\
&\quad \times \sum_{\gamma_{r_1+r_2+1},...,\gamma_{r_1+2r_2}\in G} \prod_{1\leq i\leq r_2} \epsilon(u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r_1+2r_2+1-i}^{\gamma_{r_1+2r_2+1-i}}) \sum_{(\gamma_1,...,\gamma_{r_1-1})\in G} \prod_{1\leq i\leq r_1-1} \epsilon(u_i g_i^{\gamma_i} u_{i+1}) \\
&= \sum_{\underline{u}\in \mathrm{Inv}(G)^{r_1}/\sim} \sum_{\gamma_{r_1+1},...,\gamma_{r_1+r_2}} \sum_{\gamma_{r_1}\in G} \epsilon(u_0 u_{r_1-1} g_{r_1}^{\gamma_{r_1}} [g_{r_1+1}^{\gamma_{r_1+1}} \cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}}, u_0]) \\
&\quad \times \prod_{1\leq i\leq r_2} \sum_{\gamma_{r_1+2r_2+1-i}\in G} \epsilon(u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r_1+2r_2+1-i}^{\gamma_{r_1+2r_2+1-i}}) \prod_{1\leq i\leq r_1-1} \sum_{\gamma_i\in G} \epsilon(u_i g_i^{\gamma_i} u_{i+1})
\end{aligned}$$

Now we compute from right to left, eliminating the conjugacy terms $\gamma_1, ..., \gamma_{r_1-1}$, $\gamma_{r_1+r_2+1}, ..., \gamma_{r_1+2r_2}$, γ_{r_1} and eventually, $\gamma_{r_1+1}, ..., \gamma_{r_1+r_2}$ successively. Combining one more time lemma 4.10 and the formula $\epsilon = \frac{1}{|G|} \sum_{\chi\in \mathrm{Irr}(G)} \chi(1)\chi$ we get :

$$\begin{aligned}
\prod_{1\leq i\leq r_1-1} \sum_{\gamma_i\in G} \epsilon(u_i g_i^{\gamma_i} u_{i+1}) &= \prod_{1\leq i\leq r_1-1} \sum_{\chi_i\in Irr(G)} \chi_i(g_i)\chi_i(u_{i-1}u_i) \\
&= \sum_{(\chi_1,...,\chi_{r_1-1})\in Irr(G)} \prod_{1\leq i\leq r_1-1} \chi_i(g_i)\chi_i(u_{i-1}u_i)
\end{aligned}$$

and

$$\begin{aligned}
\prod_{1\leq i\leq r_2} \sum_{\gamma_{r_1+2r_2+1-i}\in G} \epsilon(u_0 g_{r_1+i}^{\gamma_{r_1+i}} u_0 g_{r_1+2r_2+1-i}^{\gamma_{r_1+2r_2+1-i}}) &= \prod_{1\leq i\leq r_2} \sum_{\chi_{r_1+i}\in Irr(G)} \chi_{r_1+i}(g_{r_1+i})\chi_{r_1+i}(g_{r_1+2r_2+1-i}) \\
&= \sum_{(\chi_{r_1+1},...,\chi_{r_1+r_2})\in Irr(G)} \prod_{1\leq i\leq r_2} \chi_{r_1+i}(g_{r_1+i})\chi_{r_1+i}(g_{r_1+2r_2+1-i})
\end{aligned}$$

So, substituting this back in we get :

$$|E_{\underline{g},r_1,r_2}| \leq \sum_{\substack{\chi_1,\dots,\chi_{r_1-1}\in Irr(G)\\ \chi_{r_1+1},\dots,\chi_{r_1+r_2}\in Irr(G)}} \prod_{1\leq i\leq r_1-1}\chi_i(g_i)\prod_{1\leq i\leq r_2}\chi_{r_1+i}(g_{r_1+i})\chi_{r_1+i}(g_{r_1+2r_2+1-i})$$
$$\times \sum_{\underline{u}\in \mathrm{Inv}(G)^{r_1}/\sim}\prod_{1\leq i\leq r_1-1}\chi_i(u_{i-1}u_i)\sum_{\gamma_{r_1+1},\dots,\gamma_{r_1+r_2}\in G}\sum_{\gamma_{r_1}\in G}\epsilon(u_0u_{r_1-1}g_{r_1}^{\gamma_{r_1}}[g_{r_1+1}^{\gamma_{r_1+1}}\cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}},u_0])$$

but, according to $(***)$

$$\sum_{\gamma_{r_1+1},\dots,\gamma_{r_1+r_2}\in G}\sum_{\gamma_{r_1}\in G}\epsilon(u_0u_{r_1-1}g_{r_1}^{\gamma_{r_1}}[g_{r_1+1}^{\gamma_{r_1+1}}\cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}},u_0])$$
$$=\sum_{\gamma_{r_1+1},\dots,\gamma_{r_1+r_2}\in G}\sum_{\gamma_{r_1}\in G}\epsilon(u_{r_1-1}g_{r_1}^{\gamma_{r_1}}g_{r_1+1}^{\gamma_{r_1+1}}\dots g_{r_1+r_2}^{\gamma_{r_1+r_2}}u_0(g_{r_1+1}^{\gamma_{r_1+1}}\dots g_{r_1+r_2}^{\gamma_{r_1+r_2}})^{-1})$$
$$=\sum_{x\in G}\sum_{\gamma_{r_1+1},\dots,\gamma_{r_1+r_2}\in G}\epsilon(g_{r_1+1}^{\gamma_{r_1+1}}\dots g_{r_1+r_2}^{\gamma_{r_1+r_2}}x)\sum_{\gamma_{r_1}\in G}\epsilon(u_{r_1-1}g_{r_1}^{\gamma_{r_1}}x^{-1}u_0x)$$

and, one more time we can compute from right to left, using lemma 4.10 :

$$\sum_{\gamma_{r_1}\in G}\epsilon(u_{r_1-1}g_{r_1}^{\gamma_{r_1}}x^{-1}u_0x)=\sum_{\alpha\in\mathrm{Irr}(G)}\alpha(g_{r_1})\alpha(u_{r_1-1}x^{-1}u_0x)$$

and

$$\sum_{(\gamma_{r_1+1},\dots,\gamma_{r_1+r_2})\in G}\epsilon(g_{r_1+1}^{\gamma_{r_1+1}}\dots g_{r_1+r_2}^{\gamma_{r_1+r_2}}x)=|G|^{r_2-1}\sum_{\beta\in\mathrm{Irr}(G)}\frac{\prod_{i=1}^{r_2}\beta(g_{r_1+i})}{\beta(1)^{r_2-1}}\beta(x)$$

which finally leads to :

$$|E_{\underline{g},r_1,r_2}| \leq |G|^{r_2-1}\sum_{\substack{\chi_1,\dots,\chi_{r_1-1}\in\mathrm{Irr}(G)\\ \chi_{r_1+1},\dots,\chi_{r_1+r_2}\in\mathrm{Irr}(G)\\ \alpha,\beta\in\mathrm{Irr}(G)}}\frac{\alpha(g_{r_1})}{\beta(1)^{r_2-1}}\prod_{i=1}^{r_2}\beta(g_{r_1+i})\prod_{i=1}^{r_1-1}\chi_i(g_i)\prod_{i=1}^{r_2}\chi_{r_1+i}(g_{r_1+i})\chi_{r_1+i}(g_{r_1+2r_2+1-i})$$
$$\times\sum_{\underline{u}\in\mathrm{Inv}(G)^{r_1}/\sim}\prod_{i=1}^{r_1-1}\chi_i(u_{i-1}u_i)\sum_{x\in G}\alpha(u_{r_1-1}x^{-1}u_0x)\beta(x)$$

To end the proof, just note that, once again $|\Sigma^{\mathbb{R}}(\mathbf{C};r_1,r_2)|\neq\emptyset$ implies that $C_{r_1+i}=C_{r_1+2r_2-i+1}^{-1}$ for $i=1,\dots,r_2$ so $Z_i=Z_{r_1+2r_2-i+1}$, $\chi(g_{r_1+i})\chi(g_{r_1+2r_2-i+1})=|\chi(g_{r_1+i})|^2$ and

$$\sum_{\chi\in\mathrm{Irr}(G)}\chi(g_{r_1+i})\chi(g_{r_1+2r_2-i+1})=\sum_{\chi\in\mathrm{Irr}(G)}|\chi(g_{r_1+i})|^2=Z_{r_1+i}$$

for $i=1,\dots,r_2$, which leads to the announced result.

3.4 G-covers which are not defined over their field of moduli

Except in 3.5.2.2, we will always assume we are in the complex pair configuration (C). We keep the notations from section 3.2, particularly concerning $\mathbf{A}_\chi$, $\mathbf{A}_\chi^{mod}$, α_{χ,g_0}, *etc.* In addition, say $\mathbf{C}$ is $\mathbb{C}g$*-complete symetric* if :

(1) $\Sigma(\mathbf{C},G)=\mathrm{sni}(\mathbf{C})$ and
(2) $\mathbf{C}=(C_1,\dots,C_s,C_s^{-1},\dots,C_1^{-1})$ (and so $\Sigma^{\mathbb{R}}(\mathbf{C};0,s)\neq\emptyset$)

If (1) is replaced by

$$(1)^{\mathbb{R}} \quad \Sigma^{\mathbb{R}}(\mathbf{C};0,s) = \mathrm{Sni}^{\mathbb{R}}(\mathbf{C};0,s)$$

say $\mathbf{C}$ is $\mathbb{R}$*g-complete symetric*. In the following computations we will always make the hypothesis $\mathbf{C}$ is $\mathbb{C}$*g-complete symetric*. Clearly we have g-complete implies (1), which implies $(1)^{\mathbb{R}}$. Under condition (1) one can use directly Serre's formula to compute $|\mathrm{sni}(\mathbf{C})|$, and under condition $(1)^{\mathbb{R}}$, formula $\mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s)$ to compute $|\mathrm{Sni}^{\mathbb{R}}(\mathbf{C};0,s)|$.

In the examples, we describe the $2s$-tuples $\mathbf{C}$ satisfying (2) using the following notation $\mathbf{C} = [A_1^{(a_1)},...,A_n^{(a_n)}]$ to indicate that the $2s$-tuple $\mathbf{C}$ consists of
- s first entries where A_1 occurs a_1 times,..., A_n occurs a_n times (so $s = a_1 + ... + a_n$)
- s last entries which are the inverses of the s first ones, in reversed order.

When $\mathbf{C}$ is $\mathbb{C}$g-complete symetric, Serre's formula becomes :

$$|\overline{\mathrm{sni}}(\mathbf{C})| = |Z(G)| \left(\frac{|C_1|...|C_s|}{|G|}\right)^2 \sum_{\chi\in \mathrm{Irr}(G)} \left(\frac{|\chi(g_1)|...\chi(g_s)|}{\chi(1)^{s-1}}\right)^2$$

hence :

$$\frac{|\overline{\mathrm{sni}}(\mathbf{C})|}{|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)|} = |C_1|...|C_s| \frac{\sum_{\chi\in \mathrm{Irr}G)} \left(\frac{|\chi(g_1)|...|\chi(g_s)|}{\chi(1)^{s-1}}\right)^2}{\sum_{\chi\in \mathrm{Irr}(G)} \frac{\chi(g_1)...\chi(g_s)}{\chi(1)^{s-1}} A_\chi}$$

Remark 3.10 Note that $Z(G) = \cap_{\chi\in \mathrm{Irr}(G)} Z_\chi$ where $Z_\chi = \{g \in G |\ |\chi(g)| = \chi(1)\}$, $\chi \in \mathrm{Irr}(G)$, so, if $\mathbf{C}$ is g-complete symetric, $|\Sigma(\mathbf{C})|$ remains unchanged when adding central classes whereas $|\Sigma^{mod,\mathbb{R}}(\mathbf{C};0,s)|$ and $|\Sigma^{mod,\mathbb{R}}(\mathbf{C};0,s)|$ do not. So adding central classes in $\mathbf{C}$ can change the proportion $|\overline{\mathrm{sni}}(\mathbf{C})|/|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)|$ of G-covers defined over $\mathbb{R}$ (and with field of moduli contained in $\mathbb{R}$ as well).

First we deal with the quaternion group $\mathbb{H}_8$ for which we exhibit G-covers not defined over their field of moduli. Then we generalize to obtain in particular a simple group-theoretic criterion for a finite group to be the Galois group of some G-cover not defined over its field of moduli. Lots of infinite families of groups verify this criterion.

3.4.1 Quaternion group $\mathbb{H}_8$

3.4.1.1 G-covers with group $\mathbb{H}_8$ which are not defined over their field of moduli

In the quaternion group $\mathbb{H}_8$ we have 4 non trivial conjugacy classes : $A = \{-1\}$, $A_i = \{\pm i\}$, $A_j = \{\pm j\}$, $A_k = \{\pm k\}$ Take

$$\mathbf{C} = [A^{(x)}, A_i^{(a)}, A_j^{(b)}, A_k^{(c)}] \text{ (so } s = x + a + b + c.)$$

To compute $\mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s)$ note that $\mathrm{Inv}(\mathbb{H}_8)/Z(\mathbb{H}_8)\cdot = \{1\}$, consequently $\mathbf{A}_\chi = \alpha_{\chi,1} = 8$ if $\chi = \chi_1$ and $\mathbf{A}_\chi = 0$ otherwise, which leads to :

$$\begin{cases} \bullet\ \mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s) = 2^{a+b+c} \\ \bullet\ |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)| = 2^{a+b+c-2} \\ \bullet\ |\overline{\mathrm{sni}}(\mathbf{C})| = 2^{2(a+b+c)-3} \\ \bullet\ \frac{|\overline{\mathrm{sni}}(\mathbf{C})|}{|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)|} = 2^{a+b+c-1} \\ \bullet\ |\overline{\mathrm{sni}}(\mathbf{C})| - |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)| = 2^{a+b+c-2}(2^{a+b+c-1}-1) \end{cases}$$

If $a = b = 1$, $x = c = 0$ and so $r = 2s = 4$, we get $|\overline{\mathrm{sni}}(\mathbf{C})| = 2$ and $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,2)| = 1$ [2]. This gives rise to a new example of a G-cover with group $\mathbb{H}_8$ not defined over its field of moduli (recall

[2] We can give here explicit representatives : $sni(\mathbf{C}) = \{(i,j,-j,-i),(i,j,j,i)\}$ and $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,2) = \{(i,j,-j,-i)\}$.

that such an example was already given by K.Coombes and D.Harbater in [CoH85] p.831 but with three rational branch points $(1,2,3)$ and canonical inertia invariant $\mathbf{C}=(\{\pm i\},\{\pm j\},\{\pm k\})$. Since $\mathbf{C}$ is a rigid $\mathbb{Q}$-rational 3-tuple the corresponding G-cover has field of moduli $\mathbb{Q}$ but it can't be defined over $\mathbb{R}$ since $\mathbb{H}_8$ is not generated by its involutions (cf. [DF94], Théorème 1.1).) We give a precise argument in 3.4.2, but the general idea is that, given the branch points $(z_1,z_2,\overline{z_2},\overline{z_1})\in\mathcal{U}^r$ with z_1,z_2 not real, the fiber $(\psi'_{4,\mathbb{H}_8})^{-1}((z_1,z_2,\overline{z_2},\overline{z_1}))\subset\mathcal{H}'_{4,\mathbb{H}_8}(\mathbf{C})$ consists of two points P'_1, P'_2 corresponding to two G-covers f_1, f_2, one of which, say f_1, is defined over $\mathbb{R}$ and the other one, f_2, is not. If $P_1=\Pi_4(P'_1)$ and $P_2=\Pi_4(P'_2)$ are the corresponding points on $\mathcal{H}_{4,\mathbb{H}_8}(\mathbf{C})$ then, $P_1^c=P_1$ forces $P_2^c=P_2$ so P_2 is a real point i.e. f_2 has its field of moduli contained in $\mathbb{R}$.

We can also use formula $\mathbf{n}^{mod,\mathbb{R}}(\mathbf{C};0,s)$, which is more precise : for this, note that $Z(\mathbb{H}_8)^{\frac{1}{2}}/Z(\mathbb{H}_8).=\mathbb{H}_8/Z(\mathbb{H}_8).=\{1,i,j,k\}$ so $\mathbf{A}_\chi^{mod}=\alpha_{\chi,1}+\alpha_{\chi,i}+\alpha_{\chi,j}+\alpha_{\chi,1}=20$ if $\chi=\chi_1$ and $\mathbf{A}_\chi^{mod}=4$ otherwise, which leads to

$$\begin{cases}\bullet\ \mathbf{n}^{mod\,\mathbb{R}}(\mathbf{C};0,s)=2^{a+b+c-1}\times(5+(-1)^{b+c}+(-1)^{a+c}+(-1)^{a+b})\\ \bullet\ |\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C};0,s)|=2^{a+b+c-3}\times(5+(-1)^{b+c}+(-1)^{a+c}+(-1)^{a+b})\end{cases}$$

Taking $a=b=1$, $x=c=0$ gives $|\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C};0,2)|=2$, as expected. But we get more since $\Delta^{mod}(\mathbf{C};0,s):=|\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C};0,s)|-|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C};0,s)|=2^{a+b+c-3}(3+(-1)^{b+c}+(-1)^{a+c}+(-1)^{a+b})>0$ (indeed $\Delta^{mod}(\mathbf{C};0,s)=0\Leftrightarrow b+c\equiv a+c\equiv a+b\equiv 1mod2\Rightarrow 2b\equiv 1mod2$ a contradiction) so there are exactly $\Delta^{mod;0,s}$ G-covers in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C};0,s)$ which are not defined over $\mathbb{R}$ but with their field of moduli contained in $\mathbb{R}$.

3.4.1.2 Going further

We still consider the tuple $\mathbf{C}=(\{\pm i\},\{\pm j\},\{\pm j\},\{\pm i\})$ of section 3.4.1.1, and take $\mathbf{t}'=(i,(1+i),(1-i),-i)$ for the corresponding branch points. We have computed $|\overline{\text{sni}}(\mathbf{C})|=2=|\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C};0,2)|$, $|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C};0,2)|=1$. As above, write f_1 for the G-cover which is defined over $\mathbb{R}$, f_2 for the one which is not and P_1, P_2 for the corresponding points on $\mathcal{H}_{4,\mathbb{H}_8}(\mathbf{C})$. Both f_1, f_2 have field of moduli k contained in a real quadratic number field $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$. Furthermore, the only prime where $\mathbf{t}=(X^2+1)(X^2-2X+2)$ has bad reduction is $p=2$, which is also the only prime dividing $|\mathbb{H}_8|$. So, according to Beckman's theorem [Be89], 2 is the only prime which may be ramified in k. As a result $k=\mathbb{Q}$ or $k=\mathbb{Q}(\sqrt{2})$. If $k=\mathbb{Q}$, set $\mathcal{P}=2$ and if $k=\mathbb{Q}(\sqrt{2})$, let denote by $\mathcal{P}$ the only place lying above 2. According to [DH98] corollary 4.3, f_1 and f_2 are defined over the completions $k_\mathcal{Q}$ of k at any place $\mathcal{Q}$ lying above $q\neq p$. But f_1 is also defined over $\mathbb{R}$ so, [DDo97] §3.4 implies that f_1 is defined over its field of moduli, k. Likewise, assume f_2 is defined over the completion $k_\mathcal{P}$ of k at $\mathcal{P}$ then [DDo97] §3.4 would imply, this time, f_2 is defined over $\mathbb{R}$, a contradiction. To conclude with this example, recall "being defined over its field of moduli" is a Galois invariant property. Consequently, for any $\sigma\in\text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, f_1^σ is still defined over its field of moduli whereas f_2^σ is not that is, $P_1^\sigma=P_1$ and $P_2^\sigma=P_2$. Conclude $k=\mathbb{Q}$ and
- f_1 is defined over $\mathbb{Q}$.
- f_2 has field of moduli $\mathbb{Q}$ but is not defined over $\mathbb{Q}$. Its extension $f_{2,\overline{\mathbb{Q}}_2}$ has field of moduli $\mathbb{Q}_2$ but is not defined over $\mathbb{Q}_2$. This is a new example of G-cover with p-adic moduli field but which is not defined over its field of moduli ([W02] exhibits examples of this kind with $G=\tilde{\mathcal{A}}_5$ and any prime $p>5$).

Remark 3.11 Another way to find G-cover with group $\mathbb{H}_8$ which have field of moduli $\mathbb{Q}$ but are not defined over their field of definition is the genus 0 argument. Indeed, consider the tuple $\mathbf{C}=(\{\pm i\},\{\pm j\},\{\pm j\},\{\pm i\})$ and fix the three last branch points $\mathbf{t}'=(1,2,3)$. Then $\mathcal{H}'_{r,\mathbb{H}_8}(\mathbf{C})$ is absolutely irreducible defined over $\mathbb{Q}$. Its genus can be computed applying Hurwitz formula to the cover $\Psi'_{\mathbf{t}'}:\mathcal{H}'_{r,\mathbb{H}_8}(\mathbf{C})\to\mathbb{P}^1_\mathbb{Q}$ which is branched at $1,2,3$ with corresponding branch cycle description the image of $a_{1,2}=Q_1^{-2}$, $a_{1,3}=Q_1Q_2^{-2}Q_1^{-1}$, $a_{1,4}=Q_1Q_2Q_3^{-2}Q_2^{-1}Q_1^{-1}$ in $\text{Per}(\overline{\text{sni}}(\mathbf{C},\mathbb{H}_8))$ (*cf* [DF94]). writing $a=(i,j,-j,-i)$, $b=(i,j,j,i)$, we get $a_{1,2}=a_{1,3}=(a,b)$ and $a_{1,4}=(a)(b)$. So $\mathcal{H}'_{r,\mathbb{H}_8}(\mathbf{C})$ has genus $g=0$ and the ramified point above 1 as well as the one above 2 are $\mathbb{Q}$-points. Deduce the set of $\mathbb{Q}$ is dense in $\mathcal{H}'_{r,\mathbb{H}_8}(\mathbb{C})$. Any of these $\mathbb{Q}$-point then corresponds to a G-cover with field of moduli $\mathbb{Q}$ but which is not defined over $\mathbb{R}$.

3.4.2 General criteria

With the usual notations write

$$\Delta^{mod}(\mathbf{C};r_1,r_2)=|\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C};r_1,r_2)|-|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};r_1,r_2)|$$

When $\mathbf{C}$ is $\mathbb{R}$g-complete symetric and $(r_1,r_2)=(r,0)$ or $(0,s)$,

$$\Delta^{mod}(\mathbf{C};r_1,r_2)=\mathbf{n}^{mod\,\mathbb{R}}(\mathbf{C};r_1,r_2)-\mathbf{n}^{\mathbb{R}}(\mathbf{C};r_1,r_2)$$

Thus we obtain the following simple criterion :

Proposition 3.12 *Let G be a finite group. For any $\mathbb{R}$g-complete r-tuple $\mathbf{C}=(C_1,...,C_r)$ of non trivial conjugacy classes in G and for any r-tuple $\mathbf{t}'=(t_1,...,t_r)\in\mathcal{U}^r(\mathbb{R})$ with $t_1<...<t_r$, of all the isomorphism classes of G-covers in the straight Nielsen class $\overline{\mathrm{sni}}(\mathbf{C})$ with ordered branch point set $\mathbf{t}'$, exactly*

$$\Delta^{mod}(\mathbf{C};r,0)=\frac{|Z(G)|}{|G|Z_1\cdots Z_r}\sum_{\underline{\chi}\in\mathrm{Irr}(G)^r}\chi_1(g_1)...\chi_r(g_r)(\mathbf{I}_{\underline{\chi}}^{mod}-\mathbf{I}_{\underline{\chi}})$$

have field of moduli contained in $\mathbb{R}$ but are not defined over $\mathbb{R}$.
Similarly, for any $\mathbb{R}$g-complete symetric r-tuple $\mathbf{C}=(C_1,...,C_r)$ of non trivial conjugacy classes in G and for any r-tuple $\mathbf{t}'=(z_1,...,z_s,\overline{z_s},...,\overline{z_1})\in\mathcal{U}^r(\mathbb{C})$ with z_i not real, $i=1,...,s$, of all the isomorphism classes of G-covers in the straight Nielsen class $\overline{\mathrm{sni}}(\mathbf{C})$ with ordered branch point set $\mathbf{t}'$, exactly

$$\Delta^{mod}(\mathbf{C};0,s)=\frac{|C_1|\cdots C_s|}{[G:Z(G)]|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(g_1)...\chi(g_s)}{\chi(1)^{s-1}}(\mathbf{A}_\chi^{mod}-\mathbf{A}_\chi)$$

have field of moduli contained in $\mathbb{R}$ but are not defined over $\mathbb{R}$.

Proposition 3.12 shows in particular that, once a $\mathbb{R}$g-complete symetric canonical inertia invariant $\mathbf{C}$ and a branch point configuration - (R) or (C) - are given, the number of G-covers in $\overline{\mathrm{sni}}(\mathbf{C})$ with field of moduli contained in $\mathbb{R}$ but not defined over $\mathbb{R}$ can be computed explicitly and is independent of the branch points.

Corollary 3.13 *Given a finite group G, there are G-covers with group G and branch point configuration (C) with field of moduli contained in $\mathbb{R}$ but not defined over $\mathbb{R}$ if and only if $Z(G)$ has an element which is a square in G but not in $Z(G)$.*

Proof. Let us compute $\mathbf{A}_\chi^{mod}-\mathbf{A}_\chi=\sum_{g_0}\alpha_{\chi,g_0}$ for any $\chi\in\mathrm{Irr}(G)$ and where g_0 ranges over a system of representatives of the set $Z(G)^{\frac{1}{2}}/Z(G)\cdot\backslash\mathrm{Inv}(G)/Z(G)\cdot$ For this, just note that for all $g_0\in Z(G)^{\frac{1}{2}}$ there exists $z\in Z(G)$ such that $(zg_0)^2=1$ (that is, $Z(G)g_0\in\mathrm{Inv}(G)/Z(G)\cdot$) if and only if g_0^2 is a square in $Z(G)$. Consequently, setting $E_G=\{g_0\in Z(G)^{\frac{1}{2}}|g_0^2\notin\{z^2\}_{z\in Z(G)}\}$, we get $\mathbf{A}_\chi^{mod}-\mathbf{A}_\chi=\sum_{g_0\in E_G/Z(G)\cdot}\alpha_{\chi,g_0}$. Also note that it follows from their definition that the α_{χ,g_0} are non negative integers and for $\chi=\chi_1$, they also are non zero ($\alpha_{\chi_1,g_0}=|\mathrm{Cen}_{g_0}(G)|$), so the $\mathbf{A}_\chi^{mod}-\mathbf{A}_\chi$ are non negative integers. Now, suppose there is a $\mathbb{R}$g-complete symetric $2s$-tuple $\mathbf{C}$ of non-trivial conjugacy classes of G such that $\Delta^{mod}(\mathbf{C};0,s)>0$. Then there is $\chi\in\mathrm{Irr}(G)$ such that $\mathbf{A}_\chi^{mod}-\mathbf{A}_\chi>0$, which obviously implies $E_G\neq\emptyset$.

Conversely, let $C_1,...,C_s$ be a listing of all the non trivial conjugacy classes in G and set $\mathbf{C}=(C_1,C_1^{-1},...,C_s,C_s^{-1},C_s,C_s^{-1},...,C_1,C_1^{-1})$. This $2s$-tuple is g-complete symetric. So one gets

$$\begin{aligned}\Delta^{mod}(\mathbf{C};0,s) &= \frac{(|C_1|\cdots|C_s|)^2}{[G:Z(G)]|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{|\chi(g_1)|^2\cdots|\chi(g_s)|^2}{\chi(1)^{2s-1}}(\mathbf{A}_\chi^{mod}-\mathbf{A}_\chi)\\ &= \frac{(|C_1|\cdots|C_s|)^2}{[G:Z(G)]|G|}\left(\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ deg(\chi)=1}}(\mathbf{A}_\chi^{mod}-\mathbf{A}_\chi)+\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ deg(\chi)>1}}\frac{|\chi(g_1)|^2\cdots|\chi(g_s)|^2}{\chi(1)^{2s-1}}(\mathbf{A}_\chi^{mod}-\mathbf{A}_\chi)\right)\end{aligned}$$

and, since $E_G \neq \emptyset$, $\mathbf{A}_{\chi_1}^{mod} - \mathbf{A}_{\chi_1} = \sum_{g_0 \in E_G/Z(G).} |\mathrm{Cen}_{g_0}(G)| > 0$. □

Remark 3.14 (a) Pierre Dèbes made me notice that corollary 3.13 can be proved directly, only using the definitions of $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C};0,s)$ and $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)$. However, this elementary proof also requires the 4s-tuple $\mathbf{C} = (\mathbf{C}^0, \mathbf{C}^{0\,-1})$, which appears naturally in the proof above, to construct a G-cover in $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C};0,s) \backslash \overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)$: For the necessary condition, let $(g_1,...,g_r) \in \overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C};0,s) \backslash \overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)$. The g_0 given by condition (4) is such as $g_0^2 \in Z(G)$. But, if it were a square ζ^2 in $Z(G)$, we would have $(g_0\zeta^{-1})^2 = g_0^2\zeta^{-2} = 1$ i.e. $(\zeta g_1 \zeta^{-1},...,\zeta g_r \zeta^{-1}) = (g_1,...,g_r) \in \overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)$, a contradiction. For the sufficient condition, let $u = g_0^2$ be a square in G but not in $Z(G)$, we are going to attach to it a G-cover with field of moduli contained in $\mathbb{R}$ but which is not defined over $\mathbb{R}$. For this, consider the inertia canonical invariant $\mathbf{C}$ of the proof of corollary 3.13 and a 4s-tuple $\underline{g} \in \overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C};0,2s)$ such as $\underline{g} = (g_1, g_0 g_1^{-1} g_0^{-1},..., g_s, g_0 g_s^{-1} g_0^{-1}, g_1, g_0 g_1^{-1} g_0^{-1},..., g_s, g_0 g_s^{-1} g_0^{-1})$. Then, if $\underline{g} \in \overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,2s)$ there would be $g_0' \in \mathrm{Inv}(G)$ such as $g_0' g_i g_0^{'-1} = g_0 g_i g_0^{-1}$ for $i = 1,...,s$, i.e. $g_0' g_0 \in \cap_{1 \leq i \leq s} \mathrm{Cen}_G(g_i) = Z(G)$, so $g_0 \in Z(G)$, a contradiction. □.
(b) Lots of groups satisfy the condition of corollary 3.13 - and so are groups of G-covers not defined over their field of moduli : for instance,
- $\mathrm{Gl}_n(p^m)$ with $n \geq 2$, $m \geq 1$, $p \geq 3$ prime,
- D_{2n} with $n \geq 4$ such that $4|n$,
- $(\mathrm{O}_2(p^m, \mathrm{q}^h))$ with $m \geq 1$, $p \geq 3$ prime and q^h the hyperbolic form on $\mathbb{F}_{p^m}^2$,
- any group G such that $\mathrm{Inv}(G) \subset Z(G)$ and $2|[G : Z(G)]$ (for instance $\mathrm{Sl}_2(p^m)$ with $m \geq 1$, $p \geq 3$ irreducible, T_{4n} with $n \geq 2$)...
To my knowledge, the only example of families of G-covers not defined over their field of moduli and in which the group G can be taken arbitarily large was given by S.Wewers in [W02]. He takes the G-covers f_p with group $\mathrm{Sl}_2(p)$ where $p \not\equiv \pm 1[8]$ is an odd prime, canonical inertia invariant $(4A, pA, pB) = \mathbf{C}$ and branch points (t_1, t_2, t_3) where $t_1 \in \mathbb{Q}$ and $\{t_2, t_3\}$ is $\mathbb{Q}$-rational. By [V99] I.3.3.6. this 3-tuple is rigid and $\mathbb{Q}$-rational so f_p has field of moduli $\mathbb{Q}$. But, as $\mathrm{Inv}(\mathrm{Sl}_2(p)) \subset Z(\mathrm{Sl}_2(p))$, there are no $g_0 \in \mathrm{Inv}(\mathrm{Sl}_2(p))$, $g_1 \in$4A such that $(g_0 g_1)^2 = 1$! So f_p can't be defined over $\mathbb{R}$.

Computing $\Delta^{mod}(\mathbf{C}; r_1, r_2)$ can be difficult. The following proposition gives a weaker but more practical criterion for the existence of G-covers not defined over their field of moduli. We give here the statement and proof for situation (C) but it can immediately be generalized to situations (R) and (R-C).

Proposition 3.15 *Suppose given a finite group G and a symetric 2s-tuple $\mathbf{C}$ of non trivial conjugacy classes in G. If $|\overline{\mathrm{sni}}(\mathbf{C})| - |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)|$ is odd then for any 2s-tuple of branch points $\mathbf{t}' = (z_1,...,z_s,\overline{z_s},...,\overline{z_1}) \in \mathcal{U}^r(\mathbb{C})$ with z_i not real for i=1,...,s, there is, in $\overline{\mathrm{sni}}(\mathbf{C})$, at least one isomorphism class of G-covers with field of moduli contained in $\mathbb{R}$ but not defined over $\mathbb{R}$.*

Proof. Write $m = |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)|$, $n = |\overline{\mathrm{sni}}(\mathbf{C})|$, and let $P_1',...,P_m'$ be the points in $(\psi'_{2s,G})^{-1}(\mathbf{t}')$ corresponding to the G-covers defined over $\mathbb{R}$ and $P_{m+1}',...,P_n'$ the points corresponding to the G-covers which are not. Set $P_i = \Pi_{2s}(P_i')$, $i = 1,...,n$, $E = \{P_1,...,P_m\}$, $F = \{P_{m+1},...,P_n\}$. So, with $\mathbf{t} = \pi_{2s}(\mathbf{t}')$ we have $E \cup F \subset (\psi_{2s,G})^{-1}(\mathbf{t})$. Then observe that $E \cup F = \Pi_{2s}((\psi'_{2s,G})^{-1}(\mathbf{t}'))$ is left invariant by complex conjugation c. Indeed $(\psi'_{2s,G})^{-1}(\mathbf{t}')$ is the set of all G-covers f for which C_i is the inertia canonical class associated with z_i and C_i^{-1} is the inertia canonical class associated with $\overline{z_i} = z_{2s+1-i}$ for $i = 1,...,s$ whereas $(\psi'_{2s,G})^{-1}(\mathbf{t}')^c$ is the set of all G-covers f^c, for which - by Fried's "Branch cycle argument" - C_i^{-1} is the inertia canonical class associated with $\overline{z}_i = z_{2s+1-i}$ and $(C_i^{-1})^{-1} = C_i$ is the inertia canonical class associated with $\overline{\overline{z}}_i = z_i$ for $i = 1,...,s$. Now, since $P_1,...,P_m$ are real points on $(\psi_{2s,G})^{-1}(\mathbf{t})$, we have $E^c = E$, which forces $F^c = F$. Hence, as $|F|$ is odd, F has at least one point P invariant under c. This point P is real, which means it corresponds to an isomorphism class of G-covers with field of moduli contained in $\mathbb{R}$ but, by definition of F, not defined over $\mathbb{R}$. □

3.4.3 Dicyclic groups T_{4n} of order $4n$

We give here an application of proposition 3.15. The quaternion group $\mathbb{H}_8$ is the first term of the family of dicyclic groups $(T_{4n})_{n \geq 2}$. The group T_{4n} can be defined by generators and relations :

$$T_{4n} = < a, b \mid a^{2n} = 1, a^n = b^2, b^{-1}ab = a^{-1} >$$

and contains $n+2$ non trivial conjugacy classes :
- n classes $A_1,...,A_n$ with $A_i = \{a^i, a^{-i}\}$, $i = 1,...,n$ (note that $A_n = \{a^n\}$).

- $B_1 = \{a^{2j}b\}_{0\leq j\leq n-1}$ and $B_2 = \{a^{2j+1}b\}_{0\leq j\leq n-1}$.
Take

$$\mathbf{C} = [A_n^{(\alpha_n)}, A_1^{(\alpha_1)}, ..., A_{n-1}^{(\alpha_{n-1})}, B_1^{(\beta_1)}, B_2^{(\beta_2)}]$$

and also write $\alpha = \alpha_1 + ... + \alpha_n$. So $s = \alpha + \beta_1 + \beta_2$. We have $\mathrm{Inv}(T_{4n})/Z(T_{4n})\cdot = \{1\}$, consequently $\mathbf{A}_\chi = \alpha_{\chi,1} = 4n$ if $\chi = \chi_1$ and $\mathbf{A}_\chi = 0$ otherwise. Using the character tables of these groups, which can be found in [**?**] p.385, and taking into account that, for $\mathbf{C}$ to be g-complete we need $\beta_1 + \beta_2 \geq 1$, we obtain

$$\begin{cases} \bullet\ \mathbf{n}^{mod\,\mathbb{R}}(\mathbf{C}; 0, s) = 2^\alpha n^{\beta_1+\beta_2} \\ \bullet\ \overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, s)| = 2^{\alpha-1} n^{\beta_1+\beta_2-1} \\ \bullet\ \overline{\mathrm{sni}}(\mathbf{C})| = 2^{2\alpha-1} n^{2(\beta_1+\beta_2)-2} \\ \bullet\ \frac{|\overline{\mathrm{sni}}(\mathbf{C})|}{|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C};0,s)|} = 2^\alpha n^{\beta_1+\beta_2-1} \\ \bullet\ |\overline{\mathrm{sni}}(\mathbf{C})| - |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, s)| = 2^{\alpha-1} n^{\beta_1+\beta_2-1}(2^\alpha n^{\beta_1+\beta_2-1} - 1) \end{cases}$$

For $\alpha_1 = 1$, $\beta_1 \geq 1$, $\beta_2 \geq 0$, $\alpha_1 = ... = \alpha_n = 0$, $\mathbf{C}$ is g-complete symetric and $|\overline{\mathrm{sni}}(\mathbf{C})| - |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, s)| = n^{\beta_1+\beta_2-1}(2n^{\beta_1+\beta_2-1} - 1)$ is odd when n is (and, when $\beta_1 + \beta_2 = 1$, it is always odd). So, for each $n \geq 2$, for each $\mathbf{t} = \{z_1, \overline{z}_1, ..., z_s, \overline{z}_s\} \in \mathcal{U}_r(\mathbb{Q})$ with z_i not real, $i = 1, ...s$, there is at least one isomorphism class of G-cover f_n with ramification type $[T_{4n}, \mathbf{C}, \mathbf{t}]$ which is not defined over $\mathbb{R}$ but has its field of moduli contained in $\mathbb{R}$.

3.4.4 A criterion for profinite groups

One could ask if the above criteria could be generalized to profinite groups. Recall that "being defined over its field of moduli" is a property which does not behave well when passing to quotient. Indeed, let k be a field of characteristic 0, G a finite group and $s : G \twoheadrightarrow H$ a group epimorphism. Consider a G-covers $\Phi : \pi_1^{\mathrm{alg}}(\mathbb{P}^1_{k^s}\backslash\mathbf{t}) \twoheadrightarrow G$ and its quotient $s \circ \Phi : \pi_1^{\mathrm{alg}}(\mathbb{P}^1_{k^s}\backslash\mathbf{t}) \twoheadrightarrow H$. Suppose k is the field of moduli of Φ and $k_H < k$, the one of $s \circ \Phi$. Then we have the following diagram

$$\begin{array}{ccc} H^2(k, Z(G)) & \xrightarrow{u} & H^2(k, Z(H)) \\ & & \uparrow v \\ & & H^2(k_H, Z(H)) \end{array}$$

If $\omega_\Phi \in H^2(k, Z(G))$ is the cohomological obstruction for Φ and $\omega_{s\circ\Phi} \in H^2(k_H, Z(H))$, the one for $s \circ \Phi$ we have $u(\omega_\Phi) = v(\omega_{s\circ\Phi})$, so $\omega_\Phi = 0$ only implies $\omega_{s\circ\Phi} \in \ker(\mathrm{v})$. Since $H^2(k_H, Z(H))$ is of $|Z(H)|$-torsion and $\ker(\mathrm{v}) < \mathrm{H}^2(\mathrm{k_H}, \mathrm{Z(H)})([\mathrm{k} : \mathrm{k_H}])$, $([k : k_H], |Z(H)|) = 1$ entails v is injective but this is the only case where we can conclude directly.

Consider now a finite group G and a group epimorphism $s : G \twoheadrightarrow H$. Fix also $\mathbf{C} = (C_1, ..., C_s, C_s^{-1}, ..., C_1^{-1})$ an $2s$ symetric g-complete tuple of conjugacy classes in G and observe that

$$\mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathbf{C}; 0, \mathrm{s})\backslash\mathrm{Sni}^{\mathbb{R}}(\mathbf{C}; 0, \mathrm{s}) = \left\{ (g_1, ..., g_{2s}) \in \mathrm{Sni}(\mathbf{C}, \mathrm{G}) \;\middle|\; \begin{array}{l} (4)''' \text{ there exists } g_0 \in Z(G)^{\frac{1}{2}} \text{ such that} \\ \text{(i) } g_0^2 \notin \{z^2\}_{z\in Z(G)} \\ \text{(ii) } g_0 g_i g_0^{-1} = g_{2s+1-i}^{-1},\ i = 1, ..., s \end{array} \right\}$$

So, assuming $\ker(\mathrm{s}) \cap \mathrm{Z(G)} = \{1\}$, we get

$$s(\mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathbf{C}; 0, \mathrm{s})\backslash\mathrm{Sni}^{\mathbb{R}}(\mathbf{C}; 0, \mathrm{s})) \subset \mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathrm{s}(\mathbf{C}); 0, \mathrm{s})\backslash\mathrm{Sni}^{\mathbb{R}}(\mathrm{s}(\mathbf{C}); 0, \mathrm{s})$$

Indeed, for any $\mathbf{g} = (g_1, ..., g_{2s}) \in \mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathbf{C}; 0, \mathrm{s})\backslash\mathrm{Sni}^{\mathbb{R}}(\mathbf{C}; 0, \mathrm{s})$ fix a g_0 as in condition $(4)'''$. Then $s(\mathbf{g}) \in \mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathrm{s}(\mathbf{C}); 0, \mathrm{s})$ and the set of those $h_0 \in H$ verifying condition $(4)''$ for $s(\mathbf{g})$ is exactly $Z(G) \cdot s(g_0)$. So, if $s(\mathbf{g}) \in \mathrm{Sni}^{\mathbb{R}}(\mathrm{s}(\mathbf{C}); 0, \mathrm{s})$, and since s is an epimorphism, there exists $z \in Z(G)$ such that $s(g_0)^2 = s(z)^2$ that is, $(g_0 z^{-1})^2 \in \ker(\mathrm{s}) \cap \mathrm{Z(G)} = \{1\}$, a contradiction. This gives the following statement

Proposition 3.16 *Let* $((G_{n+1}, \mathbf{C}_{n+1}) \overset{s_{n+1}}{\twoheadrightarrow} (G_n, \mathbf{C}_n))_{n\geq 0}$ *a complete projective system of finite groups and symetric g-complete* $2s$*-tuples of non trivial conjugacy classes. If*

$$\begin{cases} \textit{(1)}\ \ker(\mathrm{s_n}) \cap \mathrm{Z}(\mathrm{G_n}) = \{1\},\ n \geq 1. \\ \textit{(2)}\ \mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathbf{C}_\mathrm{n}; 0, \mathrm{s}) \backslash \mathrm{Sni}^{\mathbb{R}}(\mathbf{C}_\mathrm{n}; 0, \mathrm{s}) \neq \emptyset,\ n \geq 0. \end{cases}$$

then there exists a profinite Galois extension $K/\mathbf{C}(X)$ *with group* $G := \varprojlim_{n\geq 0} G_n$*, the field of moduli of which is contained in* $\mathbb{R}$ *but which is not defined over* $\mathbb{R}$*.*

Proof. According to (1) $(\mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathbf{C}_{\mathrm{n}+1}; 0, \mathrm{s}) \backslash \mathrm{Sni}^{\mathbb{R}}(\mathbf{C}_{\mathrm{n}+1}; 0, \mathrm{s}) \overset{\mathrm{s_{n+1}}}{\twoheadrightarrow} \mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathbf{C}_\mathrm{n}; 0, \mathrm{s}) \backslash \mathrm{Sni}^{\mathbb{R}}(\mathbf{C}_\mathrm{n}; 0, \mathrm{s}))$ is a projective system of finite sets, each of them being non empty by (2). So taking any $\mathbf{g} = (g_{1,n}, ..., g_{2s,n})_{n\geq 0} \in \varprojlim_{n\geq 0} \mathrm{Sni}^{\mathrm{mod},\mathbb{R}}(\mathbf{C}_\mathrm{n}; 0, \mathrm{s}) \backslash \mathrm{Sni}^{\mathbb{R}}(\mathbf{C}_\mathrm{n}; 0, \mathrm{s})$ and fixing an $2s$-tuple $\mathbf{t}' = (z_1, ..., z_s, \overline{z}_s, ..., \overline{z}_1) \in \mathcal{U}^r(\mathbb{R})$ in configuration (C) we get an inductive system $(K_n/\mathbf{C}(X) \hookrightarrow K_{n+1}/\mathbf{C}(X))_{n\geq 0}$ of finite Galois extensions which are not defined over $\mathbf{R}$ but such that $\mathrm{Isom}_{\mathbb{C}(\mathrm{X})}(\mathrm{K_n}, \mathrm{c}(\mathrm{K_n}))$ is a non empty finite set, $n \geq 0$. This in turn gives a profinite Galois extension $K := \cup_{n\geq 0} K_n/\mathbf{C}(X)$ which is not defined over $\mathbb{R}$ but with field of moduli contained in $\mathbf{R}$ since $\mathrm{Isom}_{\mathbb{C}(\mathrm{X})}(\mathrm{K}, \mathrm{c}(\mathrm{K})) = \varprojlim_{\mathrm{n}\geq 0} \mathrm{Isom}_{\mathbb{C}(\mathrm{X})}(\mathrm{K_n}, \mathrm{c}(\mathrm{K_n})) \neq \emptyset$. □

Example 3.17 Consider the natural projective system $((D_{8p^{n+1}}, \mathbf{C}_{n+1}) \overset{s_{n+1}}{\twoheadrightarrow} D_{8p^n}, \mathbf{C}_n))_{n\geq 0}$, where $p \geq 3$ is a prime number, and $\mathbf{C}_n = (A_{1,n}, A_{1,n}^{-1}, B_{1,n}, B_{1,n}^{-1})$, $n \geq 1$. Then, for any $n \geq 0$ we get (*cf.* [C04b] for the method of computation)

$$|\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}_n; 0, s) \backslash \overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}_n; 0, s)| = 10p^n > 0$$

so condition (2) is fulfilled. As for condition (1), just observe $\ker(\mathrm{s_n}) =< \mathrm{u}^{8\mathrm{p}^{\mathrm{n}-1}} >$ does not contain u^{2p^n}. Contrary to the preceeding examples $G := D_{8p^\infty}$ is an extension of $G_0 := D_{8p}$ by $P = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}_p$, which is not projective. More precisely, $Z(\tilde{G}) \cap P = 2.\mathbb{Z}/4\mathbb{Z}$

3.5 Descent from $\mathbb{C}$ to $\mathbb{Q}^{tr}$.

3.5.1 A general criterion

We give here a combinatorial method to determine if a finite group G admits G-covers defined over $\mathbb{Q}^{tr}$ with a prescribed ramification type $[G, \mathbf{C}, \mathbf{t}]$. For this, we look for r-tuples of non trivial conjugacy classes $\mathbf{C}$ in G such that $|\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)| = |\overline{\mathrm{sni}}(\mathbf{C})|$. In that case and if $\mathbf{t} \in \mathcal{U}_r(\mathbb{R})$, the image on $\mathcal{H}_{r,G}(\mathbf{C})$ of the fiber $(\psi'_{r,G})^{-1}(\mathbf{t}') \cap \mathcal{H}'_{r,G}(\mathbf{C})$ above any ordering $\mathbf{t}'$ of $\mathbf{t}$ as in (bp), consists of real points ; we denote it by

$$E^0_{r,G,\mathbf{t}}(\mathbf{C}) := \Pi_r((\psi'_{r,G})^{-1}(\mathbf{t}') \cap \mathcal{H}'_{r,G}(\mathbf{C})) \subset (\psi_{r,G})^{-1}(\mathbf{t}) \cap \mathcal{H}_{r,G}(\mathbf{C}))$$

Let us also write

$$E_{r,G,\mathbf{t}}(\mathbf{C}) := \bigcup_{m\geq 1 | (|G|,m)=1} E^0_{r,G,\mathbf{t}}(\mathbf{C}^m)$$

Then if for any $m \geq 1$ such that $(|G|, m) = 1$ we have $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}^m; r_1, r_2)| = |\overline{\mathrm{sni}}(\mathbf{C}^m, G)|$ $E_{r,G,\mathbf{t}}(\mathbf{C})$ consists of real points. But, if we also assume $\mathbf{t} \in \mathcal{U}_r(\mathbb{Q})$, Fried's "Branch cycle argument" asserts that $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ stabilizes $E_{r,G,\mathbf{t}}(\mathbf{C})$. So, any point in this set is $\mathbb{Q}^{tr}$-rational that is, corresponds to a G-cover with field of moduli contained in $\mathbb{Q}^{tr}$. If, for instance, $Z(G)$ is a direct summand of G, any G-cover with group G is defined over its field of moduli. As a result, all the G-covers above are actually defined over $\mathbb{Q}^{tr}$. This is a special case of the statement below

Proposition 3.18 *Let* G *be a finite group and* $\mathbf{C} = (C_1, ..., C_r)$ *an* r*-tuple of non trivial conjugacy classes of* G*. For any* $\mathbf{t}' \in \mathcal{U}^r(\mathbb{C})$ *the associated branch point divisor of which is rational, the following condition*

(1) for any $n \geq 1$ *such that* $(|G|, n) = 1$*,* $|\overline{\mathrm{sni}}(\mathbf{C}^n)| = |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}^n; r_1, r_2)|$*.*

implies all the G-covers in $\overline{\mathrm{sni}}(\mathbf{C})$ *are defined over* $\mathbb{Q}^{tr}$*.*

Remark 3.19 *1.* Observe that condition (1) can be replaced by the stronger one - easier to check when $\mathbf{C}$ is not g-complete :

(1)' for any $n \geq 1$ such that $(|G|, n) = 1$, $|\Sigma(\mathbf{C}^n, G)| = |\Sigma^{\mathbb{R}}(\mathbf{C}^n; r_1, r_2)|$ and $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}^n; r_1, r_2) \neq \emptyset$.

2. Proposition 3.18 could be replaced by the more general statement : Let G be a finite group and $\mathbf{C} = (C_1, ..., C_r)$ an r-tuple of non trivial conjugacy classes of G. For any $\mathbf{t}' \in \mathcal{U}^r(\mathbb{C})$ the associated branch point divisor of which is rational, the following conditions

(1) for any $n \geq 1$ such that $(|G|, n) = 1$, $|\overline{\text{sni}}(\mathbf{C}^n, G)| = |\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C}^n; r_1, r_2)|$.

(2) there is at least one G-cover f in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ with field of moduli $\mathbb{Q}$.

imply all the G-covers in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ with field of moduli $\mathbb{Q}$ are defined over $\mathbb{Q}^{tr}$. More generally, condition (2) could be replaced by

(2)' there is at least one G-cover f in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ such that for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$, f^σ also lies in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}^{\chi(\sigma)}; r_1, r_2)$

Proof With the notations above, condition (1) asserts that $E_{r,G,\mathbf{t}}(\mathbf{C})$ consists of real points, so of $\mathbb{Q}^{tr}$-points by Fried's "Branch cycle argument". So, all the G-covers in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ have their field of moduli contained in $\mathbb{Q}^{tr}$. Consider now one of the G-cover f in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}^n; r_1, r_2)$ and write $V(f)$ for a descent variety associated with f ; $V(f)$ is defined over $\mathbb{Q}^{tr}$. Since for any $\sigma \in \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ f^σ is defined over $\mathbb{R}$, $V(f^\sigma)(\mathbb{R}) \neq \emptyset$ and as $V(f^\sigma) \simeq V(f)^\sigma$, we get $V(f)^\sigma(\mathbb{R}) \neq \emptyset$. So, applying Moret-Bailly-Pop local-global principle on varieties, $V(f)(\mathbb{Q}^{tr}) \neq \emptyset$ that is, f is defined over $\mathbb{Q}^{tr}$. This is a special case of corollary 1.3 [DDoMo04]. □

3.5.2 Dihedral groups

Let $n \geq 3$ an integer and recall D_{2n} is given by the generators and relations

$$D_{2n} =< u, v | u^n = v^2 = 1, vuv = u^{-1} >$$

In our computations, we have to distinguish between three cases :
- $2 \not| n$ then, $Z(D_{2n}) = \{1\}$ and D_{2n} has $\frac{n-1}{2} + 1$ non trivial conjugacy classes :
- $\frac{n-1}{2}$ classes $A_1, ..., A_{n-1/2}$ with $A_i = \{u^i, u^{-i}\}$, $i = 1, ..., \frac{n-1}{2}$,
- $B = \{vu^i\}_{0 \leq i \leq n-1}$.
- $2 \mid n$ then $Z(D_{2n}) =< u^{\frac{n}{2}} >$ and D_{2n} has $\frac{n}{2} + 2$ non trivial conjugacy classes :
- $\frac{n}{2}$ classes $A_1, ..., A_{n/2}$ with $A_i = \{u^i, u^{-i}\}$, $i = 1, ..., \frac{n}{2}$,
- $B_1 = \{vu^{2i}\}_{0 \leq i \leq n/2-1}$, $B_2 = \{vu^{2i+1}\}_{0 \leq i \leq n/2-1}$.

In this situation, we will have to consider the case $4 \mid n$ ($\text{Inv}(\text{D}_{2n})/\text{Z}(\text{D}_{2n})$ is strictly contained in $Z(D_{2n})^{\frac{1}{2}}/Z(D_{2n})$) and $4 \not| n$ ($\text{Inv}(\text{D}_{2n})/\text{Z}(\text{D}_{2n}) = \text{Z}(\text{D}_{2n})^{\frac{1}{2}}/\text{Z}(\text{D}_{2n})$) separately.
We first carry out the computations and show that any dihedral group D_{2n} is the Galois group of a regular extension of $\mathbb{Q}^{tr}(X)$ with a four branch point rational divisor in configuration (C). If $2 \not| n$ we also show that for any $r \geq 3$ D_{2n} is the Galois group of a regular extension of $\mathbb{Q}^{tr}(X)$ with exactly r rational branch points (compare for instance with Conjecture 5.2 in [DF94])

3.5.2.1 Odd dihedral groups in configuration (C)

We take

$$\mathbf{C} = [A_1^{(a_1)}, ..., A_{n-1/2}^{(a_{n-1/2})}, B^{(b)}] \text{ (so } s = a_1 + ... + a_{n-1/2} + b)$$

and also write $a = a_1 + ... + a_{n-1/2}$. Here $\text{Inv}(D_{2n})/Z(D_{2n}) \cdot = \{1, \{vu^i\}_{0 \leq i \leq n-1}\}$ so we get for the $\alpha_{.,.}$:

	χ_1	χ_2	χ_{2+h} ; $1 \leq h \leq \frac{n-1}{2}$
1	2n	0	0
v	2	0	2

and for the $\mathbf{A}_\cdot$:

	χ_1	χ_2	χ_{2+h} ; $1 \leq h \leq \frac{n-1}{2}$
$\mathbf{A}_\cdot$	4n	0	2n

which, noticing that for $\mathbf{C}$ to be g-complete symetric we need $b \geq 1$, leads to :

$$\begin{cases} \mathbf{n}^{\mathbb{R}}(\mathbf{C};0,s) = 2^{a+1}n^b \\ |\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C};0,s)| = 2^a n^{b-1} \\ |\overline{\text{sni}}(\mathbf{C})| = 2^{2a-1}n^{2b-2} \\ \frac{|\overline{\text{sni}}(\mathbf{C})|}{|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C};0,s)|} = 2^{a-1}n^{b-1} \end{cases}$$

For instance, if $a_1 = b = 1$ and $a_2 = ... = a_{n-1/2} = 0$ we get $|\overline{\text{sni}}(\mathbf{C}^m)| = 2 = |\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}^n;0,s)|$ for all $m \geq 1$ such that $(2n,m) = 1$. As a result, if we choose a $2s$-tuple of branch points $\mathbf{t} = (z_1,...,z_s,\overline{z_s},...,\overline{z_1}) \in \mathcal{U}^r(\mathbb{C})$ the associated divisor of which is rational the discussion above shows that any point in $E_{4,D_{2n},\mathbf{t}}(\mathbf{C})$ is a $\mathbb{Q}^{tr}$-point and, since $Z(D_{2n}) = \{1\}$, we conclude all the G-covers in $\overline{\text{sni}}(\mathbf{C})$ are defined over $\mathbb{Q}^{tr}$. Notice that $\mathbf{C} = (C_1, C_v, C_v, C_1)$ is not rational, so all the G-covers in $\overline{\text{sni}}(\mathbf{C})$ are defined over $\mathbb{Q}^{tr}$ but none of them is over $\mathbb{Q}$.

3.5.2.2 Odd dihedral groups in configuration (R)

The example we give here corresponds to situation (R). For any $r \geq 3$ we exhibit G-covers with group D_{2n} defined over $\mathbb{Q}^{tr}$ (but not over $\mathbb{Q}$) and with r rational branch points. It also illustrates the difficulties one can encounter when trying to compute $\mathbf{n}^{\mathbb{R}}(\mathbf{C};r,0)$ directly. We will use the commutative diagram :

$$\begin{array}{ccc} \text{Inv}(G)^r & \xrightarrow{\theta} & G^{r-1} \\ \downarrow{\scriptstyle \pi} & \nearrow{\scriptstyle \overline{\theta}} & \\ \text{Inv}(G)^r/G\cdot & & \end{array}$$

where π is the canonical surjection and θ is the map given by the correspondence $(u_0,...,u_{r-1}) \to (u_0u_1, u_1u_2, ..., u_{r-2}u_{r-1})$. Rewrite $\mathbf{n}^{\mathbb{R}}(\mathbf{C};r,0)$ as follows (where c denotes as in §3.3.1 the r-cycle $(0,1,...,r-1)$) :

$$\begin{aligned} \mathbf{n}^{\mathbb{R}}(\mathbf{C};r,0) &= \frac{1}{Z_1...Z_r} \sum_{\substack{\chi_1,...,\chi_r \in \text{Irr}(G) \\ (u_0,...,u_{r-1}) \in \text{Inv}(G)^r/G\cdot}} \prod_{1 \leq i \leq r} (\chi_i(g_i)\chi_i(u_{i-1}u_{c(i-1)})) \\ &= \frac{1}{Z_1...Z_r} \sum_{(u_0,...,u_{r-1}) \in \text{Inv}(G)^r/G\cdot} \prod_{1 \leq i \leq r} \left(\sum_{\chi \in \text{Irr}(G)} \chi(g_i)\chi(u_{i-1}u_{c(i-1)}) \right) \end{aligned}$$

and also recall the general form of Serre's formula :

$$|\Sigma(\mathbf{C},G)| = \frac{|C_1|...|C_r|}{|G|} \sum_{\chi \in \text{Irr}(G)} \frac{\prod_{1 \leq i \leq r} \chi(g_i)}{\chi(1)^{r-2}}$$

When $G = D_{2n}$, we have $\overline{\chi} = \chi$ for any irreducible character $\chi \in \text{Irr}(D_{2n})$, so we get $\sum_{\chi \in \text{Irr}(G)} \chi(g_i)\chi(u_{i-1}u_{c(i-1)}) = \sum_{\chi \in \text{Irr}(G)} \overline{\chi(g_i)}\chi(u_{i-1}u_{c(i-1)})$ is equal to Z_i if g_i and $u_{i-1}u_{c(i-1)}$ are conjugate, and is equal to 0 otherwise, for $i = 1,...,r$. Consequently, the only tuples $\underline{u} = (u_0,...,u_{r-1}) \in \text{Inv}(G)/G\cdot$ we will need in our computation are the $(\overline{\theta}^{-1}(g_1^{\gamma_1},...,g_{r-1}^{\gamma_{r-1}}))_{\gamma_1,...,\gamma_{r-1} \in G}$ when they exist. So,

$$\mathbf{n}^{\mathbb{R}}(\mathbf{C};r,0) = \frac{1}{Z_r} \sum_{\underline{u} \in \overline{\theta}^{-1}(C_1 \times ... \times C_{r-1})} \sum_{\chi \in \text{Irr}(G)} \overline{\chi(g_r)}\chi(u_{r-1}u_0)$$

With the notations of 3.5.2 let us try and apply these remarks to the specific r-tuple

$$\mathbf{C} = (B, A_{i_1}, ..., A_{i_t}, B) \text{ (so } r = t+2)$$

where we choose $1 \leq i_1, ..., i_t \leq \frac{n-1}{2}$ so that $\mathbf{C}$ is g-complete. A representative of $\overline{\theta}^{-1}(vu^k, u^{\epsilon_1 i_1}, ..., u^{\epsilon_t i_t})$ is $(1, vu^k, vu^{k+\epsilon_1 i_1}, ..., vu^{k+\epsilon_1 i_1 + ... + \epsilon_t i_t})$, $k = 0, ..., n-1$, $\epsilon_1, ..., \epsilon_t \in \{\pm 1\}$. Moreover, since $u_{r-1}u_0 = vu^{k+\epsilon_1 i_1 + ... + \epsilon_t i_t} \in B$, we obtain :

$$\mathbf{n}^{\mathbb{R}}(\mathbf{C}; r, 0) = \frac{1}{2^2 n^t} \sum_{\epsilon_1, ..., \epsilon_t \in \{\pm 1\}} \sum_{k=0}^{n-1} 2 \times n^t \times 2 = 2^t n$$

Hence on the one hand for all $m \geq 1$ such that $(2n, m) = 1$ we have $|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}^m; r, 0)| = 2^{t-1}$ and on the other hand, by Serre's formula : $|\overline{\text{sni}}(\mathbf{C})| = 2^{t-1}$. So if we fix a r-tuple of rational branch points $\mathbf{t} = (t_1, ..., t_r) \in \mathcal{U}^r(\mathbb{Q})$, using the same argument as above we get that all the G-covers in $\overline{\text{sni}}(\mathbf{C})$ are defined over $\mathbb{Q}^{tr}$. Moreover choosing for instance $i_1 = ... = i_t = 1$, we can assert those G-covers are not defined over $\mathbb{Q}$.

Remark 3.20 The computation we made above can be generalized to any tuple

$$\mathbf{C} = (B, A_{i_{1,1}}, ..., A_{i_{1,u_1}}, B, B, A_{i_{2,1}}, ..., A_{i_{2,u_2}}, B, B, ..., B, A_{i_{t,1}}, ..., A_{i_{t,u_t}})$$

with $r = 2t + u_1 + ... + u_t$, we obtain $|sni^{\mathbb{R}}(\mathbf{C}; r, 0)| = 2^{u_1 + ... + u_t - 1} n^{t-1}$ and $|\overline{\text{sni}}(\mathbf{C})| = 2^{u_1 + ... + u_t - 1} n^{2t-2}$, so $\frac{|\overline{\text{sni}}(\mathbf{C})|}{|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; r, 0)|} = n^{t-1}$ which only depends on t.

3.5.2.3 Even dihedral groups in configuration (C)

Take

$$\mathbf{C} = [A_1^{(a_1)}, ..., A_{n/2}^{(a_{n/2})}, B_1^{(b_1)}, B_2^{(b_2)}]$$

and also write $a = a_1 + ... + a_{n/2-1}$, $b = b_1 + b_2$ so $s = a + a_{n/2} + b$.

Suppose first $4 \mid n$, then

- $\text{Inv}(\text{D}_{2\text{n}})/\text{Z}(\text{D}_{2\text{n}}) = \{1, \{\text{vu}^{2\text{i}}\}_{0 \leq \text{i} \leq \text{n}/4-1}, \{\text{vu}^{2\text{i}+1}\}_{0 \leq \text{i} \leq \text{n}/4-1}\}$.
- $Z(D_{2n})^{\frac{1}{2}}/Z(D_{2n}) = \{1, \{vu^{2i}\}_{0 \leq i \leq n/4-1}, \{vu^{2i+1}\}_{0 \leq i \leq n/4-1}, u^{\frac{n}{4}}\}$.

so, we get for the $\alpha_{.,.}$:

	1	$u^{\frac{n}{4}}$	v	vu
χ_1	2n	n	4	4
χ_2	0	0	0	4
χ_3	0	n	0	0
χ_4	0	0	4	0
χ_{4+h} ; $1 \leq h \leq \frac{n}{2} - 1$ and $2 \mid h$	0	0	4	4
χ_{4+h} ; $1 \leq h \leq \frac{n}{2} - 1$ and $2 \not\mid h$	0	0	0	0

and for the $\mathbf{A}_{.}^{mod}$, $\mathbf{A}_{.}$:

	χ_1	χ_2	χ_3	χ_4	χ_{4+h} ; $1 \leq h \leq \frac{n}{2} - 1$ and $2 \mid h$	χ_{4+h} ; $1 \leq h \leq \frac{n}{2} - 1$ and $2 \not\mid h$
$\mathbf{A}_{.}$	4n	n	0	n	2n	0
$\mathbf{A}_{.}^{mod}$	5n	n	n	n	2n	0

So, we get :

$$\begin{cases} |\overline{\text{sni}}(\mathbf{C})| = 2^{2(a-b)+1} n^{2(b-1)} \\ |\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{C}; 0, a+b+a_{n/2})| = 2^{a-b-1} n^{b-1} (5 + (-1)^b + (-1)^{\sum_{i=1}^{n/2} i a_i} ((-1)^{b_1} + (-1)^{b_2})) \\ |\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; 0, a+b+a_{n/2})| = 2^{a-b-1} n^{b-1} (4 + (-1)^{\sum_{i=1}^{n/2} i a_i} ((-1)^{b_1} + (-1)^{b_2})) \end{cases}$$

So, for instance, taking $b_1 = 1, a_1 = 1, b_2 = a_2 = ... = a_{n/2} = 0$ we obtain $|\overline{\text{sni}}(\mathbf{C})| = 2 = |\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; 0, 2)|$. So, all the G-covers in $\overline{\text{sni}}(\mathbf{C})$ are defined over $\mathbb{Q}^{tr}$.
Suppose now $4 \not| n$ then

$$\text{Inv}(\text{D}_{2\text{n}})/\text{Z}(\text{D}_{2\text{n}}) = \{1, \{\text{vu}^{2\text{i}}\}_{0\leq \text{i} \leq \text{n}/2-1}\} = \text{Z}(\text{D}_{2\text{n}})^{\frac{1}{2}}/\text{Z}(\text{D}_{2\text{n}})$$

so, we get for the $\alpha_{.,.}$:

	χ_1	χ_2	χ_3	χ_4
1	2n	0	0	0
v	4	0	0	0

and for the $\mathbf{A}_.$:

	χ_1	χ_2	χ_3	χ_4
$\mathbf{A}_.$	4n	0	0	0

(We do not carry out the computations for the χ_{4+h} ; $1 \leq h \leq \frac{n}{2} - 1$, since they play no part in the computations of $|\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; 0, a + b + a_{n/2})|$.) So, we get :

$$\begin{cases} |\overline{\text{sni}}(\mathbf{C})| = 2^{2(a-b)+1} n^{2(b-1)} \\ |\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; 0, a + b + a_{n/2})| = 2^{a-b+1} n^{b-1} \end{cases}$$

So, for instance, taking $b_1 = 1, a_1 = 1, b_2 = a_2 = ... = a_{n/2} = 0$ we obtain $|\overline{\text{sni}}(\mathbf{C})| = 2 = |\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}; 0, 2)|$. So, all the G-covers in $\overline{\text{sni}}(\mathbf{C})$ are defined over $\mathbb{Q}^{tr}$.

3.5.2.4 Application to regular realizations of D_{2a^∞} (with $a \geq 3$) over $\mathbb{Q}^{tr}(X)$

The results obtained in 3.5.2.1, 3.5.2.2 and 3.5.2.3 do not depend on $n \geq 3$, which yields regular realizations of the profinite groups $D_{2a^\infty} := \varprojlim_{n \geq 0} D_{2a^n} \simeq \mathbb{Z}_a \rtimes \mathbb{Z}/2\mathbb{Z}$, $a \geq 3$, over $\mathbb{Q}^{tr}(X)$. Indeed, for any $a \geq 3$ and for any $n \geq 1$ write
- $A_{1,a,n}, ..., A_{a^n-1/2,a,n}$ with $A_i = \{u^i, u^{-i}\}$, $i = 1, ..., \frac{a^n-1}{2}$,
- $B_{a,n} = \{vu^i\}_{0 \leq i \leq a^n - 1}$ if $2 \not| a$ and $B_{a,n} = \{vu^{2i}\}_{0 \leq i \leq \frac{a^n}{2} - 1}$ else.
for the non trivial conjugacy classes of D_{2a^n}. Also set $\mathbf{C}_{a,n} = (A_{1,a,n}, B_{a,n}, B_{a,n}, A_{1,a,n})$. This gives rise to a tower of Hurwitz spaces

$$\cdots \to \mathcal{H}'_{4,D_{2a^{n+1}}}(\mathbf{C}_{a,n+1}) \to \mathcal{H}'_{4,D_{2a^n}}(\mathbf{C}_{a,n}) \to \cdots \to \mathcal{H}'_{4,D_{2a}}(\mathbf{C}_{a,1})$$

Fix $\mathbf{t}' = (z_1, \overline{z}_1, z_2, \overline{z}_2) \in \mathcal{U}^4(\mathbb{C})$ with $z_i \in \mathbb{P}^1(\mathbb{C}) \backslash \mathbb{P}^1(\mathbb{R})$ and $\{z_i, \overline{z}_i\} \in \mathcal{U}_2(\mathbb{Q})$, $i = 1, 2$, and consider the projective system of finite sets of $\mathbb{Q}^{tr}$-points

$$\cdots \to \Pi_4(\mathcal{H}'_{4,D_{2a^{n+1}}}(\mathbf{C}_{a,n+1})_{\mathbf{t}'}) \to \Pi_4(\mathcal{H}'_{4,D_{2a^n}}(\mathbf{C}_{a,n})_{\mathbf{t}'}) \to \cdots \to \Pi_4(\mathcal{H}'_{4,D_{2a^1}}(\mathbf{C}_{a,1})_{\mathbf{t}'})$$

then, $\varprojlim_{n \geq 0} \Pi_4(\mathcal{H}'_{4,D_{2a^n}}(\mathbf{C}_{a,n})_{\mathbf{t}'}) \neq \emptyset$ and, according to 3.5.2.1 and 3.5.2.3, any $\mathbf{p} \in \varprojlim_{n \geq 0} \Pi_4(\mathcal{H}'_{4,D_{2a^n}}(\mathbf{C}_{a,n})_{\mathbf{t}'})$ corresponds to a regular Galois realization of D_{2a^∞} over $\mathbb{Q}^{tr}(X)$ with branch points $\mathbf{t}'$ and inertia canonical invariant $(A_{1,a,\infty}, B_{a,\infty}, B_{a,\infty}, A_{1,a,\infty})$ (where $B_{a,\infty} = \{vu^i\}_{i \geq 0}$ if $2 \not| a$, $B_{a,\infty} = \{vu^{2i}\}_{i \geq 0}$ else and $A_{i,a,\infty} = \{u^i, u^{-i}\}$, $i \geq 1$) *cf* §5.3.1. (Likewise, if $2 \not| a$ using the results of 3.5.2.2, one gets regular Galois realization of D_{2a^∞} over $\mathbb{Q}^{tr}(X)$ with rational branch points $\mathbf{t}' = (t_1, ..., t_{t+2}) \in \mathcal{U}^{t+2}(\mathbb{Q})$ and inertia canonical invariant $(B_{a,\infty}, A_{i_1,a,\infty}, ..., A_{i_t,a,\infty}, B_{a,\infty})$ where $i_1, ..., i_t \geq 1$ such that, for instance, $(i_j, a) = 1$, $j = 1, ..., t$.) As a result, we can state :

Theorem 3.21 (Regular realization of D_{2a^∞} over $\mathbb{Q}^{tr}(X)$) *For any $a \geq 3$ the profinite group $D_{2a^\infty} = \mathbb{Z}_a \rtimes \mathbb{Z}/2\mathbb{Z}$ is the Galois group of a regular extension $K/\mathbb{Q}^{tr}(X)$ with a four branch point rational divisor in configuration (C) and inertia canonical invariant $(A_{1,a,\infty}, B_{a,\infty}, B_{a,\infty}, A_{1,a,\infty})$.*

This statement, as stressed in the introduction, is the first one giving a non trivial (That is, which is not already defined over $\mathbb{Q}$) regular realization of a profinite group over $\mathbb{Q}^{tr}(X)$. This - though our method probably works only for very specific groups - show the problem raised in section 4.3(b) of [DDes04] can have positive answers in non trivial situations.

Remark 3.22 Actually, our argument also trivially works for any profinite abelian group $A = \varprojlim_{n\geq 0} A_n$. since one can always build a projective system of g-complete symetric tuples $\{\mathbf{a}_n = (a_{1,n}, ..., a_{s_n,n}, -a_{s_n,n}, ..., -a_{1,n})\}_{n\geq 0}$ as well as a corresponding sequence of branch points $(\mathbf{t}'_n = (z_{1,n}, ..., z_{s_n,n}, \overline{z}_{s_n,n}, ..., \overline{z}_{1,n}))_{n\geq 0}$ (where $z_{i,n+1} = z_{i,n}$ for $1 \leq i \leq s_n$, $n \geq 0$). Then for any $n \geq 0$ and any $m \geq 1$ such that $(|A_n|, m) = 1$ we have $|\overline{sni}(\{m\mathbf{a}_n\}, A_n)| = 1 = |\overline{sni}^{\mathbb{R}}(\{m\mathbf{a}_n\}; 0, s_n)|$, so we get a regular realization of A over $\mathbb{Q}^{tr}(X)$. If, futhermore, A is of finite rang r, this realization can be chosen with a $2r$-branch point rational divisor in configuration (C).

3.5.3 A family generalizing dihedral groups

Let $m \geq 3$, $n \geq 1$ two integers and write

$$U_{m,n} =< u, v | u^m = v^{2n} = 1, vuv^{-1} = u^{-1} >$$

(Observe that $U_{m,1} = D_{2m}$, $m \geq 3$). We will not carry out all the computations for these groups but we will only consider the case $2 \not| m$. Then $U_{m,n}$ has $n(2 + \frac{m-1}{2})$ conjugacy classes :
- $n\frac{m+1}{2}$ classes $A_{i,j} = \{v^{2i}u^j, v^{2i}u^{-j}\}$, $i = 0, ..., n-1$, $j = 0, ..., \frac{m-1}{2}$.
- n classes $B_i = \{v^{2i+1}u^j\}_{0\leq j\leq m-1}$, $i = 0, ..., n-1$.

and we have
- $Z(U_{m,n}) =< v^2 >$.
- $\begin{array}{rcl} \mathrm{Inv(U_{m,n})} & = & \{1, v^n\} \text{ if } 2 \mid n \\ & = & \{1, \{v^n u^j\}_{0\leq j\leq m-1}\} \text{ else.} \end{array}$
- $Z(U_{m,n})^{\frac{1}{2}} = \{\{v^i\}_{0\leq i\leq 2n-1}, \{v^{2i+1}u^j\}_{\substack{0\leq i\leq n-1 \\ 1\leq j\leq m-1}}\}$ Taking

$$\mathbf{C} = [A_{i,j}^{(a_{i,j})},\ i = 0, ..., n-1,\ j = 0, ..., \frac{m-1}{2},\ (i,j) \neq (0,0),\ B_i^{(b_i)},\ i = 0, ..., n-1]$$

and setting $a = \sum_{j=1}^{\frac{m-1}{2}} \sum_{i=0}^{n-1} a_{i,j}$, $b = \sum_{i=1}^{m-1}$ (so $s = a + b + \sum_{i=0}^{n-1} a_{i,0}$) we get, noticing that for $\mathbf{C}$ to be g-complete symetric we need $b \geq 1$:

$$\begin{cases} |\overline{\mathrm{sni}}(\mathbf{C})| = 2^{2a-1}m^{2(b-1)} \\ |\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; 0, s)| = 2^a m^{b-1} \\ |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, s)| = \begin{array}{ll} 2^a m^{b-1} & \text{if } 2 \not| n \\ 2^{a-1}m^{b-1} & \text{else.} \end{array} \end{cases}$$

As a result, taking $a_{0,1} = b_0 = 1$, $a_{i,j} = b_k = 0$ if $(i,j) \neq (0,1)$, $k \neq 0$ we obtain $|\overline{\mathrm{sni}}(\mathbf{C})| = |\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; 0, 2)| = |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, 2)| = 2$ if $2 \not| n$ and $|\overline{\mathrm{sni}}(\mathbf{C}, U_{m,n})| = 2 = |\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; 0, 2)|$, $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, 2)| = 1$ else. So, when $2 \not| n$ the two G-covers in $\overline{\mathrm{sni}}(\mathbf{C})$ are defined over $\mathbb{Q}^{tr}$ and when $2 \mid n$ one of them is defined over $\mathbb{R}$ whereas the other is not, but both of them have their field of moduli contained in $\mathbb{Q}^{tr}$. Applying the argument of 3.5.2.4, we obtain *For any $b \geq 1$, for any $a \geq 3$ such that $2 \not| a$ the profinite group $U_{a^\infty,b} := \varprojlim_{n\geq 0} U_{a^n,b}$ is the Galois group of a regular extension of $\mathbb{Q}^{tr}(X)$ with a four branch point rational divisor in configuration (C).* Likewise, one can consider the projective groups U_{a,b^∞} or U_{a^∞,b^∞}.

3.6 Examples of computations

3.6.1 $F_{p,q}$ with p, q prime number such that $p > q$ and $p|q-1$

First recall that for any prime numbers p, q such that $p > q$ we have :
(1) if $q \not| p-1$ then any group G with order pq is abelian.

(2) if $q \mid p-1$ then any group G with order pq is either abelian or isomorphic to $F_{p,q}$.
where $F_{p,q}$ is the group given by the generators and relations $F_{p,q} =< a, b | a^p = b^q = 1, b^{-1}ab = a^u >$ with $u \in \mathbb{Z}/p\mathbb{Z}^*$ of order q . Fixing $v_1, ..., v_s$, a system of representative of $\mathbb{Z}/p\mathbb{Z}^*/ < u >$ (where $s = \frac{p-1}{q}$), we obtain the following description of $F_{p,q}$:
$F_{p,q} = \{a^x b^y\}_{\substack{0 \le x \le p-1 \\ 0 \le y \le q-1}}$. When $q = 2$, $F_{p,2} = D_{2p}$, so we will always assume $q > 2$.
And $F_{p,q}$ has $s + q - 1$ non trivial conjugacy classes :
- s classes $A_1, ..., A_s$ with $A_i = \{a^{v_i u^j}\}_{0 \le j \le q-1}, i = 1, ..., s$.
- $q-1$ classes $B_1, ..., B_{q-1}$ with $B_i = \{a^j b^i\}_{0 \le j \le p-1}$, $i = 1, ..., q-1$.
Take

$$\mathbf{C} = [A_1^{(a_1)}, ..., A_s^{(a_s)}, B_1^{(b_1)}, ..., B_{q-1}^{(b_{q-1})}]$$

We also write $\alpha = \sum_{1 \le i \le s} a_i$ and $\beta = \sum_{1 \le n \le q-1} b_n$, so $r = \alpha + \beta$ When q is odd we have $\mathrm{Inv}(F_{p,q})/Z(F_{p,q}) \cdot = \{1\}$ so $\mathbf{A}_{\chi_{\mathbf{1,0}}} = \alpha_{\chi_{1,0},1} = pq$ and $\forall \chi \neq \chi_{1,0}$ $\mathbf{A}_\chi = \alpha_{\chi,1} = 0$.
So we get, noticing that for $\mathbf{C}$ to be g-complete symetric we need $a, b \ge 1$:

$$\begin{cases} - \ \mathbf{n}^{\mathbb{R}}(\mathbf{C}; 0, s) = \frac{q^a p^b}{pq} \times pq = q^a p^b \\ - \ |\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, s)| = q^{a-1} p^{b-1} \\ - \ |\overline{\mathrm{sni}}(\mathbf{C}, F_{p,q})| = q^{2a-1} p^{2b-2} \\ - \ \frac{|\overline{\mathrm{sni}}(\mathbf{C}, F_{p,q})|}{|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, s)|} = q^a p^{b-1} \end{cases}$$

For instance, if $a_1 = b_1 = 1$ et $a_2 = ... = a_r = b_2 = ... = b_{q-1} = 0$ we get $|\overline{\mathrm{sni}}(\mathbf{C}, F_{p,q})| = q$ and $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, s)| = 1$.

3.6.2 The Mathieu group M_{11}

Our formulas are manageable even for more complicated groups, particularly in the branch point configuration (C). In our last example, the group is the Mathieu group M_{11}.

According to the Atlas $|M_{11}| = 11.5.3^2.2^4$ and M_{11} has 10 conjugacy classes : 1A, 2A, 3A, 4A, 5A, 6A, 8A, B*, 11A, B**. The difficulty here is to compute $\mathrm{Cen}_{M_{11}}(2A)$. We apply theorem 3.4 to the specific 4-tuple (8A,B*,11A,B**) to do this. We will use that $|\mathrm{Cen}_{M_{11}}(2A)| = 3.2^4$ and that any 2-Sylow S_2 of $\mathrm{Cen}_{M_{11}}(2A)$ is semidihedral with order 16 i.e. $S_2 = < x, a \mid x^2 = 1 = a^8, xax = a^3 > = SD_{16}$ (cf. [R82] Ex. 7.4.4 p.205) to prove the following lemma, which is needed to carry out computations of $\mathbf{n}^{\mathbb{R}}(\mathbf{C}; 0, s)$.

Lemma 3.23 $\mathrm{Cen}_{M_{11}}(2A)$ *contains : 1 element with order 1, 13 elements with order 2, 8 elements with order 3, 6 elements with order 4, 8 elements with order 6, 12 elements with order 8 (6 in each conjugacy class).*

First, note that SD_{16} contains :
- 4 elements with order 8 : a, a^3, a^5, a^7
- 6 elements with order 4 : a^2, a^6, xa, xa^3, xa^5, xa^7
- 5 elements with order 2 : a^4, xa^2, xa^4, xa^6, x
- 1 element with order 1 : 1
Moreover, $Z(SD_{16}) =< a^4 >$ and SD_{16} has 3 kinds of subgroups of index 2 : $\mathbb{Z}/8\mathbb{Z} =< a >$, $D_8 =< a^2, x >$, $\mathbb{H}_8 =< a^2, xa >$.

We are now able to describe $\mathrm{Cen}_{M_{11}}(2A)$ more precisely. According to the Atlas, there is an unsplit short exact sequence : $1 \to \mathbb{Z}/2\mathbb{Z} \to \mathrm{Cen}_{M_{11}}(2A) \xrightarrow{\theta} S_4 \to 1$. So, as the center of S_4 is trivial, we get the inclusions $< 2A > \subset Z(\mathrm{Cen}_{M_{11}}(2A)) \subset \mathbb{Z}/2\mathbb{Z}$, which obviously are equalities. Consequently, for all $\sigma \in S_4$:
- If σ has order $2k+1, k = 0, 1$ then $\theta^{-1}(\sigma)$ contains an element with order $2k+1$ and an element with order $4k+2$.

- If σ has order 2 then $\theta^{-1}(\sigma)$ contains either two elements with order 2 or two elements with order 4 or two elements with order 6. Let us denote by n the number of elements with order 6 we obtain this way ($0 \leq n \leq 6$).
- If σ has order 4 then $\theta^{-1}(\sigma)$ contains either two elements with order 4 or two elements with order 8. In particular, we have exactly 8 elements with order 3 and $8+n$ elements with order 6 in $\mathrm{Cen}_{M_{11}}(2A)$. All the other ones have order 1,2,4 or 8, so are contained in the 2-Sylow subgroups of $\mathrm{Cen}_{M_{11}}(2A)$. Let us write n_p for the number of p-Sylows in $\mathrm{Cen}_{M_{11}}(2A)$. From the above we deduce $n_3 = 4$. Furthermore, since $n_2|3$ and $n_2 \equiv 1$ [mod2] we have $n_2 = 1, 3$. But if $n_2 = 1$, $|\mathrm{Cen}_{M_{11}}(2A)| = 32+n$: a contradiction, hence $n_2 = 3$. Still according to the Atlas $\mathrm{Cen}_{M_{11}}(2A)$ contains a normal subgroup with order 8, V, and as the 2-Sylows of $\mathrm{Cen}_{M_{11}}(2A)$ are conjugate, for all $S, T \in \mathcal{S}_2(\mathrm{Cen}_{M_{11}}(2A))$ we get $S \cap T = V$. Consequently, computing the order of $\mathrm{Cen}_{M_{11}}(2A)$ we get now $|\mathrm{Cen}_{M_{11}}(2A)| = 48 + n$, which leads to $n = 0$. There are 4 possibilities for V :

1/ $V = \mathbb{Z}/8\mathbb{Z}$ and we have in $\mathrm{Cen}_{M_{11}}(2A)$: 1 element with order 1, 13 elements with order 2, 8 elements with order 3, 14 elements with order 4, 8 elements with order 6, 4 elements with order 8 (2 in each conjugacy class).

2/ $V = D_8$ and we have in $\mathrm{Cen}_{M_{11}}(2A)$: 1 element with order 1, 5 elements with order 2, 8 elements with order 3, 14 elements with order 4, 8 elements with order 6, 12 elements with order 8 (6 in each conjugacy class).

3/ $V = \mathbb{H}_8$ and we have in $\mathrm{Cen}_{M_{11}}(2A)$: 1 element with order 1, 13 elements with order 2, 8 elements with order 3, 6 elements with order 4, 8 elements with order 6, 12 elements with order 8 (6 in each conjugacy class).

Here are the computations corresponding to the three configurations above :

	A_{χ_1}	A_{χ_2}	A_{χ_3}	A_{χ_4}	A_{χ_5}	A_{χ_6}	A_{χ_7}	A_{χ_8}	A_{χ_9}	$A_{\chi_{10}}$
$V = \mathbb{Z}/8\mathbb{Z}$	15840	10560	0	0	7920	0	0	15840	2640	5280
$V = D_8$	15840	7920	2640	2640	2640	0	0	10560	5280	7920
$V = \mathbb{H}_8$	15840	7920	0	0	7920	0	0	15840	0	7920

Finally, since the maximal subgroups of M_{11} have order 720, 660, 144, 120, 48 and none of these orders can be divided by both 8 and 11, we conclude that (8A, B*, 11A, B**) is g-complete symetric. Now, the first two configurations give $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, 2)| = \frac{538}{3}$ and $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, 2)| = \frac{536}{3}$ respectively whereas the third one gives $|\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; 0, 2)| = 180$. So $V = \mathbb{H}_8$, which gives a description of the centralizer of the involution class in M_{11}. For this 4-uple Serre's formula gives $|\overline{\mathrm{sni}}(\mathbf{C})| = 8752$.

3.7 the case of mere covers

The computations we made for G-covers can be generalized to mere covers easily. We give here the statements and proofs only for configurations (R) and (C). Before explaining how to describe the mere covers with field of moduli contained in $\mathbb{R}$ or defined over $\mathbb{R}$ in terms of Nielsen classes, we introduce the notations we will use. We then state the theorems and prove them.

3.7.1 Notations and statements

3.7.1.1 Notations

We fix a transitive permutation representation of G $T : G \hookrightarrow \mathcal{S}_n$, a real branch point divisor $\mathbf{t} = \{t_1, ..., t_{r_1}, z_1\overline{z}_1, ..., z_{r_2}, \overline{z}_{r_2}\} \in \mathcal{U}_r(\mathbb{R})$ with the usual convention and an r-tuple $\mathbf{C} = (C_1, ..., C_r)$ of non trivial conjugacy classes of G. We introduce then the straight normalizer

$$\mathrm{SN(G, \mathbf{C})} = \{\sigma \in \mathrm{Nor}_{\mathcal{S}_n}(\mathrm{G}) \mid \sigma \mathrm{C_i} \sigma^{-1} = \mathrm{C_i},\ \mathrm{i} = 1, ..., \mathrm{r}\}$$

and the absolute Nielsen class

$$\mathrm{Sni}^{\mathrm{ab}}(\mathbf{C},\mathrm{G}) = \left\{ (g_1,...,g_r) \in G^r \;\middle|\; \begin{array}{l} (1)\ G =< g_1,...,g_r > \\ (2)\ g_1\cdots g_r = 1 \\ (3)\ g_i \in C_i,\ i=1,...,r \end{array} \right\}$$

As in 3.1, we also define the subsets of $\mathrm{Sni}^{\mathrm{ab}}(\mathbf{C},\mathrm{G})$ corresponding to covers with field of moduli contained in $\mathbb{R}$, $\mathrm{Sni}^{\mathrm{ab,mod},\mathbb{R}}(\mathbf{C};\mathrm{r}_1,\mathrm{r}_2)$ and defined over $\mathbb{R}$, $\mathrm{Sni}^{\mathrm{ab},\mathbb{R}}(\mathbf{C};\mathrm{r}_1,\mathrm{r}_2)$ that is,

– the set $\mathrm{Sni}^{\mathrm{ab,mod},\mathbb{R}}(\mathbf{C};\mathrm{r}_1,\mathrm{r}_2)$ consists of those $(g_1,...,g_r)$ in $\mathrm{Sni}^{\mathrm{ab}}(\mathbf{C},\mathrm{G})$ verifying the additional condition

(5) there exists $\sigma \in \mathrm{SN}(\mathrm{G},\mathbf{C})$ such that
- $\sigma g_1\cdots g_i\sigma^{-1} = (g_1\cdots g_i)^{-1}$, $i=1,...,r_1$
- $\sigma g_{r_1+i}\sigma^{-1} = g_{r_1+i-1}$, $i=1,...,2r_2$

– the set $\mathrm{Sni}^{\mathrm{ab},\mathbb{R}}(\mathbf{C};\mathrm{r}_1,\mathrm{r}_2)$ consists of those $(g_1,...,g_r)$ in $\mathrm{Sni}^{\mathrm{ab,mod},\mathbb{R}}(\mathbf{C};\mathrm{r}_1,\mathrm{r}_2)$ for which

(5)' in addition to (5) σ can be taken in such a way that $\sigma^2 = 1$

Observe that, in (5), the generating condition (1) $G =< g_1, g_1g_2, ..., g_1g_2\cdots g_{r_1}, g_{r_1+1}, ..., g_r >$ implies that $\sigma^2 \in \mathrm{Cen}_{\mathrm{SN}(\mathrm{G},\mathbf{C})}(\mathrm{G})$. So we can rewrite (5) this way
(5) there exists $\sigma \in \mathrm{SN}(\mathrm{G},\mathbf{C})$ such that $\sigma^2 \in \mathrm{Cen}_{\mathrm{SN}(\mathrm{G},\mathbf{C})}(\mathrm{G})$ and
- $\sigma g_1\cdots g_i\sigma^{-1} = (g_1\cdots g_i)^{-1}$, $i=1,...,r_1$
- $\sigma g_{r_1+i}\sigma^{-1} = g_{r_1+i-1}$, $i=1,...,r_2$

We write $\Sigma^{ab}(\mathbf{C},G)$, $\Sigma^{ab,mod,\mathbb{R}}(\mathbf{C};r_1,r_2)$, $\Sigma^{ab,\mathbb{R}}(\mathbf{C};r_1,r_2)$ for the sets obtained by removing the generating condition (1) and $\overline{\mathrm{sni}}^{ab}(\mathbf{C},G)$, $\overline{\mathrm{sni}}^{ab,mod,\mathbb{R}}(\mathbf{C};r_1,r_2)$, $\overline{\mathrm{sni}}^{ab,\mathbb{R}}(\mathbf{C};r_1,r_2)$ for the quotient sets modulo $\mathrm{SN}(\mathrm{G},\mathbf{C})$. We still have

$$\begin{aligned} |\overline{\mathrm{sni}}^{ab}(\mathbf{C},G)| &= \tfrac{|\mathrm{Sni}^{\mathrm{ab}}(\mathbf{C},\mathrm{G})|}{[\mathrm{SN}(\mathrm{G},\mathbf{C}):\mathrm{Cen}_{\mathrm{SN}(\mathrm{G},\mathbf{C})}(\mathrm{G})]} \leq \frac{|\Sigma^{ab}(\mathbf{C},G)|}{[\mathrm{SN}(\mathrm{G},\mathbf{C}):\mathrm{Cen}_{\mathrm{SN}(\mathrm{G},\mathbf{C})}(\mathrm{G})]} \\ |\overline{\mathrm{sni}}^{ab,(mod),\mathbb{R}}(\mathbf{C},G)| &= \tfrac{|\mathrm{Sni}^{\mathrm{ab},(\mathrm{mod}),\mathbb{R}}(\mathbf{C},\mathrm{G})|}{[\mathrm{SN}(\mathrm{G},\mathbf{C}):\mathrm{Cen}_{\mathrm{SN}(\mathrm{G},\mathbf{C})}(\mathrm{G})]} \leq \frac{|\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C},G)|}{[\mathrm{SN}(\mathrm{G},\mathbf{C}):\mathrm{Cen}_{\mathrm{SN}(\mathrm{G},\mathbf{C})}(\mathrm{G})]} \end{aligned}$$

For the computations, we will also set

$$\begin{aligned} U^{mod}(\mathbf{C}) &= \{\sigma \in \mathrm{SN}(\mathrm{G},\mathbf{C}) \mid \sigma^2 \in \mathrm{Cen}_{\mathrm{SN}(\mathrm{G},\mathbf{C})}(\mathrm{G})\} \\ U(\mathbf{C}) &= \{\sigma \in \mathrm{SN}(\mathrm{G},\mathbf{C}) \mid \sigma^2 = 1\} \end{aligned}$$

3.7.1.2 Mere covers and Nielsen class

Fix an ordered branch point set $\mathbf{t}' = (t_1,...,t_{r_1,z_1,\overline{z}_1,...,z_{r_2},\overline{z}_{r_2}}) \in \mathcal{U}^r(\mathbb{C})$, the associated branch point divisor of which, $\mathbf{t}$, is real and a topological bouquet $\underline{\gamma}$ for $\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t}$ as in 3.1. Then the monodromy gives a bijective correspondence between $(\Psi^{ab}_{r,G})^{-1}(\mathbf{t})$ that is, the isomorphism classes of degree n connected mere covers of $\mathbb{P}^1_{\mathbb{C}}$ with branch point divisor $\mathbf{t}$, and isomorphism classes of transitive representations $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t},t_0) \twoheadrightarrow \mathcal{S}_n$. When fixing the monodromy group $G \hookrightarrow \mathcal{S}_n$ and the inertia canonical invariant $\mathbf{C} \in G/\mathrm{Int}(\mathrm{G})$ we obtain a bijective correspondence between the isomorphism classes of degree n connected mere covers of $\mathbb{P}^1_{\mathbb{C}}$ with branch point divisor $\mathbf{t}'$, monodromy group G, inertia canonical invariant $\mathbf{C}$ and $\overline{sni}^{ab}(\mathbf{C},G)$. And, in this correspondence, the subset $\overline{sni}^{ab,mod,\mathbb{R}}(\mathbf{C};r_1,r_2)$ corresponds to mere covers with field of moduli contained in $\mathbb{R}$. Likewise, the subset $\overline{sni}^{ab,\mathbb{R}}(\mathbf{C};r_1,r_2)$ corresponds to mere covers defined over

$\mathbb{R}$.

Proof. Given $\underline{\gamma}$ as in 3.1, we get

$$\begin{cases} \gamma_i^c = (\gamma_1 \cdots \gamma_{i-1})\gamma_i^{-1}(\gamma_1 \cdots \gamma_{i-1})^{-1},\ i = 1, ..., r_1 \\ \gamma_{r_1+i}^c = \gamma_{r+1-i}^{-1},\ i = 1, ..., 2r_2 \end{cases}$$

And, for any $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$ degree n connected mere cover with monodromy group G and branch point divisor $\mathbf{t}$, $BCD_{\underline{\gamma}}(\phi^c) = (T_\phi(\gamma_1^c), ..., T_\phi(\gamma_r^c))$, where T_ϕ denotes the monodromy action associated with $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$. As a result, the field of moduli of $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$ is contained in $\mathbb{R}$ if and only if ϕ is isomorphic to ϕ^c that is, there exists $\sigma \in \mathrm{SN}_{\mathcal{S}_\mathrm{n}}(\mathbf{C}, \mathrm{G})$ such that $\sigma(T_\phi(\gamma_1), ..., T_\phi(\gamma_r))\sigma^{-1} = (T_\phi(\gamma_1^c), ..., T_\phi(\gamma_r^c))$. Conversely, suppose $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$ is a degree n connected mere cover with monodromy group G, branch point divisor $\mathbf{t}$ and branch cycle description $BCD_{\underline{\gamma}}(\phi) = (g_1, ..., g_r) \in \overline{\mathrm{sni}}^{ab,mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$. Then any $\sigma \in U^{mod}(\mathbf{C})$ such that

$$\begin{cases} \sigma g_i \sigma^{-1} = (g_1 \cdots g_{i-1})g_i^{-1}(g_1 \cdots g_{i-1})^{-1},\ i = 1, ..., r_1 \\ \sigma g_{r_1+i}\sigma^{-1} = g_{r+1-i}^{-1},\ i = 1, ..., 2r_2 \end{cases}$$

corresponds to one and only one isomorphism $\delta_\sigma : \phi \tilde{\to} \phi^c$. Writing $\phi^{-1}(t_0) = \{x_1, ..., x_n\}$ we get ${\phi^c}^{-1}(t_0) = \{x_1^c, ..., x_n^c\}$ and $\delta_\sigma(x_i) = x_{\sigma(i)}^c$, $i = 1, ..., r$. Now, since $\mathrm{Gal}(\mathbb{C}|\mathbb{R}) =< 1, \mathrm{c} >$, Weil cocycle conditions only reduce to $\delta_c^c \circ \delta_c = 1$. But, here, $\delta_c^c \circ \delta_c(x_i) = \delta_c^c(x_{\sigma(i)^c}) = (\delta_c(x_{\sigma(i)}))^c = (x_{\sigma^2(i)}^c)^c = x_{\sigma^2(i)}$. So $\phi : X \to \mathbb{P}^1_{\mathbb{C}}$ is defined over $\mathbb{R}$ if and only if σ can be chosen in $U(\mathbf{C})$. □

3.7.1.3 Statements

In the following, we will always assume $\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; r_1, r_2) \neq \emptyset$

1. *Configuration (R).* For all $\underline{\chi} \in \mathrm{Irr(G)^r}$ we set :

$$\mathbf{J}_{\underline{\chi}}^{(mod)} = \sum_{\sigma \in U^{(mod)}(\mathbf{C})/\mathrm{Cen}_{\mathrm{SN(G,C)}}(\mathrm{G})} \left(\sum_{\substack{\underline{\alpha} \in G^{r-1} \\ \sigma\alpha_i\sigma^{-1} = \alpha_i^{-1},\ i=1,...,r-1}} \chi_1(\alpha_1^{-1}) \prod_{i=2}^{r-1} \chi_i(\alpha_i^{-1}\alpha_{i+1})\chi_r(\alpha_{r-1}) \right)$$

and

$$\mathbf{n}^{ab,(mod),\mathbb{R}}(\mathbf{C}; r, 0) = \frac{1}{Z_1 \cdots Z_r} \sum_{\underline{\chi} \in \mathrm{Irr(G)^r}} \chi_1(C_1) \cdots \chi_r(C_r)\mathbf{J}_{\underline{\chi}}^{(mod)}$$

Theorem 3.24 (Real branch points) *We have*

$$|\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; r, 0)| \leq \mathbf{n}^{ab,(mod),\mathbb{R}}(\mathbf{C}; r, 0)$$

with equality if $\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; r, 0) = Sni^{ab,(mod),\mathbb{R}}(\mathbf{C}; r, 0)$

2. *Configuration (C).* For all $\chi \in \mathrm{Irr(G)}$ we set :

$$\mathbf{B}_{\chi}^{(mod)} = \sum_{\sigma \in U^{(mod)}(\mathbf{C})/\mathrm{Cen}_{\mathrm{SN(G,C)}}(\mathrm{G})} \left(\sum_{\substack{\alpha \in G \\ \sigma\alpha\sigma^{-1} = \alpha}} \chi(\alpha) \right)$$

and

$$\mathbf{n}^{ab,(mod),\mathbb{R}}(\mathbf{C}; 0, s) = \frac{|G|^{s-1}}{Z_1 \cdots Z_s} \sum_{\chi \in \mathrm{Irr(G)}} \frac{\chi(C_1) \cdots \chi(C_r}{\chi(1)^{s-1}} \mathbf{B}_{\chi}^{(mod)}$$

Theorem 3.25 (Complex conjugate branch points) *We have*

$$|\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; 0, s)| \leq \mathbf{n}^{ab,(mod),\mathbb{R}}(\mathbf{C}; 0, s)$$

with equality if $\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; 0, s) = Sni^{ab,(mod),\mathbb{R}}(\mathbf{C}; 0, s)$.

3.7.2 Proofs

3.7.2.1 Real branch points

Once again fix $g_1, ..., g_r \in G$ with $g_i \in C_i$, $i = 1, ..., r$ and consider the set $E_{\mathbf{g}}^{(mod)}$ of those r-tuples $\underline{\gamma} = (\gamma_1, ..., \gamma_r) \in G^r$ such that $\sigma(g_1^{\gamma_1} \cdots g_i^{\gamma_i})\sigma^{-1} = (g_1^{\gamma_1} \cdots g_i^{\gamma_i})^{-1}$, $i = 1, ..., r-1$ for some $\sigma \in U^{(mod)}(\mathbf{C})$ and $g_1^{\gamma_1} \cdots g_r^{\gamma_r} = 1$. This is the same as the set of those $\underline{\gamma} = (\gamma_1, ..., \gamma_r) \in G^r$ such that

$$(*) \begin{cases} g_1^{\gamma_1} = \alpha_1^{-1} \\ g_i^{\gamma_i} = \alpha_i^{-1}\alpha_{i+1},\ i = 2, ..., r-1 \\ g_r = \alpha_{r-1}^{-1} \end{cases}$$

for some $\sigma \in U^{(mod)}(\mathbf{C})$, $\underline{\alpha} = (\alpha_1, ..., \alpha_{r-1}) \in G^{r-1}$ with $\sigma\alpha_i\sigma^{-1} = \alpha_i^{-1}$, $i = 1, ..., r-1$. The correspondence $\underline{\gamma} \to (g_1^{\gamma_1}, ..., g_r^{\gamma_r})$ provides a surjective map $E_{\mathbf{g}}^{(mod)} \to \Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; r, 0)$ and two distinct r-tuples $\underline{\gamma}, \underline{\gamma}' \in G^r$ have the same image if and only if $\gamma_i^{-1}\gamma_i' \in \mathrm{Cen_G(g_i)}$, $i = 1, ..., r$. So

$$|\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; r, 0)| = \frac{|E_{\mathbf{g}}^{(mod)}|}{Z_1 \cdots Z_r}$$

Then, for each $\underline{\gamma} \in G^r$ we check for every $\sigma \in U^{(mod)}(\mathbf{C})$ whether there exists $\underline{\alpha} = (\alpha_1, ..., \alpha_{r-1}) \in G^{r-1}$ with $\sigma\alpha_i\sigma^{-1} = \alpha_i^{-1}$, $i = 1, ..., r-1$ and verifying (*). In this case, $\underline{\alpha}$ is necessarily unique. Or, equivalently, we check whether

$$\sum_{\substack{\underline{\alpha} \in G^{r-1} \\ \sigma\alpha_i\sigma^{-1} = \alpha_i^{-1}, i = 1, ..., r-1}} \epsilon(\alpha_1^{-1} g_1^{\gamma_1}) \prod_{i=2}^{r-1} \epsilon(\alpha_i^{-1} g_i^{\gamma_i} \alpha_{i+1}) \epsilon(g_r^{\gamma_r} \alpha_{r-1}) = 1$$

Futhermore, given $\underline{\gamma} \in G^r$, distinct permutations $\sigma, \sigma' \in U^{(mod)}(\mathbf{C})$ can satisfy $\sigma g_i \sigma^{-1} = (g_1 \cdots g_{i-1}) g_i^{-1} (g_1 \cdots g_{i-1})^{-1} = \sigma' g_i \sigma'^{-1}$, $i = 0, ..., r-1$; this is equivalent to $\sigma^{-1}\sigma' \in \mathrm{Cen_{SN(C,G)}}(\mathrm{g_1^{\gamma_1}}, ..., \mathrm{g_r^{\gamma_r}})$, which, in turn, is implied by $\sigma^{-1}\sigma' \in \mathrm{Cen_{SN(C,G)}(G)}$. As a result, writing $U^{(mod)}/\mathrm{C}$ for $U^{(mod)}(\mathbf{C})/\mathrm{Cen_{SN(G,C)}(G)}$, we obtain

$$\begin{aligned} |E_{\mathbf{g}}^{(mod)}| &\leq \sum_{\substack{\underline{\gamma} \in G^r \\ \sigma \in U^{(mod)}/\mathrm{C}}} \sum_{\substack{\underline{\alpha} \in G^{r-1} \\ \sigma\alpha_i\sigma^{-1} = \alpha_i^{-1}}} \epsilon(\alpha_1^{-1} g_1^{\gamma_1}) \prod_{i=2}^{r-1} \epsilon(\alpha_i^{-1} g_i^{\gamma_i} \alpha_{i+1}) \epsilon(g_r^{\gamma_r} \alpha_{r-1}) \\ &\leq \sum_{\sigma \in U^{(mod)}/\mathrm{C}} \sum_{\substack{\underline{\alpha} \in G^{r-1} \\ \sigma\alpha_i\sigma^{-1} = \alpha_i^{-1}}} \sum_{\gamma \in G} \epsilon(\alpha_1^{-1} g_1^{\gamma}) \prod_{i=2}^{r-1} \sum_{\gamma \in G} \epsilon(\alpha_i^{-1} g_i^{\gamma} \alpha_{i+1}) \sum_{\gamma \in G} \epsilon(g_r^{\gamma} \alpha_{r-1}) \end{aligned}$$

But, applying lemma 4.10, we get

$$\begin{cases} \sum_{\gamma \in G} \epsilon(\alpha_1^{-1} g_1^{\gamma}) = \sum_{\chi \in \mathrm{Irr(G)}} \chi(g_1)\chi(\alpha_1^{-1}) \\ \sum_{\gamma \in G} \epsilon(\alpha_i^{-1} g_i^{\gamma} \alpha_{i+1}) = \sum_{\chi \in \mathrm{Irr(G)}} \chi(g_i)\chi(\alpha_i^{-1}\alpha_{i+1}),\ i = 2, ..., r-1 \\ \sum_{\gamma \in G} \epsilon(g_r^{\gamma} \alpha_{r-1}) = \sum_{\chi \in \mathrm{Irr(G)}} \chi(g_r)\chi(\alpha_{r-1}) \end{cases}$$

So

$$\begin{aligned} |E_{\mathbf{g}}^{(mod)}| &\leq \sum_{\sigma \in U^{(mod)}/\mathrm{C}} \sum_{\substack{\underline{\alpha} \in G^{r-1} \\ \sigma\alpha_i\sigma^{-1} = \alpha_i^{-1}}} \sum_{\chi \in \mathrm{Irr(G)}} \chi(g_1)\chi(\alpha_1^{-1}) \prod_{i=2}^{r-1} \sum_{\chi \in \mathrm{Irr(G)}} \chi(g_i)\chi(\alpha_i^{-1}\alpha_{i+1}) \sum_{\chi \in \mathrm{Irr(G)}} \chi(g_r)\chi(\alpha_{r-1}) \\ &\leq \sum_{\underline{\chi} \in \mathrm{Irr(G)^r}} \prod_{i=1}^{r} \chi_i(g_i) \mathbf{I}_{\underline{\chi}}^{(mod)} \end{aligned}$$

3.7.2.2 Complex conjugate branch points

We still follow the same method, introducing the set $E_{\mathbf{g}}^{(mod)}$ of those $\underline{\gamma} = (\gamma_1, ..., \gamma_{2s}) \in G^{2s}$ such that $\sigma g_i^{\gamma_i} \sigma^{-1} = g_{2s+1-i}^{-1\,\gamma_{2s+1-i}}$, $i = 1, ..., s$ and $g_1^{\gamma_1} \cdots g_s^{\gamma_s} \sigma (g_1^{\gamma_1} \cdots g_s^{\gamma_s})^{-1} \sigma^{-1} = 1$ for some $\sigma \in U^{(mod)}(\mathbf{C})$. The correspondence $\underline{\gamma} \to (g_1^{\gamma_1}, ..., g_{2s}^{\gamma_{2s}}$ provides a surjective map $E_{\mathbf{g}}^{(mod)} \to \Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; 0, s)$ and two distinct r-tuples $\underline{\gamma}, \underline{\gamma}' \in G^{2s}$ have the same image if and only if $\gamma_i^{-1}\gamma_i' \in \mathrm{Cen_G(g_i)}$, $i = 1, ..., 2s$. So

$$|\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C}; 0, s)| = \frac{|E_{\mathbf{g}}^{(mod)}|}{Z_1 \cdots Z_{2s}}$$

Then, for each $\underline{\gamma} \in G^{2s}$ we check for every $\sigma \in U^{(mod)}(\mathbf{C})$ whether $\sigma g_i^{\gamma_i} \sigma^{-1} = g_{2s+1-i}^{-1\,\gamma_{2s+1-i}}$, $i = 1, ..., s$ and $g_1^{\gamma_1} \cdots g_s^{\gamma_s} \sigma (g_1^{\gamma_1} \cdots g_s^{\gamma_s})^{-1} \sigma^{-1} = 1$ that is, whether

$$\prod_{i=1}^{s} \epsilon(\sigma g_i^{\gamma_i} \sigma^{-1} g_{2s+1-i}^{\gamma_{2s+1-i}}) \epsilon([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, \sigma]) = 1$$

Futhermore, given $\underline{\gamma} \in G^{2s}$, distinct permutations $\sigma, \sigma' \in U^{(mod)}(\mathbf{C})$ can satisfy $\sigma g_i^{\gamma_i} \sigma^{-1} = g_{2s+1-i}^{-1\,\gamma_{2s+1-i}} = \sigma' g_i^{\gamma_i} \sigma'^{-1}$; this is equivalent to $\sigma^{-1}\sigma' \in \mathrm{Cen}_{\mathrm{SN}(\mathbf{C},\mathrm{G})}(\mathrm{g}_1^{\gamma_1}, ..., \mathrm{g}_{\mathrm{r}}^{\gamma_{\mathrm{r}}})$, which, in turn, is implied by $\sigma^{-1}\sigma' \in \mathrm{Cen}_{\mathrm{SN}(\mathbf{C},\mathrm{G})}(\mathrm{G})$. So, with $U^{(mod)}/\mathrm{C}$ for $U^{(mod)}(\mathbf{C})/\mathrm{Cen}_{\mathrm{SN}(\mathrm{G},\mathbf{C})}(\mathrm{G})$, we get

$$\begin{aligned} |E_{\mathbf{g}}^{(mod)}| &\leq \sum_{\substack{\underline{\gamma} \in G^{2s} \\ \sigma \in U^{(mod)}/\mathrm{C}}} \prod_{i=1}^{s} \epsilon(\sigma g_i^{\gamma_i} \sigma^{-1} g_{2s+1-i}^{\gamma_{2s+1-i}}) \epsilon([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, \sigma]) \\ &\leq \sum_{\substack{(\gamma_1,...,\gamma_s) \in G^s \\ \sigma \in U^{(mod)}/\mathrm{C}}} \epsilon([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, \sigma]) \prod_{i=1}^{s} \sum_{\gamma \in G} \epsilon(\sigma g_i^{\gamma_i} \sigma^{-1} g_{2s+1-i}^{\gamma}) \end{aligned}$$

Lemma 4.10 gives for $i = 1, ..., s$

$$\begin{aligned} \sum_{\gamma \in G} \epsilon(\sigma g_i^{\gamma_i} \sigma^{-1} g_{2s+1-i}^{\gamma}) &= \sum_{\chi \in \mathrm{Irr(G)}} \chi(\sigma g_i^{\gamma_i} \sigma^{-1}) \chi(g_{2s+1-i}) \\ &= \sum_{\chi \in \mathrm{Irr(G)}} \chi(\sigma g_i \sigma^{-1}) \chi(g_{2s+1-i}) \end{aligned}$$

Consequently,

$$|E_{\mathbf{g}}^{(mod)}| \leq \sum_{\sigma \in U^{(mod)}/\mathrm{C}} \left(\prod_{i=1}^{s} \sum_{\chi \in \mathrm{Irr(G)}} \chi(\sigma g_i \sigma^{-1}) \chi(g_{2s+1-i}) \right) \sum_{(\gamma_1,...,\gamma_s) \in G^s} \epsilon([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, \sigma])$$

And, using one more time lemma 4.10

$$\begin{aligned} \sum_{(\gamma_1,...,\gamma_s) \in G^s} \epsilon([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, \sigma]) &= \sum_{(\gamma_1,...,\gamma_s) \in G^s} \sum_{\substack{\alpha \in G \\ \sigma\alpha\sigma^{-1} = \alpha}} \epsilon(g_1^{\gamma_1} \cdots g_s^{\gamma_s} \alpha) \\ &= \sum_{\substack{\alpha \in G \\ \sigma\alpha\sigma^{-1} = \alpha}} \sum_{(\gamma_1,...,\gamma_s) \in G^s} \epsilon(g_1^{\gamma_1} \cdots g_s^{\gamma_s} \alpha) \\ &= \sum_{\substack{\alpha \in G \\ \sigma\alpha\sigma^{-1} = \alpha}} \sum_{\chi \in \mathrm{Irr(G)}} \frac{|G|^{s-1}}{\chi(1)^{s-1}} \prod_{i=1}^{s} \chi(g_i) \chi(\alpha) \end{aligned}$$

So, finally,

$$|E_{\mathbf{g}}^{(mod)}| \leq \sum_{\sigma \in U^{(mod)}/\mathrm{C}} \sum_{\substack{\alpha \in G \\ \sigma\alpha\sigma^{-1}=\alpha}} \sum_{\chi \in \mathrm{Irr(G)}} \frac{|G|^{s-1}}{\chi(1)^{s-1}} \prod_{i=1}^{s} \chi(g_i)\chi(\alpha) \left(\prod_{i=1}^{s} \sum_{\chi \in \mathrm{Irr(G)}} \chi(\sigma g_i \sigma^{-1})\chi(g_{2s+1-i}) \right)$$

Now, recalling that $\Sigma^{ab,(mod),\mathbb{R}}(\mathbf{C};0,s) \neq \emptyset$ we have $\sigma C_i \sigma^{-1} = C_{2s+1-i}^{-1}$ for $i = 1, ..., s$, $\sigma \in U^{(mod)}(\mathbf{C})$ so $\chi(\sigma g_i \sigma^{-1}) = \overline{\chi(g_{2s+1-i})}$ for $i = 1, ..., s$, $\chi \in \mathrm{Irr(G)}$ and $\sum_{\chi \in \mathrm{Irr(G)}} \chi(\sigma g_i \sigma^{-1})\chi(g_{2s+1-i}) = \sum_{\chi \in \mathrm{Irr(G)}} \chi(g_{2s+1-i})|^2 = Z_{2s+1-i}$, which leads to the announced result.

3.8 A lower bound for the number of G-covers defined over the p-adics

A crucial point in the proof of theorem 3.1, [DF94] is the fact complex conjugation c is continuous for the usual complex topology. There is (probably) no p-adic analog of theorem 3.1 (*cf.* [DF94], §3.6) ; however, patching methods can be used to give a lower bound for the number of G-covers with prescribed invriants defined over a henselian field (k, v), provided the inertia canonical invariant and the branch point divisor satisfy some technical proprties. A good tool for this is Pop's half Riemann's existence theorem with Galois action [P94].

3.8.1 Half Riemann's existence theorem with Galois action

Let (k, v) be a henselian valued field ; we denote by k^s its separable closure, by $k(v)$ its residue field and by p the characteristic of $k(v)$.

Given a finite closed subset $S \subset \mathbb{P}_k^1$

(1) We say that S is pairwise v-adjusted if $S \times_k k^s = S_1 \coprod S_2$ with $|S_1| = |S_2| = r$ and $S_1 = \{x_1, ..., x_r\}$, $S_2 = \{y_1, ..., y_r\}$ such that $v(x_i - y_i) > v(x_i - x_j)$, $1 \leq i \neq j \leq r$, $\Gamma_k \cdot S_i = S_i$, $i = 1, 2$ (one then necessarily has $\sigma(x_i) = x_{i_\sigma}$ iff $\sigma(y_i) = y_{i_\sigma}$, $\sigma \in \Gamma_k$, $i = 1, ..., r$).

(2) With the notations of (1), let us define s_i, $i = 1, ..., r$ as follows :

- If we are in the equal characteristic case, then s_i is the Steinitz number defining $\hat{\mathbb{Z}}$, $i = 1, ..., r$.
- Else, s_i is the Steinitz number defining $\mathbb{Z}/p^{e_i}\mathbb{Z} \times \hat{\mathbb{Z}}/\mathbb{Z}_p$, where $e_i = \max\{0, e_i'\}$ and e_i' is the maximal integer $e_i \in \mathbb{Z}$ satisfying $v(x_i - y_i) - \frac{e_i'+1}{p-1} v(p) > v(x_i - x_j)$, $1 \leq i \neq j \leq r$, $i = 1, ..., r$.

(3) With the notations of (1), (2), let $\overline{\Pi}_S$ be the profinite group defined by the generators and relations

$$\overline{\Pi}_S = < g_{x_i}, g_{y_i},\ i = 1, ..., r \mid g_{x_i} g_{y_i} = 1,\ g_{x_i}^{s_i} = 1,\ i = 1, ..., r >$$

$\overline{\Pi}_S$ can be endowed with the right Γ_k-action $g_{x_i}^{\sigma} = g_{\sigma^1(x_i)}^{\chi(\sigma)}$, where $\chi : \Gamma_k \to \mathbb{Z}^\times$ denotes as usual the cyclotomic character of Γ_k.

We can now state :

Theorem 3.26 (Half Riemann's existence theorem with Galois action) *Let $S \subset \mathbb{P}_k^1$ be a pairwise v-adjusted finite closed subset and write $U = \mathbb{P}_k^1 \setminus S$, $U^s = U \times_k k^s$. Then the canonical short exact sequence of profinite groups*

$$1 \to \pi_1^{\mathrm{alg}}(U^s) \to \pi_1^{\mathrm{alg}}(U) \to \Gamma_k \to 1$$

has, in a canonical way, the following quotient

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi_1^{\mathrm{alg}}(U^s) & \longrightarrow & \pi_1^{\mathrm{alg}}(U) & \longrightarrow & \Gamma_k & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \rho_S^s} & & \downarrow{\scriptstyle \rho_S} & & \downarrow{\scriptstyle \simeq} & & \\ 1 & \longrightarrow & \overline{\Pi}_S & \longrightarrow & \overline{\Pi}_S \rtimes \Gamma_k & \longrightarrow & \Gamma_k & \longrightarrow & 1 \end{array}$$

Furthermore, g_{x_i} (resp. g_{y_i}) is an inertia element associated with x_i (resp. y_i), $i = 1, ..., r$.

3.8.2 A construction

From now on, we assume that k is of characteristic 0. Let G be a finite group and $c_1, ..., c_r$ a generating system of G. For each $1 \leq i \leq r$, set $n_i = | < c_i > | = p^{u_i} m_i$ with $p \not| m_i$. Let $x_{i,1} \in k(\zeta_{n_i})$ such that $k(x_{i,1}) = k(\zeta_{n_i})$ and, with $\Gamma_k.x_{i,1} = \{x_{i,1}, ..., x_{i,r_i}\}$ (where $r_i = [k(\zeta_{n_i}) : k]$), choose a system of representatives $\wr brace\sigma_{i,1}, ..., \sigma_{i,r_i}\}$ of $\Gamma_k/\Gamma_{k(\zeta_{n_i})}$ verifying $\sigma_{i,j}(x_{i,1}) = x_{i,j}$, $j = 1, ..., r_i$. By Hensel's lemma, the minimal polynomial of $a_{i,1}$ over k can be written $\prod_{1 \leq j \leq r_i}(X - u_{i,j}(T))$ where $u_{i,j} \in k[[T]]$ has a positive radius $\epsilon > 0$ and $u_{i,j}(0) = x_{i,j}$, $j = 1, ..., r_i$. So, one can find $t_i \in k$ such that $0 < |t_i| < \epsilon$ and $(y_{i,j} = u_{i,j}(t_i))_{1 \leq j \leq r_i}$ satisfy (1), (2) of 3.8.1 with $(x_{i,j})_{1 \leq j \leq r_i}$, $u_i \leq e_i$, $i = 1, ..., r$.

Thus, up to translating, we can assume that $S = \{x_{i,1}, ..., x_{i,r_i}\}_{1 \leq i \leq r} \coprod \{y_{i,1}, ..., y_{i,r_i}\}_{1 \leq i \leq r}$ is pairwise v-adjusted and define $\phi^0_{\underline{1}} : \overline{\Pi}_S \rtimes \Gamma_k \to G$ by $\phi^0_{\underline{1}}(g_{x_{i,j}}) = c_i^{\chi(\sigma_{i,j}^{-1})}$, $1 \leq j \leq r_i$, $i = 1, ..., r$ and $\phi^0_{\underline{1}}(\sigma) = 1$, $\sigma \in \Gamma_k$ (in the following, write $u_{i,j} = \chi(\sigma_{i,j}^{-1})$, $1 \leq j \leq r_i$, $i = 1, ..., r$). One easily checks that $\phi^0_{\underline{1}}$ is a well-defined group epimorphism and, setting $\phi_{\underline{1}} = \phi^0_{\underline{1}} \circ \rho_S : \pi_1^{\mathrm{alg}}(U) \twoheadrightarrow G$, one obtains a group epimorphism corresponding to a G-cover defined over k with invariants G, $\mathbf{C}$, S, where $\mathbf{C} = ((C_{i,j}, C_{i,j}^{-1})_{1 \leq j \leq r_i})_{1 \leq i \leq r}$ and $C_{i,j} = (C_{c_i}^G)^{u_{i,j}}$, $1 \leq j \leq r_i$, $i = 1, ..., rr$. Observe that the construction above can also be performed replacing c_i by $c_i^{\alpha_i}$ for any $\underline{\alpha} = (\alpha_1, ..., \alpha_r) \in G^r$ such that (*) $c_1^{\alpha_1}, ..., c_r^{\alpha_r}$ still generate G. We denote by $\phi^0_{\underline{\alpha}}$, $\phi_{\underline{\alpha}}$ the corresponding group epimorphisms. Then, for all $\underline{\alpha}, \underline{\beta} \in G^r$ verifying (*), $\phi_{\underline{\alpha}}$ is equivalent to $\phi_{\underline{\beta}}$ iff $\phi_{\underline{\beta}} =^g \phi_{\underline{\alpha}}$ for some $g \in G$, which in turn is equivalent to ${}^{\alpha_i}c_i =^{g\beta_i} c_i$ for some $g \in G$. (Indeed, let $\tilde{M}_S/k^s(T)$ be the Galois extension corresponding to $\overline{\Pi}_S$, $\tilde{P}_{x_{i,j}}$ the place of $\tilde{M}_S/k^s$ dividing $T - x_{i,j}$ and with inertia group $< g_{x_{i,j}} >$, $P_{x_{i,j}}$ a place of $\overline{M}_S/k^s$ dividing $\tilde{P}_{x_{i,j}}$ and $\gamma_{x_{i,j}}$ one of the generators of its inertia group such that $\rho_S^s(\gamma_{x_{i,j}}) = g_{x_{i,j}}$; likewise, define $\gamma_{y_{i,j}}$, $1 \leq j \leq r_i$, $i = 1, ..., r$ and conclude using $\pi_1^{\mathrm{alg}}(U^s) =< \gamma_{x_{i,j}}, \gamma_{y_{i,j}} \mid 1 \leq j \leq r_i,\ i = 1, ..., r >$. So, there is a bijection between the isomorphism classes of G-covers of the form $\phi_{\underline{\alpha}}$, $\underline{\alpha} \in G^r$ verifying (*) and the quotient set $\{(g_{i,1}, ..., g_{i,r_i})_{1 \leq i \leq r} \in G \mid g_{i,j} \in C_{i,j},\ 1 \leq j \leq r_i,\ i = 1, ..., r \text{ and } G =< \{g_{i,1}, ..., g_{i,r_i}\}_{1 \leq i \leq r} >\}/\mathrm{Inn}(G)$. In particular, if $\mathrm{sni}_S^k(\mathbf{C})$ denotes the set of all G-covers defined over k with invariants G, $\mathbf{C}$, S and $\overline{\mathrm{sni}}_S^k(\mathbf{C})$ the set of all isomorphism classes of G-covers defined over k with invariants G, $\mathbf{C}$, S (or, equivalently, the quotient set of $\mathrm{sni}_S^k(\mathbf{C})$ modulo componentwise inner conjugation), we obtain

Proposition 3.27

$$|\overline{\mathrm{sni}}_S^k(\mathbf{C})| \geq |\overline{\mathrm{hm}}(\mathbf{C})|,$$

where $\mathrm{hm}(\mathbf{C})$ *denotes the set of all* $\mathbf{g} \in \mathrm{sni}(\mathbf{C})$ *of the form* $\mathbf{g} = ((g_{i,j}, g_{i,j}^{-1})_{1 \leq j \leq r_i})_{1 \leq i \leq r}$ *and* $\overline{\mathrm{hm}}(\mathbf{C})$*, its quotient set modulo componentwise inner conjugation. In particular, if* $(C_{1,1}, ..., C_{r,1})$ *is g-complete we have*

$$|\overline{\mathrm{sni}}_S^k(\mathbf{C})| \geq \frac{|C_{1,1}|^{r_1} \cdots |C_{r,1}|^{r_r}}{[G : Z(G)]} =: \mathbf{m}_S^k(\mathbf{C})$$

and so

$$|\overline{\mathrm{sni}}(\mathbf{C})| = \mathbf{m}_S^k(\mathbf{C}) \frac{|C_{1,1}|^{r_1} \cdots |C_{r,1}|^{r_r}}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \left(\frac{|\chi(C_{1,1})|^{r_1} \cdots |\chi(C_{r,1})|^{r_r}}{\chi(1)^{s-1}} \right)^2$$

3.9 tables of characters

- $\mathbb{H}_8$:

C	1	-1	+/-i	+/-j	+/- k
$\lvert C_G(g)\rvert$	8	8	4	4	4
χ_1	1	1	1	1	1
χ_2	1	1	1	-1	-1
χ_3	1	1	-1	1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

- D_{2n}, $n = 2m+1$ odd :

C	1	r^k	sr^k
$\lvert C_G(g)\rvert$	2n	n	2
χ_1	1	1	1
χ_2	1	1	-1
$\chi_{2+h}\,;\, 1 \leq h \leq \frac{n-1}{2}$	2	$2cos(\frac{2\pi hk}{n})$	0

- D_{2n}, $n = 2m$ even :

C	1	$r^{\frac{n}{2}}$	r^k	sr^k
$\lvert C_G(g)\rvert$	2n	2n	n	4
χ_1	1	1	1	1
χ_2	1	$(-1)^{\frac{n}{2}}$	$(-1)^k$	$(-1)^{k+1}$
χ_3	1	1	1	-1
χ_4	1	$(-1)^{\frac{n}{2}}$	$(-1)^k$	$(-1)^k$
$\chi_{4+h}\,;\, 1 \leq h \leq \frac{n}{2}-1$	2	$(-1)^h 2$	$2cos(\frac{2\pi hk}{n})$	0

- $U_{m,n}$, $n \geq 1$, $m \geq 3$ such that $2 \not| m$:

C	1	$A_{i,0},\ 1 \leq j \leq \frac{m-1}{2}$	$A_{i,j},\ \substack{1\leq i\leq n-1 \\ 0\leq j\leq \frac{m-1}{2}}$	$B_i,\ 0 \leq i \leq n-1$
$\lvert C_G(g)\rvert$	2mn	2mn	mn	2n
$\psi_k\,;\, 0 \leq k \leq 2n-1$	1	ϵ_k^{2i}	ϵ_k^{2i}	ϵ_k^{2i+1}
$\chi_{k,l}\,;\, \substack{0\leq k\leq n-1 \\ 1\leq l\leq \frac{m-1}{2}}$	2	$2\epsilon_k^{2i}$	$\epsilon_k^{2i}(\omega_l^j + \omega_l^{-j})$	0

where $\epsilon_k = e^{\frac{k2\pi i}{2n}}$, $k = 0, ..., n-1$ and $\omega_l = e^{\frac{l2\pi i}{m}}$, $l = 1, ..., \frac{m-1}{2}$.

- $F_{p,q}$ where p, q are odd primes such as $p > q$ and $p|q-1$:

C	1	$a^{v_i}\,;\, 1 \leq i \leq s$	$b^n\,;\, 1 \leq n \leq q-1$
$\lvert C_G(g)\rvert$	pq	p	q
$\chi_{1,k}\,;\, 0 \leq k \leq q-1$	1	1	$e^{\frac{2\pi ikn}{q}}$
$\chi_{q,l}\,;\, 1 \leq l \leq s$	q	$\sum_{0<j<q-1} e^{\frac{2\pi v_l v_i u^j}{q}}$	0

- M_{11} :

C	1A	2A	3A	4A	5A	6A	8A	B^*	11A	B^{**}
$\lvert C_G(g)\rvert$	7920	48	18	8	5	6	8	8	11	11
χ_1	1	1	1	1	1	1	1	1	1	1
χ_2	10	2	1	2	0	-1	0	0	-1	-1
χ_3	10	2	1	2	0	-1	0	0	-1	-1
χ_4	10	-2	1	0	0	1	i2	-i2	-1	-1
χ_5	11	3	2	-1	1	0	-1	-1	0	0
χ_6	16	0	-2	0	1	0	0	0	b11	**
χ_7	16	0	-2	0	1	0	0	0	**	b11
χ_8	44	4	-1	0	-1	1	0	0	0	0
χ_9	45	-3	0	1	0	0	-1	-1	1	1
χ_{10}	55	-1	1	-1	0	-1	1	1	0	0

Chapitre 4

Harbater-Mumford subvarieties of moduli spaces of covers

*Il s'agit essentiellement de l'article [C04c] auquel nous avons rajouté une dernière partie (§**??**) présentant quelques questions ouvertes liées aux résultats de [C04c]. Nous y avons aussi developpé le §4.4.2 en y ajoutant une sous-section (4.4.2.3) et détaillé l'exemple **??**.*

Introduction

The regular inverse Galois problem over some field k, (RIGP/k), essentially reduces to finding k-rational points on Hurwitz moduli spaces of covers [FV91]. In this context, two main methods can be distinguished : on the one hand, genus 0 methods [Ma89] which may provide $\mathbb{Q}$ or $\mathbb{Q}^{ab}$-rational points on usually low-dimensional Hurwitz spaces and, on the other hand, large field methods [DF94], [D92], [Des95][1], which combine irreducibility Conway and Parker type results [FV91], realization results over local fields [H03], [DF94] and the local-global principle for varieties [Mo89], [P96] to provide $\mathbb{Q}^{\Sigma 2}$-rational points. Our main theorem (theorem 4.4) conjoins these two aspects : it is, as Conway and Parker's theorem, a global structure result about high-dimensional Hurwitz spaces but, as genus 0 methods, it deals with low-dimensional closed subvarieties (of those high-dimensional Hurwitz spaces) obtained by specializing most of the branch points.

The starting point are special components of Hurwitz moduli spaces of covers introduced by M. Fried [F95a] - the Harbater-Mumford components (*cf.* §4.2.1). We consider the closed subvarieties - we call HM-subvarieties - of these HM-components obtained by specializing most of the branch points ; our main result is a general criterion to ensure they are geometrically irreducible. If for instance G is any group verifying the assumptions of theorem 1 below, our criterion produces infinitely many Hurwitz spaces carrying geometrically irreducible HM-curves, defined over the same field as the whole Hurwitz space, and lying in the sublocus corresponding to covers with all their branch points but one fixed. In general, "all their branch points but one" should be replaced by "all their branch points but $r(G)$" for some integer $r(G)$ depending only on the finite group G in question.

One motivation for this work was to gain more information about the branch point divisor of covers defined over large fields. Indeed, when applying the local-global principle to solve for instance (RIGP/$\mathbb{Q}^{tr}$), this information is entirely lost. Showing that any finite group G can be regularly realized over $\mathbb{Q}^{tr}$ with a $\mathbb{Q}$-rational branch point divisor would be a significant step towards the (RIGP/$\mathbb{Q}$) : as explained in [D95], the monodromy of such a cover and its conjugates obeys strong group-theoretical constraints. Also, showing all the groups G_n of a projective system $(G_{n+1} \twoheadrightarrow G_n)_{n\geq 0}$ can be regularly

[1] See also works of Pop et al who have developped a parallel approach based on common principles but not using Hurwitz spaces [P96], [H03], [V99].

[2] Given a global field k and a finite set Σ of places of k, we always denote by k^{Σ} the maximal algebraic extension of k (in a fixed separable closure of k) which is totally split at each place $P \in \Sigma$.

realized over a large field k with the same branch point divisor $\mathbf{t}$ is a missing step to investigate the (RIGP/k) for profinite groups; this is the underlying idea of works like [DDes04]. Our result enables us to handle the derived problem - we denote by (RIGP/$\mathbf{t}_2 \subset \mathbf{t}$) - where the subset $\mathbf{t}_2 \subset \mathbf{t}$ is fixed and its complement, $\mathbf{t}_1$ is allowed to vary (the cardinality $|\mathbf{t}_1|$ of $\mathbf{t}_1$ corresponding to the dimension of the HM-subvarieties we consider). We are particularly interested in the case when $\mathbf{t}_2$ is defined over $\mathbb{Q}$ and $|\mathbf{t}_1|$ is as small as possible. The first and most difficult step, which is to ensure the HM-subvarieties are geometrically irreducible, is given by our criterion. The second one consists in showing these HM-subvarieties can be built in such a way they carry real or p-adic points; this requires a careful use of recent results from [DE03] about the existence of p-adic points on HM-components. We can then apply the usual local-global machinery to obtain results like

Theorem 1 *Let G be a finite group containing two conjugacy classes A, B such that $G =< A >=< B >$ and $G =< a, b >$ for any $a \in A$, $b \in B$. Let $o(A)$ denote the order of the elements in A and write $k_A := \mathbb{Q}(\mathrm{e}^{\frac{2\pi i}{o(A)}})$. Then, for any finite set Σ of non archimedean places of k_A of residue characteristic not dividing $|G|$ there exists a $\mathbb{Q}$-rational divisor $\mathbf{t}_\Sigma$ and G-covers (f, α) defined over k_A^Σ with group G and branch point divisor $\mathbf{t}_f = \mathbf{t}_{f,1} + \mathbf{t_\Sigma}$ where $|\mathbf{t}_{f,1}| = 1$.*

As another application, we obtain new regular realizations of some prodihedral groups over $\mathbb{Q}^{tr}$ (*cf.* also [**?**]).

Moreover, our irreducibility criterion behaves well with Frattini extensions. This allows us to investigate the arithmetic of Fried's modular towers [F95a] (section 4.4.1.2) and tackle the related (RIGP/$\mathbf{t}_2 \subset \mathbf{t}$) for profinite groups like the universal p-Frattini cover ${}_p\tilde{G}$ of a finite p-perfect group G (for some prime p dividing $|G|$). For instance, with the notation and hypotheses of theorem 1 but assuming in addition that G is p-perfect and A, B are p'-conjugacy classes, one obtains this structure result

Theorem 2 *There exist modular towers $(\mathcal{H}_{n+1} \to \mathcal{H}_n)_{n\geq 0}$ associated with G such that for any finite set Σ of non archimedean places of k of residue characteristic not dividing $|G|$ there exists a $\mathbb{Q}$-rational divisor $\mathbf{t}_\Sigma$ and a projective system $(\mathcal{C}_{n+1,\Sigma} \to \mathcal{C}_{n,\Sigma})_{k\geq 0}$ of geometrically irreducible HM-curves defined over k verifying :*

(i) $\mathcal{C}_{n,\Sigma} \subset \mathcal{H}_n$ classifies G-covers (f_n, α_n) with group ${}_p^n\tilde{G}$ and branch point divisor $\mathbf{t}_{f_n} = \mathbf{t}_{f_n,1} + \mathbf{t_\Sigma}$ where $|\mathbf{t}_{f_n,1}| = 1$, $n \geq 0$.

(ii) $\varprojlim_{n\geq 0} \mathcal{C}_{n,\Sigma}(k_P)^{noob} \neq \emptyset$, $P \in \Sigma$.

(iii) $\mathcal{C}_{n,\Sigma}(k^\Sigma)^{noob} \neq \emptyset$, $n \geq 0$.

Here ${}_p^n\tilde{G}$ denotes the nth characteristic quotient of ${}_p\tilde{G}$ and the "noob" labelling (for no obstruction) means we consider the sets of k-rational points corresponding to G-covers defined over k and not only with field of moduli k.

The preceding statement shows a strong arithmetical property is kept along some modular towers. It is a positive result which emphasizes the difficulty of Fried's conjectures about the disappearence of rational points over a number field on a modular tower beyond a certain level [D04], [F95a].

The paper is organized as follows. In section 1 we recall necessary definitions and basic results, section 2 is devoted to the statements and examples, section 3 to the proofs. In section 4, we give applications of our results such as theorems 1, 2.

I wish to thank P. Dèbes for encouraging me to write this paper and the careful re-reading he made of it.

4.1 Preliminaries

This section is devoted to recalling the necessary definitions and some basic facts about Hurwitz spaces.

Given a morphism $V \to W$ of algebraic varieties and $W_0 \hookrightarrow W$ a subvariety, we will often denote the fiber product $V \times_W W_0$ by V_{W_0}. Also, given a finite group G and an integer $r \geq 1$ we will denote the set of all the r-tuples $\mathbf{C} = (C_1, ..., C_r)$ of non trivial conjugacy classes of G by $\mathcal{C}_r(G)$; we will sometimes write $l(\mathbf{C}) := r$ for the length of such a tuple $\mathbf{C} \in \mathcal{C}_r(G)$. And for any conjugacy class C, we will write $o(C)$ for the order of any element in C. Eventually, given a tuple $\mathbf{t}' = (t_1, ..., t_r)$ and two integers $1 \leq i < j \leq r$, we will write $\mathbf{t}'_{i,j} := (t_i, ..., t_j)$.

4.1.1 G-covers and Hurwitz spaces

Recall a G-cover with group G is a pair (f, α) where $f : X \to \mathbb{P}^1$ is a Galois cover with group G and $\alpha : \mathrm{Aut}(f) \to G$ is a group isomorphism. One can attach to each G-cover of $\mathbb{P}^1_{\mathbb{C}}$ the three following invariants : the monodromy group G, the branch point set $\mathbf{t} = \{t_1, ..., t_r\} \subset \mathbb{P}^1(\mathbb{C})$ and for each $t \in \mathbf{t}$ the *associated inertia canonical conjugacy class* C_t . To summarize this, we will sometimes say the considered G-cover has invariants G, $(C_t)_{t \in \mathbf{t}}$, $\mathbf{t}$. Adopting the topological point of view, let us recall what these invariants correspond to : given $\mathbf{t} = \{t_1, ..., t_r\}$, introduce a *topological bouquet* $\underline{\gamma}$ of $\mathbb{P}^1_{\mathbb{C}} \backslash \mathbf{t}$, that is an r-tuple of homotopy classes of loops $\gamma_1, ..., \gamma_r$ based at some point $t_0 \notin \mathbf{t}$ such that (1) $\gamma_1, ..., \gamma_r$ generate the topological fundamental group $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \backslash \mathbf{t}, t_0)$ with the single relation $\gamma_1 ... \gamma_r = 1$ and (2) γ_i is a loop revolving once, counterclockwise, about t_i, $i = 1, ..., r$. Now, considering a G-cover $f : X \to \mathbb{P}^1_{\mathbb{C}}$, the monodromy action defines a permutation representation $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \backslash \mathbf{t}, t_0) \to \mathrm{Per}(f^{-1}(t_0))$. The image group G of this representation is the monodromy group (or, equivalently the Galois group) of f and the conjugacy class C_{t_i} of the image of γ_i in G is the inertia canonical class corresponding to t_i, $i = 1, ..., r$.

For any integer $r \geq 3$ let $\mathcal{U}^r \subset (\mathbb{P}^1_{\mathbb{C}})^r$ be the subset of $(\mathbb{P}^1_{\mathbb{C}})^r$ consisting of all r-tuples $\mathbf{t}' = (t_1, ..., t_r) \in (\mathbb{P}^1_{\mathbb{C}})^r$ such that $t_i \neq t_j$ for $1 \leq i \neq j \leq r$, let $\mathcal{U}_r = \mathcal{U}^r / S_r$ be the quotient space of $\mathcal{U}^r$ by the natural action of the symmetric group S_r and $\sigma_r : \mathcal{U}_r \to \mathcal{U}^r / S_r$ the canonical projection. Given a finite group G let $\psi_{r,G} : \mathcal{H}_{r,G} \to \mathcal{U}_r$ be the coarse moduli space (fine assuming $Z(G) = \{1\}$) for the category of G-covers of $\mathbb{P}^1_{\mathbb{C}}$ with group G and r branch points, where $\psi_{r,G}$ is the application which to a given isomorphism class of G-covers associates its branch point set. For any r-tuple $\mathbf{C} = (C_1, ..., C_r) \in \mathcal{C}_r(G)$ let $\mathcal{H}_{r,G}(\mathbf{C})$ be the corresponding *Hurwitz space* [FV91], that is the union of irreducible components of $\mathcal{H}_{r,G}$ parametrizing the isomorphism classes of G-covers with invariants G, $\mathbf{C}$, $\mathbf{t}$. A point $\mathbf{h} = (h, (t_1, ..., t_r))$ of the fiber product$\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$ then corresponds to a G-cover given with an ordering of its branch points, which allows us to define a monodromy application :

$$\begin{array}{rccc} \mathrm{M} : & \mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r & \to & \{C_1, ..., C_r\}^r \\ & (h, (t_1, ..., t_r)) & \to & (C_{t_1}, ..., C_{t_r}) \end{array}$$

This application, being continuous, is constant on each connected component of $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$. So, $M^{-1}(\mathbf{C})$ is a union of connected components of $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$; we will denote this variety by $\mathcal{H}'_{r,G}(\mathbf{C})$. We have a cartesian square :

$$\begin{array}{ccc} \mathcal{H}'_{r,G}(\mathbf{C}) & \xrightarrow{\Sigma_r} & \mathcal{H}_{r,G}(\mathbf{C}) \\ \downarrow{\scriptstyle \psi'_{r,G}} & \square & \downarrow{\scriptstyle \psi_{r,G}} \\ \mathcal{U}^r & \xrightarrow{\sigma_r} & \mathcal{U}_r \end{array}$$

We will freely use the general theory of Hurwitz spaces (see for instance [FV91] and [V99]), and only recall here the description of the fibers of $\psi_{r,G}$ and $\psi'_{r,G}$ in terms of *Nielsen classes* $\mathrm{ni}(\mathbf{C})$ and *straight*

Nielsen classes $\mathrm{sni}(\mathbf{C})$ respectively, where :

$$\mathrm{ni}(\mathbf{C}) = \left\{ (g_1,...,g_r) \in G^r \;\middle|\; \begin{array}{l} (1)\ G =< g_1,...,g_r > \\ (2)\ g_1 \cdots g_r = 1 \\ (3)\ g_i \in C_{\sigma(i)},\ i = 1,...,r \text{ for some } \sigma \in S_r \end{array} \right\}$$

and $\mathrm{sni}(\mathbf{C})$ is the set defined as $\mathrm{ni}(\mathbf{C})$, but replacing (3) by

$$(3)'\ g_i \in C_i \text{ for } i = 1,...,r.$$

We use the notation $\overline{\mathrm{ni}}(\mathbf{C})$ and $\overline{\mathrm{sni}}(\mathbf{C})$ for the corresponding quotient sets modulo the componentwise action of the inner automorphism group, $\mathrm{Inn}(G)$.

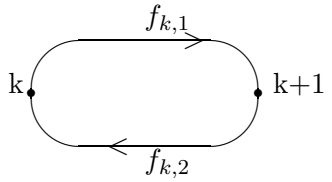
Given $\mathbf{t} \in \mathcal{U}_r$, it is classical that $(\psi_{r,G})^{-1}(\mathbf{t})$ is in bijection with $\overline{\mathrm{ni}}(\mathbf{C})$. Furthermore, if we choose an ordering of the branch points $\mathbf{t}' = (t_1,...,t_r)$ in $\mathbf{t}$, then $\overline{\mathrm{sni}}(\mathbf{C})$ is in bijection with $(\psi'_{r,G})^{-1}(\mathbf{t}')$. The correspondence is given by the monodromy action and depends on the choice of a topological bouquet $\underline{\gamma}$ for $\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t}$; we denote it by $BCD_{\underline{\gamma}}$ (for B(ranch) (C)ycle (D)escription).

For later use, we also recall that two finite cyclotomic field extensions of $\mathbb{Q}$ - which we denote by $\mathbb{Q}_{\mathbf{C}}$ and $\mathbb{Q}'_{\mathbf{C}}$ - are associated to $\mathbf{C}$. Precisely, $\mathbb{Q}_{\mathbf{C}} = \overline{\mathbb{Q}}^{\Delta_{\mathbf{C}}}$ and $\mathbb{Q}'_{\mathbf{C}} = \overline{\mathbb{Q}}^{\Delta'_{\mathbf{C}}}$ where $\Delta_{\mathbf{C}}$ and $\Delta'_{\mathbf{C}}$ are the closed subgroups of finite indice of $\mathrm{G}_{\mathbb{Q}}$ defined by $\Delta_{\mathbf{C}} = \{\sigma \in \mathrm{G}_{\mathbb{Q}} | \mathbf{C}^{\chi(\sigma)} = \mathbf{C} \text{ up to permutation}\}$ and $\Delta'_{\mathbf{C}} = \{\sigma \in \mathrm{G}_{\mathbb{Q}} | \mathbf{C}^{\chi(\sigma)} = \mathbf{C}\}$ (here, $\chi : \mathrm{G}_{\mathbb{Q}} \to \hat{\mathbb{Z}}$ is the cyclotomic character). Resulting from the branch cycle argument [V99] lemma 2.8, $\mathbb{Q}_{\mathbf{C}}$ is the field of definition of $\mathcal{H}_{r,G}(\mathbf{C})$ and $\mathbb{Q}'_{\mathbf{C}}$, the one of $\mathcal{H}'_{r,G}(\mathbf{C})$. When $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}$, we say that $\mathbf{C}$ is *a rational union of conjugacy classes* and, when $\mathbb{Q}'_{\mathbf{C}} = \mathbb{Q}$, that $\mathbf{C}$ is *a tuple of rational conjugacy classes*.

Finally, since Hurwitz spaces are only coarse moduli spaces in general, we will write $\mathcal{H}_{r,G}(\mathbf{C})(k)^{noob}$ for the set of all the k-rational points in the non obstruction locus that is, corresponding to G-covers defined over k.

4.1.2 The covers $\Psi_{r,G}$ and $\Psi'_{r,G}$

From now on, we will always assume $r \geq 4$. We first recall useful results about Hurwitz braid groups and then give a description of the covers $\Psi_{r,G}$ and $\Psi'_{r,G}$ in terms of group actions. Fix $\mathbf{t} = \{1,...,r\} \in \mathcal{U}_r(\mathbb{C})$ and $\mathbf{t}' = (1,...,r) \in \mathcal{U}^r(\mathbb{C})$ and for $k = 1,...,r-1$ define the simple arcs $f_{k,i} : [0,1] \to \mathbb{P}^1(\mathbb{C})$, $i = 1,2$ by



and write $q_k : \begin{array}{ccc} [0,1] & \to & \mathcal{U}^r(\mathbb{C}) \\ t & \to & (1,...,k-1,f_{k,1}(t),f_{k,2}(t),k+2,...,r) \end{array}$ for the usual topological braid.

Let H_r be the abstract group given by the presentation with generators $Q_1,...,Q_{r-1}$ and defining relations

(1)	$Q_iQ_{i+1}Q_i = Q_{i+1}Q_iQ_{i+1}$	for $i = 1,...,r-2$
(2)	$Q_iQ_j = Q_jQ_i$	for $i,j = 1,...,r-1$ with $\lvert j-i\rvert > 1$
(3)	$Q_1Q_2\cdots Q_{r-1}Q_{r-1}\cdots Q_2Q_1 = 1$	

and SH_r the kernel of the morphism $H_r \to \mathcal{S}_r,\ Q_i \to (i,i+1)$. Set

$$A_{i,j} := Q_{j-1}^{-1}\cdots Q_{i+1}^{-1}Q_i^{-2}Q_{i+1}\cdots Q_{j-1} = Q_i\cdots Q_{j-2}Q_{j-1}^{-2}Q_{j-2}^{-1}\cdots Q_i^{-1},\ 1 \leq i < j \leq r$$

(we will also often use the notation $a_{i,j} = A_{i,j}^{-1}$, $1 \leq i < j \leq r$) and denote by $\Pi_{k,r}$ the subgroup of SH_r generated by $\{A_{i,j}\}_{1\leq i\leq k, i<j\leq r}$, $k = 1,...,r-1$. The following result will play an important part in the proof of theorem 4.4. It is a direct corollary of lemma 1.8.2 [Bi74], which gives a presentation of SH_r with generators $A_{i,j}$, $1 \leq i < j \leq r$ and defining relations.

Theorem 4.1 *The groups $\Pi_{k,r}$ are normal in SH_r, $k = 1, ..., r-1$.*

The next theorem gives the link between the abstract groups H_r, SH_r and the topological fundamental groups $\pi_1^{\text{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})$, $\pi_1^{\text{top}}(\mathcal{U}^r(\mathbb{C}), \mathbf{t}')$, more precisely, it states that

Theorem 4.2 (Artin (1925), Fadell and Van Buskirk (1962)) *The group homomorphisms*
$$\begin{array}{cccccccc} u_r: & H_r & \to & \pi_1^{\text{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) & \text{and} & v_r: & SH_r & \to & \pi_1^{\text{top}}(\mathcal{U}^r(\mathbb{C}), \mathbf{t}') \\ & Q_i & \to & [(\sigma_r)_*(q_i)] & & & A_{i,j} & \to & [q_i \cdots q_{j-2} q_{j-1}^{-2} q_{j-2}^{-1} \cdots q_i^{-1}] \end{array}$$
are isomorphisms.

Let us use this result to show that $\Pi_{k,r} \simeq \pi_1^{\text{top}}(\mathcal{U}^r_{\mathbf{t}'_{k+1,r}}(\mathbb{C}), \mathbf{t}'_{1,k})$, $k = 1, ..., r-1$. For this, consider the homotopy sequence of the fibration with connected fibers
$$\begin{array}{rccc} p_{k+1,r}: & \mathcal{U}^r(\mathbb{C}) & \to & \mathcal{U}^{r-k}(\mathbb{C}) \\ & (t_1, ..., t_r) & \to & (t_{k+1}, ..., t_r) \end{array}$$
which gives rise to the short exact sequence of topological fundamental groups
$$1 \to \pi_1^{\text{top}}(\mathcal{U}^r_{\mathbf{t}'_{k+1,r}}, \mathbf{t}'_{1,k}) \to \pi_1^{\text{top}}(\mathcal{U}^r, \mathbf{t}') \overset{(p_{k+1,r})_*}{\to} \pi_1^{\text{top}}(\mathcal{U}^{r-k}, \mathbf{t}'_{k+1,r}) \to 1$$
It follows from the definition of the topological braids $(q_i)_{1 \le i \le r-1}$ that $v_r(\Pi_{k,r}) < \ker((p_{k+1,r})_*)$. The group homomorphism $\eta_{k,r} : SH_r \to SH_{r-k}$ defined by $\eta_{k,r}(A_{i,j}) = A_{i-k,j-k}$ if $k < i < j \le r$ and $\eta_{k,r}(A_{i,j}) = 1$ else is well defined and we get the commutative diagram with exact rows
$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Pi_{k,r} & \longrightarrow & SH_r & \xrightarrow{\eta_{k,r}} & SH_{r-k} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle v_r|_{\Pi_{k,r}}} & & \downarrow{\scriptstyle v_r} & & \downarrow{\scriptstyle v_{r-k}} & & \\ 1 & \longrightarrow & \pi_1^{\text{top}}(\mathcal{U}^r_{\mathbf{t}'_{k+1,r}}, \mathbf{t}'_{1,k}) & \longrightarrow & \pi_1^{\text{top}}(\mathcal{U}^r, \mathbf{t}') & \xrightarrow[(p_{k+1,r})_*]{} & \pi_1^{\text{top}}(\mathcal{U}^{r-k}, \mathbf{t}'_{k+1,r}) & \longrightarrow & 1 \end{array}$$
But, according to theorem 4.2, the two last vertical arrows v_r, v_{r-k} are isomorphisms and, by the five lemma so is the first one, $v_r|_{\Pi_{k,r}}$.

For any $\mathbf{t} \in \mathcal{U}_r(\mathbb{C})$, for any $t_0 \in \mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$, any ordering $\mathbf{t}'$ of $\mathbf{t}$ defines generators $Q_1, ..., Q_{r-1}$ of $\pi_1^{\text{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) \simeq H_r$ [FV91] §1.3 as above. With these generators, the cover $\Psi_{r,G} : \mathcal{H}_{r,G}(\mathbf{C}) \to \mathcal{U}_r$ corresponds to the action of H_r on the fiber $(\Psi_{r,G})^{-1}(\mathbf{t}) \simeq \overline{\text{ni}}(\mathbf{C})$ given by
$$Q_i.\mathbf{g} = (g_1, ..., g_{i-1}, g_{i+1}^{g_i}, g_i, g_{i+2}, ..., g_r), \ i = 1, ..., r-1$$
Likewise, the cover $\Psi'_{r,G} : \mathcal{H}'_{r,G}(\mathbf{C}) \to \mathcal{U}^r$ corresponds to the action of SH_r on the fiber $(\psi'_{r,G})^{-1}(\mathbf{t}) \simeq \overline{\text{sni}}(\mathbf{C})$ induced by the one of H_r on $\overline{\text{ni}}(\mathbf{C})$ [FV91] §1.4.

Fix now an $(r-k)$-tuple $\mathbf{t}'_{k+1,r} = (t_{k+1}, ..., t_r) \in \mathcal{U}^{r-k}(\mathbb{C})$ and consider the following cartesian square
$$\begin{array}{ccc} (\mathcal{H}'_{r,G})_{\mathbf{t}'_{k+1,r}} & \longrightarrow & \mathcal{H}'_{r,G} \\ \downarrow{\scriptstyle (\Psi'_{r,G})_{\mathbf{t}'_{k+1,r}}} & \square & \downarrow{\scriptstyle \Psi'_{r,G}} \\ \mathcal{U}^r_{\mathbf{t}'_{k+1,r}} & \longrightarrow & \mathcal{U}^r \end{array}$$
By Grauert-Remmert's Theorem (for $k = 1$, Riemann's Existence Theorem) the etale cover $(\Psi'_{r,G})_{\mathbf{t}'_{k+1,r}} : (\mathcal{H}'_{r,G})_{\mathbf{t}'_{k+1,r}} \to \mathcal{U}^r_{\mathbf{t}'_{k+1,r}}$ extends to a ramified cover $(\overline{\Psi}'_{r,G})_{\mathbf{t}'_{k+1,r}} : (\overline{\mathcal{H}}'_{r,G})_{\mathbf{t}'_{k+1,r}} \to \mathcal{U}^k$ associated with the action of $\Pi_{k,r}$ induced by the one of SH_r on $\overline{\text{sni}}(\mathbf{C})$. When $k = 1$, we obtain a ramified cover $(\overline{\Psi}'_{r,G})_{\mathbf{t}'_{2,r}} : (\overline{\mathcal{H}}'_{r,G})_{\mathbf{t}'_{2,r}} \to \mathbb{P}^1_{\mathbb{C}}$ with branch points $t_2, ..., t_r$ and branch cycle description the images of $(A_{1,i})_{2 \le i \le r}$ under the permutation action of SH_r on $\overline{\text{sni}}(\mathbf{C})$.

Resulting from the branch cycle argument [V99] lemma 2.8, $(\mathcal{H}'_{r,G})_{\mathbf{t}'_{k+1,r}}$ is defined over the field $\mathbb{Q}'_{\mathbf{C}}(\mathbf{t}'_{k+1,r})$ and its image $\Sigma_r((\mathcal{H}'_{r,G})_{\mathbf{t}'_{k+1,r}})$ is defined over a subfield $\mathbb{Q}(\mathbf{C}', \mathbf{t}'_{k+1,r})$ of $\mathbb{Q}'_{\mathbf{C}}(\mathbf{t}'_{k+1,r})$ which can be explicitely computed taking into account the rationality property of $(\mathbf{C}', \mathbf{t}'_{k+1,r})$ (for instance, if $\mathbf{C}$ is a tuple of rational conjugacy classes then $\mathbb{Q}(\mathbf{C}', \mathbf{t}'_{k+1,r}) = \mathbb{Q}(\mathbf{t}_{k+1,r})$). Similar fields can be defined for any field Q of characteristic 0.

4.2 HM-subvarieties

4.2.1 HM-components of Hurwitz spaces

We recall here the definition and main properties of H(arbater)-M(umford) components of Hurwitz spaces, which have been introduced by M. Fried [F95a] and then studied by P. Dèbes and M. Emsalem [DE03]. To do this, we need the notion of H(arbater)-M(umford) type for covers of $\mathbb{P}^1$. Given a finite group G, an even integer $r = 2s \geq 4$ and a *symmetric* r-tuple $\mathbf{C}$ of non trivial conjugacy classes of G, that is consisting of s pairs (C_i, C_i^{-1}), any r-tuple in $\overline{\text{ni}}(\mathbf{C})$ of the form $\mathbf{g} = (g_1, g_1^{-1}, ..., g_s, g_s^{-1}) =: \underline{[g_1, ..., g_s]}$ is called a *Harbater-Mumford representative*; we denote the set of all these r-tuples by $\overline{\text{hm}}(\mathbf{C})$. A G-cover $f : X \to \mathbb{P}^1_{\mathbb{C}}$ with ramification type $[G, \mathbf{C}, \mathbf{t}]$ is said to be *of Harbater-Mumford type* (a HM-G-cover for short) if there exists a topological bouquet $\underline{\gamma}$ for $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ and an r-tuple $\mathbf{g} \in \overline{\text{hm}}(\mathbf{C})$ such that $BCD_{\gamma}(f) = \mathbf{g}$. A *HM-component* of the Hurwitz space $\mathcal{H}_{r,G}(\mathbf{C})$ is the component of some HM-cover. Equivalently, it is a component that corresponds to the orbit of some HM representative under the action of the Hurwitz braid group H_r. The following theorem is proved in [F95a], with the assumption $Z(G) = \{1\}$, and in [DE03] without this assumption; a main tool of these proofs is Wewer's compactification of Hurwitz spaces [W98].

Theorem 4.3 *The union $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})$ of all the HM-components of the Hurwitz space $\mathcal{H}_{2s,G}(\mathbf{C})$ is defined over $\mathbb{Q}_{\mathbf{C}}$. Likewise, the union $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})$ of all the HM-components of the Hurwitz space $\mathcal{H}'_{2s,G}(\mathbf{C})$ is defined over $\mathbb{Q}'_{\mathbf{C}}$.*

Using Fried's terminology, say an r-tuple $\mathbf{C}$ of non trivial conjugacy classes of G is g-*complete* if for any $g_i \in C_i$, $i = 1, ..., r$, we have $G =< g_1, ..., g_r >$ and an $2s$-tuple $\mathbf{C}$ consisting of s pairs (C_i, C_i^{-1}) of non trivial conjugacy classes of G is *HM-*g*-complete* if, when removing a pair (C_i, C_i^{-1}), the remaining $(2s-2)$-tuple is g-complete. Being HM-g-complete is a condition that ensures there is a single HM-component in $\mathcal{H}'_{2s,G}(\mathbf{C})$, as proved in [F95a] Th. 3.21. In particular, if $\mathbf{C}$ is both a rational union of non trivial conjugacy classes of G and HM-g-complete, then the HM-component $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})$ of $\mathcal{H}_{2s,G}(\mathbf{C})$ is an geometrically irreducible variety defined over $\mathbb{Q}$. Likewise, if $\mathbf{C}$ is both a tuple of non trivial rational conjugacy classes of G and HM-g-complete, then the HM-component $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})$ of $\mathcal{H}'_{2s,G}(\mathbf{C})$ is an geometrically irreducible variety defined over $\mathbb{Q}$.

4.2.2 Definition

Given a finite group G and an integer r, the closed subvarieties of $\mathcal{H}_{r,G}$, $\mathcal{H}'_{r,G}$ obtained by specializing some of the branch points are of particularly interest when considering the regular inverse Galois problem. We will deal with special kinds of such subvarieties - we call HM-subvarieties. More precisely, given a symmetric $2s$-tuple $\mathbf{C} = (C_1, C_1^{-1}, ..., C_s, C_s^{-1})$ of non trivial conjugacy classes of G, for any $\mathbf{t}'_{k+1,2s} \in \mathcal{U}^{2s-k}(\overline{\mathbb{Q}})$, with $1 \leq k \leq 2s-1$ we will say that $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})'_{\mathbf{t}'_{k+1,2s}}$ is the *HM-subvariety associated with the data* $(G, \mathbf{C}, \mathbf{t}'_{k+1,2s})$ and that $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'} := \Sigma_{2s}(\mathcal{H}^{HM}_{2s,G}(\mathbf{C})'_{\mathbf{t}'_{k+1,2s}})$ (which is a subset of the fiber of $\Psi_{2s,G}$ above the set of all $\tau \in \mathcal{U}_{2s}(\overline{\mathbb{Q}})$ such that $\mathbf{t} \subset \tau$) is the *symmetrised HM-subvariety associated with the data* $(G, \mathbf{C}, \mathbf{t}'_{k+1,2s})$. Finding HM-subvarieties which are geometrically irreducible and defined over $\mathbb{Q}$ with k small is the aim of this paper.

Starting from a symmetric $2s$-tuple $\mathbf{C} = (C_1, C_1^{-1}, ..., C_s, C_s^{-1})$ such that there is one single HM-component in $\mathcal{H}'_{2s,G}(\mathbf{C})$ - or, equivalently, such that all the HM representatives fall in one single

orbit $O^{HM}(\mathbf{C}) \in \overline{\text{sni}}(\mathbf{C})/SH_{2s}$ - and given $1 \leq k \leq 2s-1$, for any $\mathbf{t}'_{k+1,2s} \in \mathcal{U}^{2s-k}(\overline{\mathbb{Q}})$, the number of geometrically irreducible components of $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{k+1,2s}}$ corresponds to the number of orbits of $O^{HM}(\mathbf{C})/\Pi_{k,2s}$. Consider the associated symmetrised HM-subvariety, $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{k+1,2s}}$. An obvious necessary condition to get one of its geometrically irreducible component defined over $\mathbb{Q}$ is given by the branch cycle argument [V99] Lemma 2.8 that is,

$$(\mathbf{BCArg}) \begin{cases} \bullet\ (\mathbf{C}_{k+1}, ..., \mathbf{C}_{2s}) \text{ is a rational union of conjugacy classes and } \mathbf{t}_{k+1,2s} \in \mathcal{U}_{2s-k}(\mathbb{Q}). \\ \bullet \text{ For any } \sigma \in \mathrm{G}_{\mathbb{Q}},\ \mathbf{C}^{\chi(\sigma)}_{\alpha(\sigma)(i)} = \mathbf{C}_i, \text{ with } k+1 \leq i \leq 2s \text{ where } \chi : \mathrm{G}_{\mathbb{Q}} \to \hat{\mathbb{Z}} \text{ is the} \\ \text{cyclotomic character and } \alpha : \mathrm{G}_{\mathbb{Q}} \to \mathcal{S}_{2s-k} \text{ is the natural representation induced} \\ \text{by the action of } \mathrm{G}_{\mathbb{Q}} \text{ on } \mathbf{t}'_{k+1,2s}. \end{cases}$$

The starting point of our work was problem **B**.2 [F95a] raised by M.Fried and which asks for a sufficient condition to ensure

(**C**1) all the HM representatives fall in one single orbit $O^{HM}_1(\mathbf{C}) \in \overline{\text{sni}}(\mathbf{C})/\Pi_{1,2s}$

Our main theorem (theorem 4.4) gives such a sufficient condition. However, $O^{HM}_1(\mathbf{C})$ may be strictly contained in $O^{HM}(\mathbf{C})$, in which case, for general $\mathbf{t}'$, no geometrically irreducible component of $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'}$ is defined over $\mathbb{Q}$.

Indeed, assume $k=1$ and consider a birational equation $H(t_1, ..., t_{2s}, Y) = 0$ of $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})$. Then $H(t_1, ..., t_{2s}, Y) \in \mathbb{Q}[t_1, ..., t_{2s}, Y]$ is absolutely irreducible. Let $H(t_1, ..., t_{2s}, Y) = \prod_{1 \leq i \leq r} F_i(t_1, Y)$ be the factorization of $H(t_1, ..., t_{2s}, Y)$ into a product of irreducible factors in $\overline{\mathbb{Q}(t_2, ..., t_{2s})}[t_1, Y]$. Assume $r \geq 2$ that is, $H(t_1, ..., t_{2s}, Y)$ splits and let z be a primitive element of the field generated over $\mathbb{Q}(t_2, ..., t_{2s})$ by the coefficients of the $(F_i)_{1 \leq i \leq r}$. The finite Galois extension $\mathbb{Q}(t_2, ..., t_{2s}, z)/\mathbb{Q}(t_2, ..., t_{2s})$ is not trivial and we denote by $h(t_2, ..., t_{2s}, Z) \in \mathbb{Q}[t_2, ..., t_{2s}, Z]$ the irreducible polynomial of z (up to multiplication by an element of $\mathbb{Q}[t_2, ..., t_{2s}]$) over $\mathbb{Q}(t_2, ..., t_{2s})$. By the Bertini-Noether theorem, there exists a Zariski closed subset F of the hypersurface $V(h)$ defined by $h(t_2, ..., t_{2s}, Z) = 0$ such that for any $(t^0_2, ..., t^0_{2s}, z^0) \in V(h)(\overline{\mathbb{Q}}) \setminus F$, the polynomials $(F_i(t^0_2, ..., t^0_{2s}, z^0, t_1, Y))_{1 \leq i \leq r}$ remain irreducible in $\overline{\mathbb{Q}}[t_1, Y]$. Setting $W := (V(h)(\overline{\mathbb{Q}}) \cap \mathbb{Q}^{2s-1} \times \overline{\mathbb{Q}}) \setminus F$, Hilbert irreducibility theorem states there exists a Zariski dense subset U of W such that for any $(t^0_2, ..., t^0_{2s}, z^0) \in U$, $\mathbb{Q}(z^0)/\mathbb{Q}$ is a Galois extension with group $\mathrm{Gal}(\mathbb{Q}(z^0)|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(t_2, ..., t_{2s}, z)|\mathbb{Q}(t_2, ..., t_{2s}))$. In particular, $\mathrm{G}_{\mathbb{Q}}$ acts transitively on the $(F_i(t^0_2, ..., t^0_{2s}, z^0, t_1,$
$Y))_{1 \leq i \leq r}$ the same way as $\mathrm{G}_{\mathbb{Q}(t_2, ..., t_{2s})}$ does on the $(F_i)_{1 \leq i \leq r}$.

To get geometrically irreducible (symmetric) HM-subvarieties defined over $\mathbb{Q}$ we will have to choose $\mathbf{C} = (C_1, C_1^{-1}, ..., C_s, C_s^{-1})$, $1 \leq k \leq 2s-1$ and $\mathbf{t}'_{k+1,2s} \in \mathcal{U}^{2s-k}(\overline{\mathbb{Q}})$ in such a way that (**BCArg**) holds and $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})'_{\mathbf{t}'_{k+1,2s}}$ is geometrically irreducible, which is equivalent to the group theoretic following transitivity condition :

(**C**2) $\Pi_{k,2s}$ acts transitively on the SH_{2s}-orbit $O^{HM}(\mathbf{C})$

Theorem 4.4 gives a sufficient condition depending on the conjugacy classes of G to obtain (**C**2) with k as small as possible.

4.2.3 Irreducible HM-subvarieties defined over $\mathbb{Q}$

4.2.3.1 Statements and comments

Given a group G, for any tuple $\mathbf{a} = (a_1, ..., a_m) \in G^m$ and any tuple $(E_1, ..., E_n)$ of subsets of G, we will write

$$< \mathbf{a}^{<E_1, ..., E_n>} >:=< \{a_1^{e_1}, ..., a_m^{e_m}\}_{e_1, ..., e_m \in <E_1, ..., E_n>} >$$

Given a tuple $\mathbf{A} = (A_1, ..., A_m)$ of subsets of G, the symbol $\mathbf{a} \in \mathbf{A}$ means we consider a tuple of elements $\mathbf{a} = (a_1, ..., a_m)$ with $a_i \in A_i$, $i = 1, ..., m$. Finally, given a tuple $\mathbf{A} = (A_1, ..., A_m)$ of conjugacy classes of G, we write $[\mathbf{A}] = (A_1, A_1^{-1}, ..., A_m, A_m^{-1})$ and $[\mathbf{A}]^r$ for the tuple obtained by repeating r times $[\mathbf{A}]$.

Theorem 4.4 (**Main Theorem**) *Let G be a finite group containing two tuples $\mathbf{A} = (A_1, ..., A_m)$, $\mathbf{B} = (B_1, ..., B_n)$ of non trivial conjugacy classes and consider the following hypotheses :*

$$(\mathbf{H}1)\begin{cases} (\mathbf{H}1.0) & \text{There exists } \mathbf{a} \in \mathbf{A} \text{ such that } G =< \mathbf{a}, \mathbf{B} >. \\ (\mathbf{H}1.1) & < \mathbf{a}^{<\mathbf{b}>} > \text{ acts transitively on } B_i, \text{ for all } \mathbf{a} \in \mathbf{A},\ \mathbf{b} \in \mathbf{B},\ i = 1, ..., n. \\ (\mathbf{H}1.2) & < \mathbf{a}_i^{<\mathbf{B}>} > \text{ acts transitively on } A_i, \text{ for all } \mathbf{a}_i = (a_1, ..., a_{i-1}) \in A_1 \times \cdots \times A_{i-1}, \\ & i = 2, ..., m. \end{cases}$$

$$(\mathbf{H}2) \quad \text{There exists } b_i \in B_i,\ b_j \in B_j \text{ such that } b_i b_j = b_j b_i,\ 1 \leq i \neq j \leq n.$$

Then we have the conclusions

- $(\mathbf{C}1)$ *If $\mathbf{A}$, $\mathbf{B}$ verify $(\mathbf{H}1)$ then for s large enough and writing $\mathbf{C}_s := ([\mathbf{A}], [\mathbf{B}]^s)$, all the HM-representatives fall in one single orbit $\mathrm{O}^{\mathrm{HM}}_{2\mathrm{m}-1}(\mathbf{C}_\mathrm{s}) \in \overline{\mathrm{sni}}(\mathbf{C}_\mathrm{s})/\Pi_{2\mathrm{m}-1,2(\mathrm{m}+\mathrm{sn})}$.*
- $(\mathbf{C}2)$ *If, in addition $\mathbf{B}$ verify $(\mathbf{H}2)$ then $\Pi_{2m-1,2(m+sn)}$ acts transitively on the $SH_{2(m+sn)}$ -orbit $O^{HM}(\mathbf{C}_s) \in \overline{\mathrm{sni}}(\mathbf{C}_s)/SH_{2(m+sn)}$.*

Comments

1. For any $\mathbf{t}' := \mathbf{t}'_{2m,2(m+sn)} \in \mathcal{U}^{2sn+1}(\overline{\mathbb{Q}})$, conclusion $(\mathbf{C}1)$ in theorem 4.4 asserts that the points corresponding to HM-representatives all lie on the same connected component of $\mathcal{H}'^{HM}_{2(m+sn),G}(\mathbf{C}_s)_{\mathbf{t}'}$. Conclusion $(\mathbf{C}2)$ asserts that $\mathcal{H}'^{HM}_{2(m+sn),G}(\mathbf{C}_s)_{\mathbf{t}'}$ is connected and consequently geometrically irreducible defined over $\mathbb{Q}'_{\mathbf{C}_s}(\mathbf{t}')$. The same is true for the corresponding HM-subvariety $\mathcal{H}^{HM}_{2(m+sn),G}(\mathbf{C}_s)_{\mathbf{t}'}$, which is defined over the field $\mathbb{Q}(\mathbf{C}_s, \mathbf{t}')$ contained in $\mathbb{Q}'_{\mathbf{C}_s}(\mathbf{t}')$. Both $\mathcal{H}'^{HM}_{2(m+sn),G}(\mathbf{C}_s)_{\mathbf{t}'}$ and $\mathcal{H}^{HM}_{2(m+sn),G}(\mathbf{C}_s)_{\mathbf{t}'}$ are of dimension $2m-1$. In particular, when $m = 1$, we obtain HM-curves and condition $(\mathbf{H}1.2)$ is empty. The constant $c(G)$ mentioned in the introduction can be defined by

$$c(G) = \min\{2m - 1 | \text{ there exists } \mathbf{A}, \mathbf{B} \text{ verifying } (\mathbf{H}1), (\mathbf{H}2) \text{ with } |\mathbf{A}| = m\}$$

   Also observe that the tuple $\mathbf{C}_s = ([\mathbf{A}], [\mathbf{B}]^s)$ built in theorem 4.4 is far from being unique. For instance, any tuple of the form $(\mathbf{C}_s, B_{i_1}, B_{i_1}^{-1}, ..., B_{i_t}, B_{i_t}^{-1})$, $1 \leq i_1, ..., i_t \leq n$, $t \geq 0$ also works.

2. Instead of $(\mathbf{H}1.1)$ and $(\mathbf{H}1.2)$ one can consider the stronger -but easier to check - conditions

$$\begin{cases} (\mathbf{H}1.1^+) & < \mathbf{a}^{<\mathbf{b}>} >= G, \text{ for all } \mathbf{a} \in \mathbf{A},\ \mathbf{b} \in \mathbf{B}. \\ (\mathbf{H}1.2^+) & < \mathbf{a}_i^{<\mathbf{B}>} >= G, \text{ for all } \mathbf{a}_i = (a_1, ..., a_{i-1}) \in A_1 \times \cdots \times A_{i-1},\ i = 2, ..., m. \end{cases}$$

   These lead to the following practical corollary

   Corollary 4.5 *Let G be a finite group containing two tuples $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$ and $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$ such that*

   - *(i)* $G =< A_1 >=< \mathbf{B} >$.
   - *(ii)* $(\mathbf{A}, \mathbf{B}) \in \mathcal{C}_{m+n}(G)$ *is g-complete.*
   - *(iii)* *There exists $b_i \in B_i$, $b_j \in B_j$ such that $b_i b_j = b_j b_i$, $1 \leq i \neq j \leq n$.*

   Then, for s large enough, writing $\mathbf{C}_s := ([\mathbf{A}], [\mathbf{B}]^s)$, there is a unique $SH_{2(m+sn)}$ HM-orbit $O^{HM}(\mathbf{C}_s) \in \overline{\mathrm{sni}}(\mathbf{C}_s)/SH_{2(m+sn)}$ and $\Pi_{2m-1,2(m+sn)}$ acts transitively on it.

   Proof. For any $\mathbf{a} \in \mathbf{A}$, $\mathbf{b} \in \mathbf{B}$, $< \mathbf{a}^{<\mathbf{b}>} >$ is normal in $< \mathbf{a}, \mathbf{b} >$. But by (ii) $< \mathbf{a}, \mathbf{b} >= G$ thus, $< \mathbf{a}^{<\mathbf{b}>} >$ is normal in G and, in particular, contains $< A_1 >= G$ (by (i)), which implies $(\mathbf{H}1.1^+)$. As for $(\mathbf{H}1.2^+)$, since $< \mathbf{a}_i^{<\mathbf{B}>} >$ is normal in $< B >= G$ (by (i)) so it contains $< A_1 >= G$ (by (i)), which implies $(\mathbf{H}1.2^+)$. □

The hypotheses of corollary 4.5 are fulfilled automatically when G is simple and $(\mathbf{A}, \mathbf{B})$ g-complete (*cf.* example (2)). They also are preserved by Frattini extensions (*cf.* proposition 4.8). However compared with theorem 4.4, corollary 4.5 is often too restrictive (*cf.* examples (1) and (3))

3. Compared with theorem 3.21 of [F95a], observe that theorem 4.4 usually provides lower dimensional geometrically irreducible varieties. For instance, with $G = M_{11}$ and $\mathbf{A} = (8A)$, $\mathbf{B} = (11A)$ (*cf.* example (2) below), the former provides an 8-dimensional variety whereas the latter provides a curve.

4.2.3.2 Examples

The purpose of this section is to give examples of groups verifying (**H**1.1), (**H**1.2) and (**H**2) (condition (**H**1.0) is here to ensure $\overline{\text{hm}}(\mathbf{C})$ is not empty and it will always be fulfilled in our examples - where either the tuple $(\mathbf{A}, \mathbf{B})$ is g-complete or the stronger condition (**H**1.1^+) holds). We are particularly interested in minimizing m that is, obtaining HM-subvarieties of low dimension.

(1) Symmetric and alternating groups : Consider the symmetric group $\mathcal{S}_p$ where $p \geq 5$ is a prime number, $\mathbf{A} = (C^{(p)})$ and $\mathbf{B} = (C^{(2)})$ where $C^{(i)}$ denotes the conjugacy class of i-cycles in G, $i = 2, ..., p$. For any $a \in C^{(p)}, b \in C^{(2)}$, $< a^{<b>} ><\lhd< a, b >$. But $< a, b >$ is a transitive group of prime degree p, so it is primitive [Wi84] Th.8.3 and, since it contains a 2-cycle, it is $\mathcal{S}_p$ Th.13.3 [Wi84]. As a consequence $< a^{<b>} >= \mathcal{A}_p$, which acts transitively on the 2-cycles class. Likewise, consider the alternating group $G := \mathcal{A}_p$ where $p \geq 5$ is a prime number, $\mathbf{A} = (C^{(p)})$ and $\mathbf{B} = (C^{(3)})$. For any $a \in C^{(p)}, b \in C^{(3)}$, $< a^{<b>} ><\lhd< a, b >$. But $< a, b >$ is a transitive group of prime degree p, so it is primitive and, since it contains a 3-cycle it is $\mathcal{A}_p$ [Wi84] Th. 13.3. So conditions (**H**1) and (**H**2) hold.

(2) Non abelian finite simple groups : Suppose G is a non abelian finite simple group. With the notation of corollary 4.5, observe that since G is simple hypotheses (i) is automatically fulfilled since the groups $< A_1 >, < \mathbf{B} >$ are normal. So we are only left to check hypotheses (ii) and (iii). Taking $n = 1$, (iii) is automatically fulfilled too. So, for a simple group G we always have $c(G) \leq 2l(G) - 3$ where $l(G)$ denotes the minimal length of a g-complete tuple $(A_1, ..., A_m, B)$ of non trivial conjugacy classes of G

Example 4.6 *1.* According to the Atlas, the Mathieu group M_{11} has 10 conjugacy classes : 1A, 2A, 3A, 4A, 5A, 6A, 8A, B**, 11A, B** and its maximal subgroups have order 720, 660, 144, 120, 48. Since none of these orders can be divided by both 8 and 11, (8A, 11A) is a g-complete 2-tuple for M_{11}. So, M_{11} satisfies (**H**1) with $\mathbf{A} = (8A)$, $\mathbf{B} = (11A)$.

2. The argument above, using the maximal subgroups given by the Atlas, works for instance with $m = 1$ and
M_{23} with $A = 7A$ and $B = 11A$, (443520, 40320, 20160, 7920, 5760, 253).
$Sz(8)$ with $A = 5A$ and $B = 7A$, (448, 52, 20, 14).
J_2 with $A = 5A$ and $B = 7A$, (6048, 2160, 1920, 1152, 720, 600, 336, 300, 60).
J_3 with $A = 5A$ and $B = 17A$, (8160, 3420, 2880, 2448, 2160, 1944, 1920, 1152).
Ly with $A = 37A$ and $B = 67A$, (5859.10^6, 5388768.10^3, 465.10^5, 299168.10^2, 9.10^6, 3849120, 699840, 1474, 666).
etc.

3. Consider the projective special linear groups $\mathrm{L}_2(p)$ where $p \equiv 3$ [mod4], $p \geq 7$ is a prime number. Then, by a theorem of Dickson [**?**] :*Let $p \geq 5$ a prime number, then the order of the maximal subgroups of the projective special linar group $L_2(p)$ belongs to $\{\frac{p(p-1)}{2}, p-1, p+1, 60\}$ if $p \equiv \pm 1$* [mod10] *and to $\{\frac{p(p-1)}{2}, p-1, p+1, 24, 12\}$ else*, the tuple $(2A, pA)$ is g-complete.

(3) Families of p-groups : All the assertions in the following can be found in [Su86], Chap. 2 §2 or Chap. 4 §4.

(3-1) $p = 2$: Then G is one of the following groups :
- Dihedral group of order 2^n : $D_{2^n} =< x, y | x^{2^{n-1}} = y^2 = 1,\ yxy = x^{-1} >$.

- Special dihedral group of order 2^n : $S_{2^n} =< x, y | x^{2^{n-1}} = y^2 = 1,\ yxy = x^{-1+2^{n-2}} >$.
- Generalized quaternion group of order 2^n : $Q_{2^n} =< x, y | x^{2^{n-1}} = y^2,\ y^{-1}xy = x^{-1} >$.

and, taking $A = C_y^G$, $B = C_x^G$, using the relations, one immediately checks that for each $a \in A$ $B = \{x, axa^{-1}\}$, so condition (**H**1.1) is fulfilled and, since $m = n = 1$, conditions (**H**1.2) and (**H**2) are empty.

(3-2) $\underline{p > 2}$: Recall that for any finite p-group G with Frattini

Lemma 4.7 *Let G be a finite group with Frattini subgroup $\Phi(G)$. Assume the quotient $G/\Phi(G)$ is abelian, then,, for any $x_1, ..., x_d \in G$ such that $G/\Phi(G) = \bigoplus_{i=1}^d < \overline{x_i} >$, the tuple $\mathbf{C} := (C_{x_1}^G, ..., C_{x_d}^G)$ is g-complete.*

Proof. Indeed, for any $g_1, ..., g_d \in G$, since $G/\Phi(G)$ is abelian, one has $\overline{x_i^{g_i}} = \overline{x_i}$, $i = 1, ..., r$ so $G =< x_1^{g_1}, ..., x_d^{g_d}, \Phi(G) >$ which, by the characterization of the Frattini subgroup, implies $G =< x_1^{g_1}, ..., x_d^{g_d} >$. □

A finite p-group G has the property that $G/\Phi(G)$ is an elementary abelian p-group. Assume furthermore that $\Phi(G) = Z(G)$ and $G/\Phi(G) =< \overline{x} > \oplus < \overline{y} >$. Then any $g \in G$ can be written in a unique way $g = x^{u_g} y^{v_g} \phi_g = y^{v_g} x^{u_g} \psi_g$ with $\phi_g, \psi_g \in Z(G)$ and all the elements in $A := C_y^G$ are of the form $y\phi$, $\phi \in Z(G)$ thus, for any $a \in A$, $B = C_x^G = \{a^i x a^{-i}\}_{i \geq 0}$ with $< a > \subset < a^{<b>} >$ for any $b \in B$. This shows (**H**1.1) is fulfilled and, once again, since $m = n = 1$, conditions (**H**1.2) and (**H**2) are empty. The following groups satisfy these hypotheses :

- $M(p^n) =< x, y | x^{p^{n-1}} = y^p = 1,\ y^{-1}xy = x^{1+p^{n-2}} >$.
- Any non abelian group of order p^3 (Recall that an abelian group of order p^3 is isomorphis to D_8 or Q_8 if $p = 2$ or to $M(p^3)$ or $E(p^3)$ if $p > 2$, where

$$E(p^3) < x, y | x^p = y^p = [x, y]^p = 1,\ [x, y] \in Z(E(p^3)) >$$

(4) $\underline{\text{Frattini extensions :}}$ The next result is about Frattini extensions ; it is related to Modular Towers §4.4.1.2 and will be proved in 4.3.2. It will give us information about regular realizations of finite unsplit extensions of a given finite group G, which is a difficult matter, even when the group G is known to be regularly realized (this is the theory of embedding problems, [MMa99], Chap.V)

Proposition 4.8 (Frattini covers) *Let G be a finite group verifying* (**H**1.0), (**H**1.1$^+$),(**H**1.2$^+$) *with* $\mathbf{A} = (A_1, ..., A_m)$, $\mathbf{B} = (B_1, ..., B_n)$. *Then, for s large enough,* $([\mathbf{A}], [\mathbf{B}]^s)$ *verifies* (**C**1) *and*

(**C**3) *Given a finite Frattini cover $\tilde{G} \to G$, for any tuples $\tilde{\mathbf{A}}$, $\tilde{\mathbf{B}}$ above $\mathbf{A}$, $\mathbf{B}$, the tuple* $([\tilde{\mathbf{A}}], [\tilde{\mathbf{B}}]^s)$ *verifies* (**C**1).

We have the following additional conclusions :

(**C**4) *If the B_i, $i = 1, ..., n$ are p'-conjugacy classes for a given prime number p and G,* $\mathbf{A}$, $\mathbf{B}$ *verify* (**H**2) *then, given a finite Frattini cover $\tilde{G} \to G$ with p-group kernel, there exists tuples* $\tilde{\mathbf{A}}$,$\tilde{\mathbf{B}}$ *of conjugacy classes of $\tilde{G}$ above* $\mathbf{A}$ *and* $\mathbf{B}$ *such that the tuple* ($[\tilde{\mathbf{A}}]$, $[\tilde{\mathbf{B}}]^s$) *verifies* (**C**1) *and* (**C**2).

(**C**5) *If $n = 1$ then, given a finite Frattini cover $\tilde{G} \to G$, for any tuples $\tilde{\mathbf{A}}$, $\tilde{\mathbf{B}}$ above* $\mathbf{A}$, $\mathbf{B}$, *the tuple* $([\tilde{\mathbf{A}}], [\tilde{\mathbf{B}}]^s)$ *verifies* (**C**1) *and* (**C**2).

Example 4.9 Here are two examples of central Frattini extensions we will deal with in the following :
- If G is perfect (that is, $G = [G, G]$) then, by Schur's theorem, the universal central extension $\hat{G} \twoheadrightarrow G$ of G exists ; furthermore, it is finite, Frattini and its kernel is the Schur Multiplier $M(G)$ of G.
- If G is p-perfect (that is generated by elements of prime-to-p order) for some prime p dividing $|G|$ then the universal central p-extension $\widehat{{}^pG} \twoheadrightarrow G$ of G exists ; furthermore, it is finite, Frattini and its kernel is the p-part $M(G)_p$ of the Schur Multiplier $M(G)$ of G.

4.3 Group theoretical proofs

This section is devoted to the proofs of theorems 4.4 and proposition 4.8. They rely on the following technical lemma, the proof of which is postponed to section 4.3.3 :

Lemma 4.10 *Given a finite group G and a symmetric $2s$-tuple $\mathbf{C} = [C_1, ..., C_s] \in \mathcal{C}_{2s}(G)$.*
(1) For any $1 \leq k \leq s$ there exists $u_k \in \Pi_{1,2s}$ such that for any HM representative $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$

$$u_k \cdot \mathbf{g} = [g_1, ..., g_k^{g_1}, ..., g_s]$$

(2) For any $2 \leq k \leq s$ and for any $\underline{i} = (i_1, ..., i_r)$ with $2 \leq i_1 < i_2 < ... < i_r \leq k-1$ there exists $v_{\underline{i},k} \in \Pi_{1,2s}$ such that for any HM representative $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$

$$v_{\underline{i},k} \cdot \mathbf{g} = [g_1, ..., g_k^{g_1^{g_{i_r} \cdots g_{i_1}}}, ..., g_s]$$

(3) For any $2 \leq k \leq s$, for any $\underline{i} = (i_1, ..., i_r)$ with $k+1 \leq i_1 < i_2 < ... < i_r \leq s-1$ there exists $w_{k,\underline{i}} \in \Pi_{1,2s}$ such that for any HM representative $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$

$$w_{k,\underline{i}} \cdot \mathbf{g} = [g_1, ..., g_k^{g_1^{g_{i_r} \cdots g_{i_1}}}, ..., g_s]$$

The underlying idea of lemma 4.10 (and of the whole proof) is that, the larger the tuple $[C_2, ..., C_s]$ is, the larger the groups G_k generated by the $g_1^{g_{i_r} \cdots g_{i_1}}$, $2 \leq i_1 < i_2 < ... < i_r \leq k-1$ (resp. $k+1 \leq i_1 < i_2 < ... < i_r \leq s-1$) are; our purpose is to show that under the assumptions of theorem 4.4 these groups are large enough to act transitively on the conjugacy classes $C_2, ..., C_s$.

4.3.1 Proof of theorem 4.4

In the following, we say $\sigma = (\sigma(1), ..., \sigma(\nu))$ is an ordered ν-tuple in a subset $\Sigma \subset \mathbb{N}$ if $\sigma(k) \in \Sigma$, $k = 1, ..., \nu$ and $\sigma(1) < \sigma(2) < ... < \sigma(\nu)$. Given such an ordered ν-tuple σ, we write $\sigma + l$ for the translated ordered ν-tuple $(\sigma(1) + l, ..., \sigma(\nu) + l)$.

4.3.1.1 Case $m = 1$

Let G be a finite group and A, $\mathbf{B} = (B_1, ..., B_n)$ be $n+1$ non trivial conjugacy classes of G.

(1) Given $\mathbf{b} = (b_1, ..., b_n) \in \mathbf{B}$, write $< \mathbf{b} >= \{\beta_1, ..., \beta_s\}$; each β_j can be written as a product of say $s(j)$ terms of the form $\mathbf{b}_{\sigma_{k,j}} := b_{\sigma_{k,j}(1)} \cdots b_{\sigma_{k,j}(\nu_{k,j})}$ where $\sigma_{k,j} = (\sigma_{k,j}(1), ..., \sigma_{k,j}(\nu_{k,j}))$ is an ordered tuple in $\{1, ..., n\}$, $k = 1, ..., s(j)$, $j = 1, ..., s$. Setting $N(\mathbf{b}) = \max\{s(j)\}_{1 \leq j \leq s}$, the set

$$\{\mathbf{b}_{\sigma_1} \cdots \mathbf{b}_{\sigma_s}\}_{\substack{\sigma \text{ ordered tuple in } \{1,...,n\} \\ s \leq N(\mathbf{b})}}$$

contains $< \mathbf{b} >$, that is, is equal to $< \mathbf{b} >$. And, since by definition $< a^{<\mathbf{b}>} >$ is the subgroup generated by $\{a^b\}_{b \in <\mathbf{b}>}$, one deduces from the above that

$$< a^{<\mathbf{b}>} >=< \{a^{\mathbf{b}_{\sigma_1} \cdots \mathbf{b}_{\sigma_s}}\}_{\substack{\sigma \text{ ordered tuple in } \{1,...,n\} \\ s \leq N(\mathbf{b})}} >$$

(2) Write $N_i = |B_i|$, $i = 1, ..., n$ and $N^0 = \max\{\mathrm{N}(\mathbf{b})\}_{\mathbf{b} \in \mathbf{B}}$ and set $N = N_1 \cdots N_n N^0$. Then, for any $(b_{i,1}, ..., b_{i,n})_{1 \leq i \leq N} \in \mathbf{B}^N$ there is at least one $\mathbf{b} = (b_1, ..., b_n) \in \mathbf{B}$ which is repeated N^0 times among the $(b_{i,1}, ..., b_{i,n})$, $i = 1, ..., N$ and since $N(\mathbf{b}) \leq N^0$, step (1) yields :

Lemma 4.11 *There exists* $N := N(\mathbf{B}) \geq 1$ *depending only on* $\mathbf{B}$ *such that for any* $(u_i)_{1\leq i\leq nN} := (b_{i,1},...,b_{i,n})_{1\leq i\leq N} \in \mathbf{B}^N$ *there exists* $\mathbf{b} \in \mathbf{B}$ *satisfying*

$$< a^{<\mathbf{b}>} >=< \{a^{u_{\sigma(\nu)}\cdots u_{\sigma(1)}}\}_{\sigma \text{ ordered tuple in } \{1,...,nN\}} >, \text{ for each } a \in A$$

We now show that, for $x \geq N(\mathbf{B})+1$, the tuple $\mathbf{C}_x = ([A],[\mathbf{B}]^{2x})$ will satisfy $(\mathbf{C}1)$ provided A, $\mathbf{B}$ satisfy $(\mathbf{H}1)$ and $(\mathbf{C}2)$ provided $\mathbf{B}$ also satisfies $(\mathbf{H}2)$.

$(\mathbf{H}1) \Rightarrow (\mathbf{C}1)$: For any $1 \leq k \leq 4nx$ one can always find in $[\mathbf{B}]^{2x}$ either $N(\mathbf{B})+1$ copies of $[\mathbf{B}]$ before k (if $2nx \leq k \leq 4nx$) or $N(\mathbf{B})+1$ copies of $[\mathbf{B}]$ after k (if $0 \leq k \leq 2nx$). Let $\mathbf{g} = [a, h_1, ..., h_{2nx}] \in \overline{\text{hm}}(\mathbf{C}_x)$ be a HM-representative and $g \in G$. We are to show that, for any $1 \leq k \leq 2nx$, $\mathbf{g}$ and $[a, h_1, ..., h_k^g, ..., h_{2nx}]$ fall in the same orbit under $\Pi_{1,4nx+2}$. Suppose for instance $2nx \leq 2k \leq 4nx$, that is there are at least $N(\mathbf{B})+1$ copies of $[\mathbf{B}]$ before k and so, according to lemma 4.11, there is at least one n-tuple $\mathbf{b} = (b_1,...,b_n) \in \mathbf{B}$ such that $< a^{<\mathbf{b}>} >$ is generated by the set $\{a^{h_{\sigma(\nu)}\cdots h_{\sigma(1)}}\}_{\sigma \text{ ordered tuple in } \{1,...,nx-1\}}$. But since $< a^{<\mathbf{b}>} >$ acts transitively on the conjugacy class of h_k, we can assume that $g \in < a^{<\mathbf{b}>} >$ and, consequently, that g can be written as a product $x_1 \cdots x_s$ of s terms of the form $x_k = a^{h_{\sigma_k(\nu_k)}\cdots h_{\sigma_k(1)}}$, where $\sigma_k = (\sigma_k(1),...,\sigma_k(\nu_k))$ is an ordered tuple in $\{1,...,nx-1\}$, $k = 1,...,s$. So, we are left to do the following s operations

$$\begin{array}{rcl} \mathbf{g} & \rightarrow & [a, h_1, ..., h_k^{x_s}, ..., h_{2nx}] \\ & \rightarrow & [a, h_1, ..., h_k^{x_{s-1}x_s}, ..., h_{2nx}] \\ & \cdots & \\ & \rightarrow & [a, h_1, ..., h_k^{x_1\cdots x_{s-1}x_s}, ..., h_{2nx}] \end{array}$$

But, according to part (2) of lemma 4.10, these can be handled by applying successively $v_{\sigma_s+1,k+1}$, $v_{\sigma_{s-1}+1,k+1}$ *etc.*, $k = 1,...,s$. If $1 \leq k \leq 4nx$, use part (3) of lemma 4.10 instead of part (2).

$(\mathbf{H}1)$ & $(\mathbf{H}2) \Rightarrow (\mathbf{C}2)$: From now on, we denote by $\mathbf{C}$ the tuple $\mathbf{C}_x$ built above and set $s = 2nx+1$. We assume furthermore $(\mathbf{H}2)$ is fulfilled that is, there exists $b_i \in B_i$, $b_j \in B_j$ such that $b_ib_j = b_jb_i$, $1 \leq i \neq j \leq n$. We have shown that all the HM-representatives fall in one single orbit $\text{O}_1^{\text{HM}}(\mathbf{C}) \in \overline{\text{sni}}(\mathbf{C})/\Pi_{1,2s}$ so in one single orbit $\text{O}_2^{\text{HM}}(\mathbf{C}) \in \overline{\text{sni}}(\mathbf{C})/\Pi_{2,2s}$ as well. In the first place, we prove the $\Pi_{2,2s}$ HM-orbit $\text{O}_2^{\text{HM}}(\mathbf{C})$ has the same length as the SH_{2s} HM-one $\text{O}^{\text{HM}}(\mathbf{C})$, that is, they coincide. In the second place we show that $\text{O}_2^{\text{HM}}(\mathbf{C}) = \text{O}_1^{\text{HM}}(\mathbf{C})$.

Condition $(\mathbf{H}2)$ implies SH_{2s} leaves $\text{O}_2^{\text{HM}}(\mathbf{C})$ globally invariant. Indeed, since $\Pi_{2,2s}$ is normal in SH_{2s}, SH_{2s} permutes the orbits of $\overline{\text{sni}}(\mathbf{C})/\Pi_{2,2s}$. But, for any HM-representative $\mathbf{g} = [g_1,...,g_s] \in \overline{\text{hm}}(\mathbf{C})$, straightforward computations give

$$\left\{\begin{array}{l} a_{2i,2j}\cdot\mathbf{g}=([g_1,...,g_{i-1}], g_i, (g_i^{-1})^{g_i^{-1}g_j}, [g_{i+1},...,g_{j-1}], g_j^{g_i^{-1}}, g_j^{-1}, [g_{j+1},...,g_{2nx+1}]),\ 2 \leq i < j \leq s \\ a_{2i,2j+1}\cdot\mathbf{g}=([g_1,...,g_{i-1}], g_i, (g_i^{-1})^{g_i^{-1}g_j^{-1}}, [g_{i+1},...,g_{j-1}], g_j, (g_j^{-1})^{g_j^{-1}g_i^{-1}}, [g_{j+1},...,g_{2nx+1}]),\ 2 \leq i \leq j \leq s-1 \\ a_{2i-1,2j}\cdot\mathbf{g}=([g_1,...,g_{i-1}], g_i^{g_j}, g_i^{-1}, [g_{i+1},...,g_{j-1}], g_j^{g_i}, g_j^{-1}, [g_{j+1},...,g_{2nx+1}]),\ 2 \leq i \leq j \leq s \\ a_{2i-1,2j+1}\cdot\mathbf{g}=([g_1,...,g_{i-1}], g_i^{g_j^{-1}}, g_i^{-1}, [g_{i+1},...,g_{j-1}], g_j, (g_j^{-1})^{g_j^{-1}g_i}, [g_{j+1},...,g_{2nx+1}]),\ 2 \leq i < j-1 \leq s-2 \end{array}\right.$$

Consequently, any HM-representative $\mathbf{g} = [g_1,...,g_s] \in \overline{\text{hm}}(\mathbf{C})$ with $g_ig_j = g_jg_i$ - such a HM representative always exists according to $(\mathbf{H}2)$ and the way $\mathbf{C}$ was built - is fixed by $a_{i,j}$ that is, $a_{i,j}\cdot O_2^{HM}(\mathbf{C}) = O_2^{HM}(\mathbf{C})$, $3 \leq i < j \leq 2s$. And, since $O_2^{HM}(\mathbf{C})$ is a $\Pi_{2,2s}$ orbit, we obviously have $a_{i,j}\cdot O_2^{HM}(\mathbf{C}) = O_2^{HM}(\mathbf{C})$, $i = 1, 2 < j \leq 2s$. Consequently

$$\begin{array}{rcccl} SH_{2s}\cdot O_2^{HM}(\mathbf{C}) & = & O_2^{HM}(\mathbf{C}) & & \\ & \supset & SH_{2s}\cdot\overline{\text{hm}}(\mathbf{C}) & = & O^{HM}(\mathbf{C}) \end{array}$$

We now show that $O_1^{HM}(\mathbf{C}) = O_2^{HM}(\mathbf{C})$. As above, $\Pi_{1,2s}$ being normal in $\Pi_{2,2s}$ entails that $\Pi_{2,2s}$ permutes the orbits of $\overline{\text{sni}}(\mathbf{C})/\Pi_{1,2s}$. Thus, it is enough to show that for any $i = 3,...,2s$ there

exists $\mathbf{g} \in \overline{\mathrm{hm}}(\mathbf{C})$ with $a_{2,i} \cdot \mathbf{g} \in O_1^{HM}(\mathbf{C})$. But, for any HM-representative $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$ straightforward computations give

$$\left\{ \begin{array}{lcl} a_{2,2i+1}^{-1} \cdot \mathbf{g} & = & (g_1, (g_1^{-1})^{g_i}, [g_2, ..., g_{i-1}], g_i, (g_i^{-1})^{g_1}, [g_{i+1}, ..., g_s]) \\ & = & (g_1^{g_i^{-1}}, g_1^{-1}, [g_2^{g_i^{-1}}, ..., g_{i-1}^{g_i^{-1}}], g_i, (g_i^{-1})^{g_i^{-1} g_1}, [g_{i+1}^{g_i^{-1}}, ..., g_s^{g_i^{-1}}]) \\ a_{2,2i}^{-1} \cdot \mathbf{g} & = & (g_1, (g_1^{-1})^{g_i^{-1}} [g_2, ..., g_{i-1}], g_i^{g_i^{-1} g_1}, g_i^{-1}, [g_{i+1}, ..., g_s]) \\ & = & (g_1^{g_i}, g_1^{-1} [g_2^{g_i}, ..., g_{i-1}^{g_i}], g_i^{g_1}, g_i^{-1}, [g_{i+1}^{g_i}, ..., g_s^{g_i}]) \end{array} \right.$$

and, by lemma 4.10, there exists $u_{i,\mathbf{g}}, v_{i,\mathbf{g}} \in \Pi_{1,2s}$ such that

$$\left\{ \begin{array}{lcl} u_{i,\mathbf{g}} \cdot \mathbf{g} & = & [g_1, [g_2^{g_i^{-1}}, ..., g_{i-1}^{g_i^{-1}}], g_i, [g_{i+1}^{g_i^{-1}}, ..., g_{2nx+1}^{g_i^{-1}}]] \\ v_{i,\mathbf{g}} \cdot \mathbf{g} & = & [g_1, [g_2^{g_i}, ..., g_{i-1}^{g_i}], g_i, [g_{i+1}^{g_i}, ..., g_{2nx+1}^{g_i}]] \end{array} \right.$$

so,

$$\left\{ \begin{array}{lcl} a_{1,2i} \cdot u_{i,\mathbf{g}} \cdot \mathbf{g} & = & a_{2,2i+1}^{-1} \cdot \mathbf{g} \\ a_{1,2i-1} v_{i,\mathbf{g}} \cdot \mathbf{g} & = & a_{2,2i}^{-1} \cdot \mathbf{g} \end{array} \right.$$

□

4.3.1.2 Case $m \geq 2$

Keeping the same notation as above the $2s$-tuple we are going to consider will be once again of the form $\mathbf{C}_x = ([\mathbf{A}], [\mathbf{B}]^{2x})$ with x large enough. The following lemma is a straightforward generalization of lemma 4.11.

Lemma 4.12 *Let G be a finite group andconsider two tuples $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$, $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$. There exists $N := N(\mathbf{B}) \geq 1$ depending only on $\mathbf{B}$ such that for any $(u_i)_{1 \leq i \leq nN} := (b_{i,1}, ..., b_{i,n})_{1 \leq i \leq N} \in \mathbf{B}^N$ there exists $\mathbf{b} \in \mathbf{B}$ satisfying*

$$< \mathbf{a}^{<\mathbf{b}>} > = < \{ a_i^{u_{\sigma(\nu)} \cdots u_{\sigma(1)}} \}_{\substack{1 \leq i \leq m \\ \sigma \text{ ordered tuple in } \{1,...,nN\}}} >, \text{ for each } \mathbf{a} \in \mathbf{A}$$

(**H**1) ⇒ (**C**1) & (**C**2) : As in section 4.3.1.1, if $x \geq N + 1$, condition (**H**1.1) ensures two HM-representatives of the form $[a_1, ..., a_m, h_1, ..., h_{2nx}]$ and $[a_1, ..., a_m, h_1^{g_1}, ..., h_{2nx}^{g_{2nx}}]$ fall in the same orbit under $\Pi_{2m-1,4nx+2m}$. To prove it, just observe the method used to construct the elements u_k, $v_{\underline{i},k}$, $w_{k,\underline{i}}$ of $\Pi_{1,2s}$ in lemma 4.10 gives similarly elements u_k^i, $v_{\underline{i},k}^i$, $w_{k,\underline{i}}^i$ of $\Pi_{2i-1,2s}$ such that

$$\left\{ \begin{array}{ll} u_k^i \cdot \mathbf{g} = [g_1, ..., g_k^{g_i}, ..., g_s] & , 1 \leq i < k \leq s \\ v_{i_1 < ... < i_r, k}^i \cdot \mathbf{g} = [g_1, ..., g_k^{g_{i_r} \cdots g_{i_1}}, ..., g_s] & , \underline{i} = (i_1, ..., i_r) \text{ with } i < i_1 < i_2 < ... < i_r < k \\ w_{k, i_1 < ... < i_r}^i \cdot \mathbf{g} = [g_1, ..., g_k^{g_{i_r} \cdots g_{i_1}}, ..., g_s] & , \underline{i} = (i_1, ..., i_r) \text{ with } i < k < i_1 < i_2 < ... < i_r \end{array} \right.$$

Now, let $2 \leq i \leq m$ and $g \in G$. We are left to show $\mathbf{g} = [a_1, ..., a_m, h_1, ..., h_{2nx}]$ and $[a_1, ..., a_i^g, ..., a_m, h_1^{g_1}, ..., h_{2nx}^{g_{2nx}}]$ fall in the same orbit under $\Pi_{2m-1,4nx+2m}$. First note that there exists a constant $M \geq 1$ such that any element of $< \mathbf{B} >$ can be written as the product of at most M elements of $\cup_{1 \leq i \leq n} B_i$. Up to increasing the number x of copies of $\mathbf{B}^0$, we assume $2x \geq M$. Since $< \mathbf{a}_i^{<\mathbf{B}>} >$ acts transitively on the conjugacy class of a_i, we can assume that $g \in < \mathbf{a}_i^{<\mathbf{B}>} >$ and consequently that g can be written as the product $x_1 \cdots x_s$ of s terms of the form $x_k = a_{i_k}^{b_{k,\nu_k} \cdots b_{k,1}}$, where $i_k \in \{1, ..., i-1\}$, $b_{k,j} \in \cup_{1 \leq i \leq n} B_i$, $j = 1, ..., \nu_k$ and $\nu_k \leq M$, $k = 1, ..., s$. So, this time, we have to carry out the following s operations

$$\begin{array}{lcl} \mathbf{g} & \rightarrow & [a_1, ..., a_i^{x_s}, ..., a_m, h_1, ..., h_{2nx}] \\ & \rightarrow & [a_1, ..., a_i^{x_{s-1} x_s}, ..., a_m, h_1, ..., h_{2nx}] \\ & \cdots & \\ & \rightarrow & [a_1, ..., a_i^{x_1 \cdots x_{s-1} x_s}, ..., a_m, h_1, ..., h_{2nx}] \end{array}$$

Since $2x \geq M$, one can always find $(h'_1, ..., h'_{2nx}) \in \mathbf{B}^{2x}$ and s ordered tuples $\sigma_k = (\sigma_k(1), ..., \sigma_k(\nu_k))$ in $\{1, ..., 2nx\}$, $k = 1, ..., s$ such that $b_{k,i} = h'_{\sigma_k(i)}$, $i = 1, ..., \nu_k$, $k = 1, ..., s$. But, as already noticed, $[a_1, ..., a_m, h_1, ..., h_{2nx}]$ and $[a_1, ..., a_m, h'_1, ..., h'_{2nx}]$ fall in the same orbit of $\Pi_{2m-1,4nx+2m}$. Then apply successively the elements $w^{i_s}_{\sigma_s+m,i}$, $w^{i_{s-1}}_{\sigma_{s-1}+m,i}$ *etc.*, $k = 1, ..., r$ to $[a_1, ..., a_m, h'_1, ..., h'_{2nx}]$ in order to obtain $[a_1, ..., a_i^g, ..., a_m, h'_1, ..., h'_{2nx}]$. To conclude, use once again that $[a_1, ..., a_i^g, ..., a_m, h'_1, ..., h'_{2nx}]$ and $[a_1, ..., a_i^g, ..., a_m, h_1, ..., h_{2nx}]$ fall in the same orbit of $\Pi_{2m-1,4nx+2m}$.

$\underline{(\mathbf{H}1)\ \&\ (\mathbf{H}2) \Rightarrow (\mathbf{C}3)}$: This part of the proof remains unchanged since $(\mathbf{H}2)$ ensures SH_{4nx+2m} leaves $O^{HM}_{2m-1}(\mathbf{C}_x)$ globally invariant.

4.3.2 Proof of proposition 4.8

We retain the notation of 4.3.1.1, 4.3.1.2 and of proposition 4.8. Consider the integer $N := N(\mathbf{B}) \geq 1$ defined in lemma 4.12. Then, according to $(\mathbf{H}1^+)$, for any $(\tilde{u}_i)_{1\leq i\leq nN} := (\tilde{b}_{i,1}, ..., \tilde{b}_{i,n})_{1\leq i\leq N} \in \tilde{\mathbf{B}}^N$ there exists $\tilde{\mathbf{b}} \in \tilde{\mathbf{B}}$ satisfying

$$G =< \{s(\tilde{a}_i^{\tilde{u}_{\sigma(\nu)}\cdots\tilde{u}_{\sigma(1)}})\}_{\substack{1\leq i\leq m \\ \sigma \text{ ordered tuple in } \{1,...,nN\}}} >, \text{ for each } \tilde{\mathbf{a}} \in \tilde{\mathbf{A}}$$

But, $s : \tilde{G} \to G$ being a Frattini cover, this entails

$$\tilde{G} =< \{\tilde{a}_i^{\tilde{u}_{\sigma(\nu)}\cdots\tilde{u}_{\sigma(1)}}\}_{\substack{1\leq i\leq m \\ \sigma \text{ ordered tuple in } \{1,...,nN\}}} >, \text{ for each } \tilde{\mathbf{a}} \in \tilde{\mathbf{A}}$$

So we can always take $N = N(\mathbf{B}) = N(\tilde{\mathbf{B}})$. Now, recall that in $(\mathbf{H}1) \Rightarrow (\mathbf{C}1)$ & $(\mathbf{C}2)$ we have also imposed that $2x \geq M$. The Frattini property shows M does not have to be increased when passing from G to $\tilde{G}$. Indeed, $(\mathbf{H}2^+)$ means that

$$G =< \{s(\tilde{a}_k^{\tilde{\beta}_1\cdots\tilde{\beta}_l})\}_{\substack{1\leq k\leq i-1 \\ \beta_j\in\cup_{1\leq i\leq n}\tilde{B}_i,\ l\leq M}} \text{ for each } \tilde{\mathbf{a}}_i \in \tilde{\mathbf{A}}_1 \times \cdots \times \tilde{\mathbf{A}}_1,\ i = 2, ..., m.$$

which entails that

$$\tilde{G} =< \{\tilde{a}_k^{\tilde{\beta}_1\cdots\tilde{\beta}_l})\}_{\substack{1\leq k\leq i-1 \\ \beta_j\in\cup_{1\leq i\leq n}\tilde{B}_i,\ l\leq M}} \text{ for each } \tilde{\mathbf{a}}_i \in \tilde{\mathbf{A}}_1 \times \cdots \times \tilde{\mathbf{A}}_1,\ i = 2, ..., m.$$

This and section 4.3.1.2 show the $4nx + 2m$-tuple $\tilde{\mathbf{C}}$ one gets replacing A_i by $\tilde{A}_i$, $i = 1, ..., n$ and B_i by $\tilde{B}_i$, $i = 1, ..., m$ satisfies $(\mathbf{C}1)$. As for the second part of proposition 4.8, we are left to show $\tilde{\mathbf{B}}$ can be chosen in such a way that the commutativity conditions $(\mathbf{H}2)$ are still fulfilled. For this, choose $b_i \in B_i$ and apply Schur-Zassenhauss lemma to the short exact sequence

$$1 \to \ker(s) \to s^{-1}(< b_i >) \xrightarrow{s} < b_i > \to 1$$

which splits uniquely up to conjugation, defining thus a single conjugacy class $\tilde{B}_i$ above B_i the elements of which have the same order as those of B_i, $i = 1, ..., n$. Let us show the n-tuple $\tilde{\mathbf{B}} = (\tilde{B}_1, ..., \tilde{B}_n)$ works. For any $1 \leq i \neq j \leq n$ let $b_i \in B_i$, $b_j \in B_j$ such that $b_ib_j = b_jb_i$ so, in particular $< b_i, b_j > \simeq < b_i > \times < b_j >$. Once again Schur-Zassenhauss lemma implies the short exact sequence

$$1 \to \ker(s) \to s^{-1}(< b_i, b_j >) \xrightarrow{s} < b_i, b_j > \to 1$$

splits uniquely up to conjugation and, in particular that, for any section σ of s we have $\sigma(b_i)\sigma(b_j) = \sigma(b_j)\sigma(b_i)$ with $\sigma(b_i) \in \tilde{B}_i$, $\sigma(b_j) \in \tilde{B}_j$. This proves (1) and (2) is straightforward since $n = 1$.

4.3.3 Proof of lemma 4.10

We proceed in two steps :

4.3.3.1 First step

Set

$$\mathcal{B}^i_{1,2s} = \left\{ Q_1^{2\alpha_1+1} Q_2^{2\alpha_2+1} ... Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} ... Q_2^{2\beta_2+1} Q_1^{2\beta_1+1} \right\}_{\substack{\alpha_1,...,\alpha_{i-1}\in\mathbb{Z} \\ \beta_1,...,\beta_{i-1}\in\mathbb{Z} \\ \gamma_i\in\mathbb{Z}-\{0\}}}, \quad i = 1, ..., 2s$$

and $\mathcal{B}_{1,2s} := \bigcup_{i=1}^{2s} \mathcal{B}^i_{1,2s}$. Then $\mathcal{B}_{1,2s}$ is contained in $\Pi_{1,2s}$. Indeed, each of the $\mathcal{B}^i_{1,2s}$, $i = 1, ..., 2s$ is. For $i = 1$, this is obvious. For $2 \leq i \leq 2s$, this results from the following equality : for any $\alpha_1, ..., \alpha_{i-1} \in \mathbb{Z}$, $\beta_1, ..., \beta_{i-1} \in \mathbb{Z}$, $\gamma_i \in \mathbb{Z} - \{0\}$

$$a_{1,2}^{\alpha_2} a_{1,3}^{\alpha_3} ... a_{1,i-1}^{\alpha_{i-1}} a_{1,i}^{\gamma_i} a_{1,i-1}^{\beta_{i-1}+1} ... a_{1,3}^{\beta_3+1} a_{1,2}^{\beta_2+1} = Q_1^{2\alpha_1+1} Q_2^{2\alpha_2+1} ... Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} ... Q_2^{2\beta_2+1} Q_1^{2\beta_1+1}$$

one can check computing "from the center", *i.e.* :

$$\begin{array}{rcl}
a_{1,i}^{\gamma_i} a_{1,i-1}^{\beta_{i-1}+1} & = & Q_1 ... Q_{i-1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+2-1} Q_{i-2}^{-1} ... Q_1^{-1} \\
a_{1,i-1}^{\alpha_{i-1}} (a_{1,i}^{\gamma_i} a_{1,i-1}^{\beta_{i-1}+1}) & = & a_{1,i-1}^{\alpha_{i-1}} Q_1 ... Q_{i-1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} Q_{i-2}^{-1} ... Q_1^{-1} \\
 & = & Q_1 ... Q_{i-2} Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} Q_{i-2}^{-1} ... Q_1^{-1} \\
(a_{1,i-1}^{\alpha_{i-1}} (a_{1,i}^{\gamma_i} a_{1,i-1}^{\beta_{i-1}+1})) a_{1,i-2}^{\beta_{i-2}+1} & = & Q_1 ... Q_{i-2} Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} Q_{i-2}^{-1} ... Q_1^{-1} a_{1,i-2}^{\beta_{i-2}+1} \\
 & = & Q_1 ... Q_{i-2} Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} Q_{i-2}^{2\beta_{i-2}+2-1} Q_{i-3}^{-1} ... Q_1^{-1} \\
etc. & & ...
\end{array}$$

4.3.3.2 Second step

We use now elements of $\mathcal{B}_{1,2s}$ to build u_k, $v_{\underline{i},k}$ et $w_{k,\underline{i}}$.
Set $\alpha_k := Q_{2k-2} Q_{2k-1}^2 Q_{2k-2}$, $k = 2, ..., s$ and note that

$$\alpha_k.(h_1, ..., h_{2k-3}, g, g_k, g_k^{-1}, h_{2k+1}, ..., h_{2s}) = (h_1, ..., h_{2k-3}, g, g_k^g, (g_k^g)^{-1}, h_{2k+1}, ..., h_{2s})$$

(1) Construction of $\mathbf{u_k}$:
Set $\beta_k := Q_{2k-3} ... Q_1$, $k = 2, ..., s$, then, for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$,
- $\beta_2 \cdot \mathbf{g} = (g_1^{-1}, g_1, [g_2, ..., g_s])$.
- $\beta_3 \cdot \mathbf{g} = (g_1^{-1}, g_2^{g_1}, (g_2^{g_1})^{-1}, g_1, [g_3, ..., g_s])$.
- By recurrence, observing that $\beta_{k+1} = Q_{2k-1} Q_{2k-2} \beta_k$, $k \geq 1$, conclude that

$$\beta_k \cdot \mathbf{g} = (g_1^{-1}, [g_2^{g_1}, ..., g_{k-1}^{g_1}], g_1, [g_k, ..., g_s])$$

So, setting $u_k = \beta_k^{-1} \alpha_k \beta_k \in \mathcal{B}_{1,2s}$, one gets :

$$\begin{array}{rcl}
u_k \cdot \mathbf{g} & = & \beta_k^{-1} \cdot (\alpha_k \cdot (g_1^{-1}, [g_2^{g_1}, ..., g_{k-1}^{g_1}], g_1, [g_k, ..., g_s]) \\
 & = & \beta_k^{-1} \cdot (g_1^{-1}, [g_2^{g_1}, ..., g_{k-1}^{g_1}], g_1, [g_k^{g_1}, ..., g_s]) \\
 & = & \beta_k^{-1} \cdot (\beta_k \cdot [g_1, g_2, ..., g_{k-1}, g_k^{g_1}, g_{k+1}, ..., g_{2s}]) \\
 & = & [g_1, g_2, ..., g_{k-1}, g_k^{g_1}, g_{k+1}, ..., g_{2s}]
\end{array}$$

In the following, given $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ and $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$, we will write $\gamma(\underline{i}, j) = g_1^{g_{i_j} \cdots g_{i_1}}$, $j = 1, ..., r$.

(2) Construction of $\mathbf{v_{\underline{i},k}}$:
In this section, given $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ and $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$, we will write $\mathbf{g}_{\underline{i},0} = [g_2^{g_1}, ..., g_{i_1-1}^{g_1}]$ and $\mathbf{g}_{\underline{i},j} = [g_{i_j+1}^{\gamma(\underline{i},j)}, ..., g_{i_{j+1}-1}^{\gamma(\underline{i},j)}]$, $j = 1, ..., r$.
For any $1 \leq i < j \leq s$, write $\gamma_{i<j} := Q_{2j-1}^{-1} Q_{2j-2} \cdots Q_{2i}$, which acts this way :

$$\gamma_{i<j}.(h_1, ..., h_{2i-1}, g, [g_{i+1}, ..., g_j], h_{2j+1}, ..., h_{2s}) = (h_1, ..., h_{2i-1}, [g_{i+1}^g, ..., g_{j-1}^g], g_j^g, g_j^{-1}, g^{g_j}, h_{2j+1}, ..., h_{2s})$$

and for any $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ set $\gamma^{(1)}_{\underline{i}} := \gamma_{i_{r-1}<i_r} \circ \cdots \circ \gamma_{i_1<i_2} \circ \gamma_{1<i_1} \circ Q_1$. Then, for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$:

- For any $1 < i_1 \leq s$, $\gamma^{(1)}_{(i_1)} \cdot \mathbf{g} = \gamma_{1<i_1} \cdot \mathbf{g} = (g_1^{-1}, [g_2^{g_1}, ..., g_{i_1-1}^{g_1}], g_{i_1}^{g_1}, g_{i_1}^{-1}, g_1^{g_{i_1}}, [g_{i_1+1}, ..., g_s])$.

- By recurrence, observing that $\gamma^{(1)}_{(\underline{i},i_{r+1})} = \gamma_{i_r<i_{r+1}} \gamma^{(1)}_{\underline{i}}$, $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r < s$, $i_r < i_{r+1} < s$, $r \geq 1$, conclude that

$$\gamma^{(1)}_{\underline{i}} \cdot \mathbf{g} = (g_1^{-1}, \mathbf{g}_{\underline{i},0}, g_{i_1}^{g_1}, g_{i_1}^{-1}, \mathbf{g}_{\underline{i},1}, ..., g_{i_{r-1}}^{\gamma(\underline{i},r-2)}, g_{i_{r-1}}^{-1}, \mathbf{g}_{\underline{i},r-1}, g_{i_r}^{\gamma(\underline{i},r-1)}, g_{i_r}^{-1}, \gamma(\underline{i}, r), [g_{i_r+1}, ..., g_s])$$

Finally, given $\underline{i} = (i_1, ..., i_r)$, k with $1 < i_1 < ... < i_r < k \leq s$ write $\gamma^{(2)}_{\underline{i},k} := Q_{2k-3}...Q_{2i_r}.\gamma^{(1)}_{\underline{i}}$ and compute

$$\gamma^{(2)}_{\underline{i},k} \cdot \mathbf{g} = (g_1^{-1}, \mathbf{g}_{\underline{i},0}, g_{i_1}^{g_1}, g_{i_1}^{-1}, \mathbf{g}_{\underline{i},1}, ..., \mathbf{g}_{\underline{i},r-1}, g_{i_r}^{\mathbf{g}(\underline{i},r-1)}, g_{i_r}^{-1}, [g_{i_r+1}^{\mathbf{g}(\underline{i},r)}, ..., g_{k-1}^{\mathbf{g}(\underline{i},r)}], \mathbf{g}(\underline{i}, r), [g_k, ..., g_s])$$

So, setting

$$v_{\underline{i},k} = (\gamma^{(2)}_{\underline{i},k})^{-1} \alpha_k \gamma^{(2)}_{\underline{i},k} \in \mathcal{B}_{1,2s}$$

for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$ one gets :

$$\begin{aligned} v_{\underline{i},k} \cdot \mathbf{g} &= (\gamma^{(2)}_{\underline{i},k})^{-1} \gamma^{(2)}_{\underline{i},k} \cdot [g_1, ..., g_{k-1}, g_k^{g_{i_r} \cdots g_{i_1}}, g_{k+1}, ..., g_s] \\ &= [g_1, ..., g_{k-1}, g_k^{g_{i_r} \cdots g_{i_1}}, g_{k+1}, ..., g_s] \end{aligned}$$

(3) Construction of $\mathbf{w_{k,\underline{i}}}$:

In this section, given $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ and $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$, we will write $\mathbf{g}_{\underline{i},0} == [g_2^{\gamma(\underline{i},r)^{-1}}, ..., g_{i_1-1}^{\gamma(\underline{i},r)^{-1}}]$ and $\mathbf{g}_{\underline{i},j} = [g_{i_j+1}^{\gamma(\underline{i},r)^{-1}}, ..., g_{i_{j+1}-1}^{\gamma(\underline{i},r)^{-1}}]$, $j = 1, ..., r$.

For any $2 \leq i < j \leq s$, write $\delta_{i<j} := Q_{2j-3}^{-1} \cdots Q_{2i-1}^{-1} Q_{2i-2}$, which acts this way :

$$\delta_{i<j}.(h_1, ..., h_{2i-3}, g, [g_i, ..., g_{j-1}], h_{2j+1}, ..., h_{2s}) = (h_1, ..., h_{2i-3}, g^g, g_i^{-1}, [g_{i+1}, ..., g_{j-1}]g^{g_i}, h_{2j+1}, ..., h_{2s})$$

and for any $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ set $\delta^{(1)}_{\underline{i}} := \delta_{i_r<i_r+1} \circ \delta_{i_{r-1}<i_r} \circ \cdots \circ \delta_{i_1<i_2} \circ \delta_{1<i_1} \circ Q_1$. Then, for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$:

$$\begin{aligned} \delta^{(1)}_{\underline{i}} \cdot \mathbf{g} &= (g_1^{-1}, [g_2, ..., g_{i_1-1}], g_{i_1}^{g_1}, g_{i_1}^{-1}, [g_{i_1+1}, ..., g_{i_2-1}], ..., g_{i_{r-1}}^{\gamma(\underline{i},r-2)}, g_{i_{r-1}}^{-1}, [g_{i_{r-1}+1}, ..., g_{i_r-1}], \\ &\quad g_{i_r}^{\gamma(\underline{i},r-1)}, g_{i_r}^{-1}, \gamma(\underline{i}, r-1), [g_{i_r+1}, ..., g_s]) \end{aligned}$$

Next, set $\delta^{(2)}_{\underline{i}} := Q_1^{-1} \cdots Q_{2i_r-1}^{-1} \cdot \delta^{(1)}_{\underline{i}} \in \mathcal{B}_{2s}$ and compute

$$\begin{aligned} \delta^{(2)}_{\underline{i}} \cdot \mathbf{g} &= (\gamma(\underline{i}, r), (g_1^{-1})^{\gamma(\underline{i},r)^{-1}}, \mathbf{g}_{\underline{i},0}, (g_{i_1}^{g_1})^{\gamma(\underline{i},r)^{-1}}, (g_{i_1}^{-1})^{\gamma(\underline{i},r)^{-1}}, \mathbf{g}_{\underline{i},1}, ..., (g_{i_{r-1}}^{\gamma(\underline{i},r-2)})^{\gamma(\underline{i},r)^{-1}}, (g_{i_{r-1}}^{-1})^{\gamma(\underline{i},r)^{-1}}, \\ &\quad \mathbf{g}_{\underline{i},r-1}, (g_{i_r}^{\gamma(\underline{i},r-1)})^{\gamma(\underline{i},r)^{-1}}, (g_{i_r}^{-1})^{\gamma(\underline{i},r)^{-1}}, [g_{i_r+1}, ..., g_s]) \end{aligned}$$

Finally, given $\underline{i} = (i_1, ..., i_r)$, k with $1 < k < i_1 < ... < i_r \leq s$ write $\delta^{(3)}_{k,\underline{i}} := e_{\underline{i}} \alpha_{i_r} e_{k,i_r}$ where

$$\begin{cases} e_{\underline{i}} &= Q_1 \cdots Q_{2i_1-3} Q_{2i_1-2}^{-1} Q_{2i_1-1} \cdots Q_{2i_{r-1}-3} Q_{2i_{r-1}-2}^{-1} Q_{2i_{r-1}-1} \cdots Q_{2i_r-3} \\ e_{k,i_r} &= Q_{2i_r-3} \cdots Q_{2k} Q_{2k-1}^{-1} Q_{2k-2}^{-1} Q_{2k-3} \cdots Q_1 \end{cases}$$

then, $\delta^{(3)}_{k,\underline{i}} \in \mathcal{B}_{2s}$, which entails $w^0_{k,\underline{i}} := \delta^{(3)}_{k,\underline{i}} \cdot \delta^{(2)}_{\underline{i}} \in \Pi_{1,2s}$ and for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$ one gets

$$w^0_{k,\underline{i}} \cdot \mathbf{g} = [g_1, ..., g_{k-1}, g_k^{(g_1^{-1})^{g_{i_r} \cdots g_{i_1}}}, g_{k+1}, ..., g_s]$$

As a result, $w_{k,\underline{i}} = (w^0_{k,\underline{i}})^{|<g_1>|-1} \in \Pi_{1,2s}$ works. Note that, this is the only step in the proof of lemma 4.10 where we use the assumption G is finite. Actually, part (1) and (2) of lemma 4.10 remain true without this assumption and part (3) only requires g_1 to be of finite order.

4.4 The regular inverse Galois problem with fixed branch points

4.4.1 General strategy

4.4.1.1 For a finite group

We would like now to apply theorem 4.4 to the regular inverse Galois problem with fixed branch points. Consider a field Q of characteristic 0, a finite group G, a symmetric $2s$-tuple (resp. rational union of conjugacy classes) $\mathbf{C} = [C_1, ..., C_s] \in \mathcal{C}_{2s}(G)$ and suppose that (**C**1) and (**C**2) from theorem 4.4 are satisfied that is, there exists $1 \leq l \leq 2s$ such that all the HM representatives of $\overline{\text{sni}}(\mathbf{C})$ fall in one single orbit $O^{HM}(\mathbf{C}) \in \overline{\text{sni}}(\mathbf{C})/SH_{2s}$ and $\Pi_{l,2s}$ acts transitively on this orbit. Then, $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})$ (resp. $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})$) is a geometrically irreducible variety defined over $Q'_{\mathbf{C}}$ (resp. over Q) such that for any $\mathbf{t}'_{l+1,2s} \in \mathcal{U}^{2s-l+1}(\overline{Q})$, the HM-subvariety $\mathcal{H}'^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{l+1,2s}}$ (resp. the symmetrised HM-subvariety $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{l+1,2s}}$) is a smooth geometrically irreducible variety of dimension l defined over the finite extension $Q'_{\mathbf{C}}(\mathbf{t}'_{l+1,2s})/Q$ (resp. the finite extension $Q(\mathbf{C}, \mathbf{t}'_{l+1,2s})/Q$). So the problem is reduced to studying the rational points of a smooth modular geometrically irreducible variety V of dimension l defined over a finite extension k_0/Q.

This situation is particularly adapted to the *Local-global principle* [Mo89], [GPR97] that is : considering a global field k_0 and a nonempty finite set of places Σ and denoting by k_0^{Σ}/k_0 the maximal extension of k_0 in a separable closure k_0^s/k_0 which is totally split at each $v \in \Sigma$, the local-global principle for varieties states that, for any smooth geometrically irreducible k_0^{Σ}-variety V, if $V(k_{0v}) \neq \emptyset$ for each embedding $k_0^{\Sigma} \hookrightarrow k_{0v}$ and each $v \in \Sigma$ then $V(k_0^{\Sigma}) \neq \emptyset$. This applies in particular to $k_0 = \mathbb{Q}$ and $\Sigma = \{p\}$, where p is a prime number (resp. ∞) that is, $k_{0p} = \mathbb{Q}_p$, $k_0^{\Sigma} = \mathbb{Q}^{tp}$ (resp. $k_{0\infty} = \mathbb{R}$, $k_0^{\Sigma} = \mathbb{Q}^{tr}$).

So, using the modular interpretation of Hurwitz spaces we can state, for instance :

Proposition 4.13 *Fix a finite group G, a symmetric $2s$-tuple $\mathbf{C} = [C_1, ..., C_s] \in \mathcal{C}_{2s}(G)$ and an integer $1 \leq l \leq 2s$. Let k_0 be a global field and Σ a nonempty finite set of places. Assume*

(Trans) *All the HM representatives fall in one single orbit $O^{HM}(\mathbf{C}) \in \overline{\text{sni}}(\mathbf{C})/SH_{2s}$ and $\Pi_{l,2s}$ acts transitively on this orbit.*

(LocReal) *There exists a tuple $\mathbf{t}'_{\Sigma,l+1,2s} \in \mathcal{U}^{2s-l}(\overline{k}_0)$ such that $Q(\mathbf{C}, \mathbf{t}'_{\Sigma,l+1,2s}) \subset k_0$ and, for each $v \in \Sigma$, there exists a HM G-cover f defined over k_{0v} with invariants G, $\mathbf{C}$ $(\mathbf{t}'_f, \mathbf{t}'_{\Sigma})$ (where $\mathbf{t}_f \in \mathcal{U}_l(k_{0v})$ depends on f).*

Then there exists a HM G-cover f defined over k_0^{Σ} with invariants $G, \mathbf{C}$ and branch points $(\mathbf{t}'_f, \mathbf{t}'_{\Sigma,l+1,2s})$ (where $\mathbf{t}_f \in \mathcal{U}_l(k_0^{\Sigma})$ depends on f).

Proof. In terms of Hurwitz spaces, condition **(Trans)** implies that $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})$ is a geometrically irreducible variety defined over k_0 and that for any $\mathbf{t}'_{l+1,2s} \in \mathcal{U}^{2s-l}(\overline{k}_0)$, $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{l+1,2s}}$ remains geometrically irreducible. Furthermore, according to condition **(LocReal)**, there exists $\mathbf{t}'_{\Sigma,l+1,2s} \in \mathcal{U}^{2s-l}(\overline{k}_0)$ such that $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}(k_{0v})^{noob} \neq \emptyset$, $v \in \Sigma$ with $Q(\mathbf{C}, \mathbf{t}'_{\Sigma,l+1,2s}) \subset k_0$. So, since $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}$ is smooth, geometrically irreducible and defined over k_0, the local-global principle entails that $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}(k_0^{\Sigma})^{noob} \neq \emptyset$, which is the expected conclusion when, for instance, $Z(G) = \{1\}$. Else, the local-global principle should be applied to the global descent variety $D_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}$ [DDoMo04] associated with $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}$ instead of $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}$ itself. Indeed, one has $D_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}(k_{0,v}) \neq \emptyset$, $v \in \Sigma$. Since $D_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}$ is smooth geometrically irreducible and defined over k_0, the local-global principle yields $D_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}(k_0^{\Sigma}) \neq \emptyset$ or, equivalently, $\mathcal{H}^{HM}_{2s,G}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}(k_0^{\Sigma})^{noob} \neq \emptyset$. □

Remark 4.14 Existentially closed extension analog Recall a field k_0 is said to be existentially closed in a regular extension k/k_0 if for any smooth geometrically irreducible k_0-variety V, $V(k) \neq \emptyset$ entails $V(k_0) \neq \emptyset$. For instance

a large field k_0 is existentially closed in $k_0((X))/k_0$ [P96]. Thus, an analog of proposition 4.13 can be stated for this situation, more precisely :*Let k_0 be a field existentially closed in a regular extension k/k_0. Fix a finite group G, a symmetric $2s$-tuple $\mathbf{C} = [C_1, ..., C_s] \in \mathcal{C}_{2s}(G)$ and an integer $1 \leq l \leq 2s$. Assume* **(Trans)** *and*

(LocReal) *There exists a HM G-cover defined over k with invariants G, $\mathbf{C}$ and branch points $\mathbf{t}' \in \mathcal{U}^{2s}(\overline{k}_0)$ such that $Q(\mathbf{C}, \mathbf{t}'_{l+1,2s}) \subset k_0$.*

Then there exists a HM G-cover f defined over k_0 with invariants $G, \mathbf{C}$ and branch points $(\mathbf{t}'_f, \mathbf{t}'_{l+1,2s})$ (where $\mathbf{t}_f \in \mathcal{U}_l(k_0)$ depends on f).

4.4.1.2 For a projective system of finite groups

The above strategy can also be developped for a complete projective system of finite groups $(s_{k+1} : G_{k+1} \twoheadrightarrow G_k)_{k\geq 0}$. Indeed, assume there exists a projective system $(\mathbf{C}_k = [C_{k,1}, ..., C_{k,s}])_{k\geq 0}$ of symmetric tuples (resp. rational union of conjugacy classes) $\mathbf{C}_k \in \mathcal{C}_{2s_k}(G_k)$ and an integer $1 \leq l \leq 2s_0$ such that (**C1**) and (**C2**) from theorem 4.4 are satisfied at each level $k \geq 0$. Then $(\mathcal{H}'^{HM}_{2s_{k+1},G_{k+1}}(\mathbf{C}_{k+1}) \to \mathcal{H}'^{HM}_{2s_k,G_k}(\mathbf{C}_k))_{k\geq 0}$ (resp. $(\mathcal{H}^{HM}_{2s_{k+1},G_{k+1}}(\mathbf{C}_{k+1}) \to \mathcal{H}^{HM}_{2s_k,G_k}(\mathbf{C}_k))_{k\geq 0}$) is a tower of geometrically irreducible varieties defined over $\cup_{k\geq 0} Q'_{\mathbf{C_k}}$ (resp. over Q) such that for any projective system of branch points $(\mathbf{t}'_k)_{k\geq 0} \in \varprojlim_{k\geq 0} \mathcal{U}^{2s_k-l}(\overline{Q})$ the corresponding tower $(\mathcal{H}'^{HM}_{2s_{k+1},G_{k+1}}(\mathbf{C}_{k+1})_{\mathbf{t}'_{k+1}} \to \mathcal{H}'^{HM}_{2s_k,G_k}(\mathbf{C}_k)_{\mathbf{t}'_k})_{k\geq 0}$ (resp. symmetrised tower $(\mathcal{H}^{HM}_{2s_{k+1},G_{k+1}}(\mathbf{C}_{k+1})_{\mathbf{t}'_{k+1}} \to \mathcal{H}^{HM}_{2s_k,G_k}(\mathbf{C}_k)_{\mathbf{t}'_k})_{k\geq 0}$) is a tower of geometrically irreducible l-dimensional varieties defined over $\cup_{k\geq 0} Q'_{\mathbf{C_k}}(\mathbf{t}'_k)$ (resp. $\cup_{k\geq 0} Q(\mathbf{C_k}, \mathbf{t}'_k)$). Theorem 4.1 of [DE03] states that, given a complete projective system of finite groups $(s_{k+1} : G_{k+1} \twoheadrightarrow G_k)_{k\geq 0}$, $(\mathbf{C}_k)_{k\geq 0}$ can always be built in such a way that (**C1**) is fulfilled for any $k \geq 0$ and that, for any henselian field λ of characteristic 0 with residue characteristic either $p = 0$ or $p > 0$ not dividing any of the $|G_k|$, $k \geq 0$ and containing all the prime-to-p roots of 1, $\varprojlim_{k\geq 0} \mathcal{H}^{HM}_{2s_k,G_k}(\mathbf{C}_k)(\lambda)^{noob} \neq \emptyset$. We would like to obtain the same kind of results replacing the towers of HM-components by towers of HM-subvarieties in order to apply the following profinite version of proposition 4.13.

Proposition 4.15 *Let k_0 be a global field and Σ a nonempty finite set of places. Fix a complete projective system of finite groups $(s_{k+1} : G_{k+1} \twoheadrightarrow G_k)_{k\geq 0}$, a projective system of symmetric tuples $(\mathbf{C}_k = [C_{k,1}, ..., C_{k,s}])_{k\geq 0}$ and an integer $1 \leq l \leq 2s_0$. Assume*

(Trans) *All the HM-representatives fall in one single orbit $O^{HM}(\mathbf{C}_k) \in \overline{\text{sni}}(\mathbf{C}_k)/SH_{2s_k}$ and $\Pi_{l,2s_k}$ acts transitively on this orbit, $k \geq 0$.*

(LocReal) *For all $k \geq 0$, there exists $\mathbf{t}'_{\Sigma,l+1,2s_k} \in \mathcal{U}^{2s_k-l}(\overline{k}_0)$ such that $Q(\mathbf{C}, \mathbf{t}'_{\Sigma,l+1,2s_k}) \subset k_0$ and for each $v \in \Sigma$, there exists a HM G-cover f_k defined over k_{0v} with invariants G_k, $\mathbf{C}_k$, $(\mathbf{t}'_{f_k}, \mathbf{t}'_{\Sigma,l+1,2s_k})$ (where $\mathbf{t}_k \in \mathcal{U}_l(k_{0v})$ depends on f_k).*

Then for each $k \geq 0$ there exists a HM G-cover f defined over k_0^Σ with invariants G_k, $\mathbf{C}_k$ and branch points $(\mathbf{t}'_{f_k}, \mathbf{t}'_{\Sigma,l+1,2s_k})$ (where $\mathbf{t}_{f_k} \in \mathcal{U}_l(k_0^\Sigma)$ depends on f_k).

We will deal with modular towers [F95a] and some towers of Hurwitz spaces associated with modular towers we call associated central towers. The end of this section is devoted to describing the construction of these objects which are the main motivation for proposition 4.8 and example **??**.

a/ <u>Modular towers</u> : Fix a finite group G and a prime number p dividing $|G|$. Consider then the universal p-Frattini cover of G, ${}_p\tilde{\phi} :_p \tilde{G} \to G$. Since $\ker({}_p\tilde{\phi})$ is a free pro-p group, its Frattini series, defined inductively by $\ker_0 = \ker({}_p\tilde{\phi})$, $\ker_1 = \ker_0^p[\ker_0, \ker_0], ...,$ $\ker_i = \ker_{i-1}^p[\ker_n, \ker_n], ...,$ is a fundamental system of neighbourhoods of 1. This provides a complete projective system of finite groups $(s_{k+1} :_p^{k+1} \tilde{G} \twoheadrightarrow_p^k \tilde{G})_{k\geq 0}$ with ${}_p^k\tilde{G} :=_p \tilde{G}/\ker_k$, $k \geq 0$ such that ${}_p\tilde{G} = \varprojlim_{k\geq 0} {}_p^k\tilde{G}$. Furthermore, for any $k \geq 0$ and any p'-conjugacy class C_k of ${}_p^k\tilde{G}$, there exists a unique conjugacy class C_{k+1} of ${}_p^{k+1}\tilde{G}$ above C_k with $o(C_{k+1}) = o(C_k)$ [F95a], lemma 3.7. As a result, if G is p-perfect, any tuple

of p'-conjugacy classes $\mathbf{C}_0 = (C_{0,1}, ..., C_{0,r}) \in \mathcal{C}_r(G)$ with $\overline{\mathrm{hm}}([\mathbf{C}_0]) \neq \emptyset$ defines a unique projective system $(\mathbf{C}_k = (C_{k,1}, ..., C_{k,r}))_{k\geq 0}$ such that for all $k \geq 0$, $o(C_{k,i}) = o(C_{k,0})$, $i = 1, ..., r$, $\overline{\mathrm{hm}}([\mathbf{C}_k]) \neq \emptyset$ (Frattini property) and $\mathbf{C}_k$ has the same rationality properties as $\mathbf{C}_0$[3]. The corresponding projective system of HM-varieties

$$(\mathcal{H}'^{HM}_{2r,p^{k+1}\tilde{G}}([\mathbf{C}_{k+1}]) \to \mathcal{H}'^{HM}_{2r,p^k\tilde{G}}([\mathbf{C}_k])_{k\geq 0}$$

is called the HM-modular tower associated with the data $(G, [\mathbf{C}_0], p)$. As usual, $(\mathcal{H}^{HM}_{2r,p^{k+1}\tilde{G}}([\mathbf{C}_{k+1}]) \to \mathcal{H}^{HM}_{2r,p^k\tilde{G}}([\mathbf{C}_k])_{k\geq 0}$ will be called the symmetrised HM-modular tower associated with the data $(G, [\mathbf{C}_0], p)$.

b/ <u>Associated central towers</u> : We keep the above notation, assuming furthermore that G is q-perfect for some prime $q \neq p$ dividing $|G|$. Denote by $\widehat{\ }^q$ the functor "universal q-central extension" and consider the projective system $(\widehat{\ }^q s_{i+1} : \widehat{{}^q(p^{k+1}\tilde{G})} \twoheadrightarrow \widehat{{}^q(p^k\tilde{G})})_{k\geq 0}$. For each $k \geq 0$ let $\mathcal{A}_k$ be the set of all symmetric $2r$-tuples of conjugacy classes of $\widehat{{}^q(p^k\tilde{G})}$ above $[\mathbf{C}_k]$. Then $(\widehat{\ }^q s_{k+1} : \mathcal{A}_{k+1} \to \mathcal{A}_k)_{k\geq 0}$ is a projective system of non empty finite sets, so its projective limit is non empty. In other words, there exists a projective system $(\widehat{{}^q[\mathbf{C}_k]})_{k\geq 0}$ of symmetric g-complete $2r$-tuples of conjugacy classes above $([\mathbf{C}_k])_{k\geq 0}$. Such a system defines a tower of Hurwitz spaces covering the HM-modular tower associated with the data $(G, [\mathbf{C}], p)$ we call an associated q-central tower. It cannot be defined uniquely in general except if $C_{0,1}, ..., C_{0,r}$ (and thus, $C_{k,1}, ..., C_{k,r}$, $k \geq 0$) are also q'-conjugacy classes, in which case, by Schur-Zassenhauss, the associated q-central tower can be defined uniquely with, furthermore, the property that $\widehat{{}^q[\mathbf{C}_k]})$ has the same rationality property as $[\mathbf{C}_k]$, $k \geq 0$ and, consequently that the associated q-central tower is defined over the same field as the original modular tower. In general, if the original modular tower is defined over $k \subset \overline{\mathbb{Q}}$, an associated q-central tower is defined over a subfield of $k(\mathrm{e}^{\frac{2\pi i}{e(M(G))_q}})$ where $e(M(G))_q$ denotes the q-part of the exponent of the Schur multiplier $M(G)$ of G. Indeed, one has $e(M(p^k\tilde{G})|\ e(p^k\tilde{G})$ with $e(p^k\tilde{G}) = p^{r_k}e(G)$ thus $e(M(p^k\tilde{G}))_q = e(M(G))_q$.

If G is perfect, one can carry out the same construction with the functor "universal central extension", $\widehat{\ }$, but the resulting associated central towers are not necessarily defined over a finite extension of k since $\{e(M(p^k\tilde{G}))\}_{k\geq 0}$ is not necessarily bounded.

Theorem 4.4 and proposition 4.4 give group-theoretical conditions to ensure the transitivity condition **(Trans)** holds. Sections 4.4.2 and 4.4.3 are devoted to prove the local realization condition **LocReal** for fields like $\mathbb{R}$, $\mathbb{Q}_p$. As a result we can give explicit forms of propositions 4.13 and 4.15 : theorems 4.18 and 4.19. Theorems 1 and 2 from the introduction are special cases of these results.

4.4.2 (RIGP/$\mathbf{t}_2 \subset \mathbf{t}$) over $\mathbb{Q}^\Sigma$

4.4.2.1 G-covers over a complete field of characteristic 0

We start with a preliminary paragraph about the regular realization of finite groups over complete fields satisfying some additional technical conditions that we will need for our construction.

Let k be a complete discrete valued field of characteristic 0 and of residue characteristic p. The main tools to deal with G-covers over k are formal geometry [H87] or rigid geometry [L95], [P94]. Given a symmetric $2s$-tuple $\mathbf{C} = [C_1, , ..., C_s] \in \mathcal{C}_{2s}(G)$, these methods provide a construction of G-covers defined over $\mathbb{Q}_p$ with invariants G, $\mathbf{C}$, $\mathbf{t} \in \mathcal{U}_{2s}(\mathbb{Q})$. However, it is not obvious these G-covers are HM G-covers - and, in general, they are not. For a prime p not dividing $|G|$, some technical assumptions on the branch points - conditions (*) and (**) below - are necessary to ensure they are [DE03] and for primes p dividing $|G|$, the problem remains open (because of the possible bad reduction of Hurwitz

[3]Indeed, for any $k \geq 1$, $[{}^k_p\tilde{G} : G] = p^{r_k}$ so, for any $q \geq 1$, q is prime to $|{}^k_p\tilde{G}|$ if and only if q is prime to $|G|$. As a result, for any $q \geq 1$ prime to $|{}^k_p\tilde{G}|$ and for any $1 \leq j \leq r$, $C^q_{k,j}$ is the only conjugacy class above C^q_j with elements of the same order as those of C^q_j. In particular, for any $q \geq 1$ prime to $|G|$, if $\sigma_q \in \mathcal{S}_r$ verifies $\mathbf{C}^q = (C_{\sigma_q(1)}, ..., C_{\sigma_q(r)})$ then $\mathbf{C}^q_k = (C_{k,\sigma_q(1)}, ..., C_{k,\sigma_q(s)})$.

spaces for these primes). Suppose given $\mathbf{t} = \{x_1, y_1, ..., x_s, y_s\} \in \mathcal{U}_{2s}(k)$ and consider the conditions

(*) x_i, y_i lie in the same coset, $i = 1, ..., s$ and $x_1, ..., x_s$ lie in pairwise distinct cosets.

(**) $|x_i - y_i| < |x_i - x_j||p|^{\frac{1}{p-1}}$, $1 \leq i \neq j \leq s$ (with the convention $|p|^{\frac{1}{p-1}} = 1$ if $p = 0$).

where $a, b \in k$ lie in the same coset means that either $|a|, |b| \leq 1$ and $|a - b| < 1$ or $|a|, |b| > 1$. We will sometimes write $\zeta_n := \mathrm{e}^{\frac{2\pi i}{n}}$, $n \geq 2$ in the following.

Remark 4.16 Comment about condition (*) The set $E_t = \{(x_1, ..., x_t) \in \mathcal{U}^t(\mathbb{Q}) \mid x_i,\ x_j$ lie in distinct cosets, $1 \leq i \neq j \leq t\}$ is empty for $t > p + 1$.

Indeed, let $(x_1, ..., x_t) \in E_t$ and assume for instance that $|x_1| > 1$ then $|x_i| \leq 1$, $i = 2, ..., t$. Write $x_i := x_2 + \frac{a_i}{b_i}$ with $a_i \in \mathbb{Z} \setminus \{0\}$, $b_i \in \mathbb{N} \setminus \{0\}$, $(a_i, b_i) = 1$, $i = 3, ..., t$. Then

- $|x_i - x_2| = 1$ implies that $p \not| a_i,\ b_i$, $i = 3, ..., t$.
- $|x_i - x_j = \frac{b_j a_i - b_i a_j}{b_i b_j}| = 1$ implies that $p \not| b_j a_i - b_i a_j$, $3 \leq i \neq j \leq t$.

In other words, writing $\overline{a}$ for the reduction of $a \in \mathbb{Z}$ modulo p, $(\overline{a}_i, \overline{b}_i), (\overline{a}_j, \overline{b}_j)$ is a basis of $\mathbb{F}_p^2$, $3 \leq i \neq j \leq t$ with $\overline{a}_i, \overline{b}_i \neq 0$, $i = 3, ..., t$. But for any $n \geq 1$, if $(v_1, ..., v_n) \in \mathbb{F}_p^2$ is a tuple of vectors with non-zero coordinates such that (v_i, v_j) is a basis of $\mathbb{F}_p^2$, $1 \leq i \neq j \leq n$, there are only $p^2 - (2(p-1) + n(p-1)) = (p-1)^2 - n(p-1)$ vectors v_{n+1} with non-zero coordinates such that (v_i, v_{n+1}) is a basis of $\mathbb{F}_p^2$, $i = 1, ..., n$. Conclude that, necessarily, $n \geq p - 1$.

Remark 4.16 underlines how careful we are to be when constructing HM-G-covers defined over $\mathbb{Q}_p$ with branch points in a given number field; for instance, we can't assert there are HM-G-covers defined over $\mathbb{Q}_p$ with $p + 3$ rational branch points. Lemma 4.17 gives a procedure to solve this problem.

Since the statement and proof of lemma 4.17 are rather technical, we first explain how we are going to proceed. As usual, the method consists in glueing cyclic G-covers in an appropriate way. But here, we want to build HM G-cover defined over k and with a rational branch points divisor so the cyclic G-covers we are to consider must be, in particular, (1) defined over $\mathbb{Q}$ with a $\mathbb{Q}$-rational unramified point the fiber of which is totally $\mathbb{Q}$-rational and (2) HM.

Classicaly, a cyclic G-cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ verifying condition (1) is a G-cover with group $< g >:= \mathbb{Z}/n\mathbb{Z}$, inertia canonical invariant $(\{g^{\epsilon u_i}\})_{i=1,...,\phi(n)/2,\ \epsilon=\pm 1}$ and associated branch points $(\zeta_n^{\epsilon u_i})_{i=1,...,\phi(n)/2,\ \epsilon=\pm 1}$ (where $(\mathbb{Z}/n\mathbb{Z})^\star = \{\pm u_i\}_{i=1,...,\phi(n)/2}$) [Des95]. But such a G-cover does not verify condition (2) ($|\zeta_n^{\epsilon_i u_i} - \zeta_n^{\epsilon_j u_j}| = 1$ when $(\epsilon_i, i) \neq (\epsilon_j, j)$). So we consider instead the cyclic G-cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ with group $< g >:= \mathbb{Z}/n\mathbb{Z}$, inertia canonical invariant $(\{g^{\epsilon u_i}\}, \{g^{-\epsilon u_i}\})_{i=1,...,\phi(n)/2,\ \epsilon=\pm 1}$ and associated branch points $(x_i^\epsilon := \zeta_n^{\epsilon u_i}, y_i^\epsilon := a + \zeta_n^{-\epsilon u_i})_{i=1,...,\phi(n)/2,\ \epsilon=\pm 1}$ where $a \in \mathbb{Q}$ is chosen in such a way that $|a| < \min\{1, |p|^{\frac{1}{p-1}}\}$. This still verifies both conditions (1) and (2) ($|x_i^\epsilon - y_i^\epsilon| = |a| < 1$, $|x_i^\epsilon - x_i^{-\epsilon}| = |\zeta_n^{\epsilon u_i} - \zeta_n^{-\epsilon u_i}| = 1$ and $|x_i^\epsilon - x_j^{\pm 1}| = |\zeta_n^{\epsilon u_i} - \zeta_n^{\pm u_j}| = 1$, $1 \leq i \neq j \leq \phi(n)/2$).

In order to obtain a HM-G-covers when glueing together two cyclic HM-G-covers $f_i : X_i \to \mathbb{P}^1_{\mathbb{Q}}$ (with invariants $< g_i >:= \mathbb{Z}/n_i\mathbb{Z}$, $(\{g_i^{\epsilon u_{i,j}}\}, \{g^{-\epsilon u_{i,j}}\})_{j=1,...,\phi(n_i)/2,\ \epsilon=\pm 1}$, $(x_{i,j}^\epsilon := a_i + \zeta_{n_i}^{\epsilon u_{i,j}}, y_{i,j}^\epsilon := a_i + a + \zeta_{n_i}^{-\epsilon u_{i,j}})_{j=1,...,\phi(n_i)/2,\ \epsilon=\pm 1}$), $i = 1, 2$ as in the preceding paragraph, we have to check $(x_{i,j}^\epsilon, y_{i,j}^\epsilon)_{\substack{j=1,...,\phi(n_i)/2,\ \epsilon=\pm 1 \\ i=1,2}}$ verify conditions (*) and (**) as well. This will occur for instance if $n_1 \neq n_2$ and $|a_1|, |a_2|, |a_1 - a_2| < 1$ (where $a_1, a_2 \in \mathbb{Q}$ are just translation terms). If $n_1 = n_2$, one can still enlarge the inertia canonical invariants replacing n_i by $n_i^{m_i}$ so that $n_1^{m_1} \neq n_2^{m_2}$. Consequently, given any integer $m \geq 1$, we will denote by Rat_m the *rationalization operator* which to each conjugacy class C of a finite group G associated the rational union of conjugacy classes

$$\mathrm{Rat}_m(C) := (C^{\epsilon u_i}, C^{-\epsilon u_i})_{i=1,...,\phi(o(C)^m)/2,\ \epsilon=\pm 1}$$

where $\{\pm u_i\}_{1 \leq i \leq \phi(o(C)^m)/2} = (\mathbb{Z}/o(C)^m\mathbb{Z})^\star$. Likewise, given any tuple $\underline{m} = (m_1, ..., m_t) \in \mathbb{N} \setminus \{0\}$, let $\mathrm{Rat}_{\underline{m}}$ be the rationalization operator which to any tuple $\mathbf{C} = (C_1, ..., C_t) \in \mathcal{C}_t(G)$ associates the tuple

$$\mathrm{Rat}_{\underline{m}}(\mathbf{C}) := (\mathrm{Rat}_{m_1}(C_1), ..., \mathrm{Rat}_{m_t}(C_t)).$$

We now state lemma 4.17 and its proof, which is just a slight adjustement of the method described above (we only give the proof of assertion (1), leaving the ones of assertions (2-1) and (2-2) to the reader as an easy exercise).

Lemma 4.17 *Let G be a finite group and $\mathbf{C} = (C_1, ..., C_t) \in \mathcal{C}_t(G)$. Assume that $p \not| |G|$, k contains all the $o(C_1)$th roots of 1.*

(1) If $t_0 \leq p$ then choose $\underline{m} = (m_{t_0+1}, ..., m_t) \in \mathbb{N} \setminus \{0\}$ such that $o(C_i)^{m_i} \neq o(C_j)^{m_j}$, $t_0 + 1 \leq i \neq j \leq t$ and write $r := l(\mathrm{Rat}_{\underline{m}}(C_{t_0+1}, ..., C_t))$. Then there exists a branch point tuple $\mathbf{t}' \in \mathcal{U}^{r+2t_0}(\mathbb{Q})$ verifying (*), (**), $\mathbf{t}'_{1,2t_0} \in \mathcal{U}^{2t_0}(\mathbb{Q})$ and $\mathbf{t}'_{2t_0+1,r+2t_0} \in \mathcal{U}_r(\mathbb{Q})$. And, for any such branch point tuple, there exist HM G-covers defined over k with invariants G, $([C_1, ..., C_{t_0}], \mathrm{Rat}_{\underline{m}}(C_{t_0+1}, ..., C_t))$, $\mathbf{t}'$.

(2) Else, choose $\underline{m} := (m_1, ..., m_t) \in \mathbb{N} \setminus \{0\}$ such that $o(C_i)^{m_i} \neq o(C_j)^{m_j}$, $1 \leq i \neq j \leq t$ and write :

(2-1) $r_{t_0+1,t} := l(\mathrm{Rat}_{(m_{t_0+1},...,m_t)}(C_{t_0+1}, ..., C_t))$. Then there exists a branch point tuple $\mathbf{t}' \in \mathcal{U}^{r+2t_0}(\mathbb{Q})$ verifying (*), (**), $\mathbf{t}'_{1,2t_0} \in \mathcal{U}^{2t_0}(\mathbb{Q}(\zeta_{N_{\underline{m},t_0}}))$ (where $N_{\underline{m},t_0} := \mathrm{lcm}\{o(C_1)^{m_1}, ..., o(C_{t_0})^{m_{t_0}}\}$) and $\mathbf{t}'_{2t_0+1,r+2t_0} \in \mathcal{U}_r(\mathbb{Q})$. And, for any such branch point tuple, there exist HM G-covers defined over k with invariants G, $([C_1, ..., C_{t_0}], \mathrm{Rat}_{\underline{m}}(C_{t_0+1}, ..., C_t))$, $\mathbf{t}'$.

(2-2) $r_{1,t_0} := l(\mathrm{Rat}_{(m_1,...,m_{t_0})}(C_1, ..., C_{t_0}))$, $r_{t_0+1,t} := l(\mathrm{Rat}_{(m_{t_0+1},...,m_t)}(C_{t_0+1}, ..., C_t))$ and $r := r_{1,t_0} + r_{t_0+1,t}$. Then there exists a branch point tuple $\mathbf{t}' \in \mathcal{U}^r(\mathbb{Q})$ verifying (*), (**), $\mathbf{t}_{1,r_{1,t_0}} \in \mathcal{U}_{r_{1,t_0}}(\mathbb{Q})$ and $\mathbf{t}'_{r_{1,t_0}+1,r} \in \mathcal{U}_{r_{t_0+1,t}}(\mathbb{Q})$. And, for any such branch point tuple, there exist HM G-covers defined over k with invariants G, $\mathrm{Rat}_{\underline{m}}(\mathbf{C})$, $\mathbf{t}'$.

Proof (of assertion (1)) Write $o_i := o(C_i)$ and choose $g_i \in C_i$, $i = 1, ..., t$. Then for each $1_l eqi \leq t_0$ and for any $a_i, b_i \in \mathbb{Q}$, the G-cover $f_i : X_i \to \mathbb{P}^1_{\mathbb{Q}}$ with group $< g_i >$, inertia canonical invariant $(\{g_1\}, \{g_i^{-1}\})$ and associated branch points $(x_i := a_i, y_i := b_i)$ is defined over $\mathbb{Q}(\zeta_{o_i})$ and has a $\mathbb{Q}(\zeta_{o_i})$-rational unramified point the fiber of which is totally $\mathbb{Q}(\zeta_{o_i})$-rational. Likewise, for each $t_0 + 1 \leq i \leq t$, write

$$\mathrm{Rat}_{m_i}(C_i) = ((C_i^{u_{i,j}}, C_i^{-u_{i,j}})_{\epsilon=\pm 1})_{j=1,...,\phi(o_i^{m_i})/2})$$

Then, for any $a_i, b_i \in \mathbb{Q}$, any G-cover $f_i : X_i \to \mathbb{P}^1_{\mathbb{Q}}$ with group $< g_i >$, inertia canonical invariant $(\{g_i^{u_{i,j}}\}, \{g_i^{-u_{i,j}}\})_{\epsilon=\pm 1})_{1 \leq j \leq \phi(o_i^{m_i})/2}$ and associated branch points $((x^{\epsilon}_{i,j} = a_i + \zeta^{\epsilon u_{i,j}}_{o_i^{m_i}}, y^{\epsilon}_{i,j} = b_i + \zeta^{-\epsilon u_{i,j}}_{o_i^{m_i}})_{\epsilon=\pm 1})_{1 \leq j \leq \phi(o_i^{m_i})/2}$ is defined over $\mathbb{Q}$ and has a $\mathbb{Q}$-rational unramified point the fiber of which is totally $\mathbb{Q}$-rational. Choose futhermore $(a_i)_{1 \leq i \leq t} \in \mathbb{Q}^t$ in such a way that

$$\begin{array}{ll} |a_i| < 1 & ,i = 1, ..., t \\ |a_i - a_j| = 1 & , 1 \leq i \neq j \leq t_0 \\ |a_i - a_j| < 1 & , 1 \leq i \leq t, \, t_0 + 1 \leq j \leq t \end{array}$$

and, given $a \in \mathbb{Q}$ such that $|a| < \min\{1, |p|^{\frac{1}{p-1}}\}$ set $b_i := a_i + a$, $i = 1, ..., t$. With $N := \prod_{2 \leq i \leq t} o_i^{m_i}$, by assumption $p \not| N$. Thus, $X^N - 1$ remains separable over the residue field of k and, as a result, $|\zeta_{o_i^{m_i}}| = 1$, $i = t_0 + 1, ..., t$ and $|\zeta^{\pm u(i,j)}_{o_i^{m_i}} - \zeta^{\pm u(k,l)}_{o_k^{m_k}}| = 1$, $(i,j) \neq (k,l)$. From this one easily check condition (*) and (**) are both fulfilled by $\mathbf{t}' := ((x_i, y_i)_{1 \leq i \leq t_0}, ((x^{\epsilon}_{i,j}, y^{\epsilon}_{i,j})_{j=1,...,\phi(o_i^{m_i})/2})_{t_0+1 \leq i \leq t, \, \epsilon=\pm 1})$. Condition (**) allows us to glue together - via rigid geometry - the G-covers $(f_i \times_{\mathbb{Q}(\zeta_{o_i})} k)_{1 \leq i \leq t_0}$ and $(f_i \times_{\mathbb{Q}} k)_{t_0+1 \leq i \leq t}$ to get a G-cover $f : X \to \mathbb{P}^1_k$ defined over k with group G, inertia canonical invariant $([C_1, ..., C_{t_0}], \mathrm{Rat}_{\underline{m}}(C_{t_0+1}, ..., C_t))$ and branch points $\mathbf{t}'$. Condition (*) combined with [DE03], proposition 2.3 and theorem 1.4 shows that the G-cover $f : X \to \mathbb{P}^1_k$ is actually a HM-cover.□

4.4.2.2 Results

To avoid rationality problems, we only deal, in this section, with fields containing enough roots of 1. We explain succintly in the next paragraph how to adapt the statements and proofs to fields without roots of 1.

Theorem 4.18 *Let G be a finite group containing two tuples $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$, $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$ verifying* (**H**1) *and* (**H**2) *from theorem 4.4. Set $k_{\mathbf{A}} := \mathbb{Q}(\zeta_{o(A_1)}, ..., \zeta_{o(A_m)})$ and write*

$$\mathbf{C}_s := ([\mathbf{A}], \mathrm{Rat}_{\underline{m}}(\mathbf{B}^s)) \quad r_s := l(\mathbf{C}_s)$$

where $\underline{m} = (m_1, ..., m_{ns}) \in \mathbb{N} \setminus \{0\}^{ns}$ is any tuple such that $o(B_i)^{m_{i+kn}} \neq o(B_j)^{m_{j+ln}}$, $(i,k) \neq (j,l)$, $1 \leq i, j \leq n$, $0 \leq k, l \leq s-1$. Then, for s large enough, $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)$ is a geometrically irreducible variety and, for any $\mathbf{t}' \in \mathcal{U}^{r_s-(2m-1)}(\overline{\mathbb{Q}})$ the $(2m-1)$-dimensional HM-subvariety $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'}$ remains geometrically irreducible. Furthermore, for any finite set Σ of (non archimedean) places of k_A of residue characteristic not dividing $|G|$,

(1) If there exists $a_1, ..., a_m \in \mathbb{Q}$ such that $|a_i - a_j|_p = 1$, $1 \leq i \neq j \leq m$ for any residue characteristic p of $P \in \Sigma$ then there exists $\mathbf{t}'_\Sigma \in \mathcal{U}^{r_s-(2m-1))}(\overline{\mathbb{Q}})$ with $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-(2m-1)}(\mathbb{Q})$ and such that the corresponding $(2m-1)$-dimensional symmetrised HM-subvariety $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}$ is defined over $k_{\mathbf{A}}$ with the property that

$$\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}(k_A^\Sigma)^{noob} \neq \emptyset.$$

(2) Else, choose furthermore $\underline{m}^0 :== (m_1^0, ..., m_m^0) \in \mathbb{N}^m$ such that $o(A_i)^{m_i^0} \neq o(A_j^{m_j^0})$, $1 \leq i \neq j \leq m$ and $o(A_i)^{m_i^0} \neq o(B_j^{m_{j+kn}})$, $1 \leq i \leq m$, $1 \leq j \leq n$, $0_l eqk \leq s-1$ and set $k_{\mathbf{A},\underline{m}^0} := \mathbb{Q}(\zeta_{o(A_1^{m_1^0})}, ..., o(A_m^{m_m^0})$. Then the above assertion remains true replacing $k_{\mathbf{A}}$ by $k_{\mathbf{A},\underline{m}^0}$.

Proof. Asume (1). According to theorem 4.4, for s large enough $\mathbf{C}_s$ verifies condition (**Trans**) of proposition 4.13 (since $([\mathbf{A}], [\mathbf{B}]^s)$ already does) so we are only left to check condition (**LocReal**). Writing $\Sigma \cap \mathbb{Q} = \{p_1, ..., p_r\}$, re-use the notation of lemma 4.17 and take for instance $a_{m+i} = (p_1 \cdots p_r)^i$, $i = 1, ..., ns$, $a := (p_1 \cdots p_r)^n$ with $n >\max\{\frac{1}{p_i - 1}\}_{1 \leq i \leq r}$. These satisfy the conditions $|a_{m+i}|_p < 1$, $|a_{m+i} - a_{m+j}|_p < 1$ and $|a|_p < |p|^{\frac{1}{p-1}}$ for all $p \in \Sigma$, $1 \leq i \neq j \leq r_s^0$. Finally set $\mathbf{t}'_\Sigma := ((x_i := a_i, y_i := a_i + a)_{1 \leq i \leq m}, ((x^\epsilon_{i+kn,j} := a_{i+kn,j} + \zeta^{\epsilon u_{i+kn,j}}_{o(B_i)^{m_i}}, y^\epsilon_{i+kn,j} := a_{i+kn,j} + a + \zeta^{-\epsilon u_{i+kn,j}}_{o(B_i)^{m_i}})_{j=1,...,\phi(o(B_i)^{m_i+kn})/2})_{\substack{1 \leq k \leq s-1,\ 1 \leq i \leq n \\ \epsilon = \pm 1}})$ and conclude thanks to lemma 4.17 that for each $P \in \Sigma$ there exists a HM-G-cover defined over $(k_{\mathbf{A}})_P$ with invariants G, $\mathbf{C}_s$, $\mathbf{t}'$ with $\mathbf{t}'_{2m,r_s} = \mathbf{t}'_\Sigma$ that is, $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}(k_P)^{noob} \neq \emptyset$. By the branch cycle argument, $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}$ is defined over $k_{\mathbf{A}}$. Thus, as in the proof of proposition 4.13 applying the local-global principle to the global descent variety yields the announced result. Part (2) can be similarly deduced from (2-1), lemma 4.17. □

In terms of G-covers, (1), theorem 4.18 means that for s large enough there exists HM-G-covers (f, α) defined over $k_{\mathbf{A}}^\Sigma$, with invariants G, $\mathbf{C}_s$, $\mathbf{t}_f$ where $\mathbf{t}_f$ can be written $\mathbf{t}_f = \mathbf{t}_{1,f} + \mathbf{t}_\Sigma$ with $|\mathbf{t}_{1,f}| = 2m-1$ and $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-(2m-1)}(\mathbb{Q})$. For instance, take for G any group of section 4.2.3.2 (1), (2), (3) ; in that case $m = 1$ and we always are in situation (1).

Combining proposition 4.8 and the constructions of section 4.4.1.2 yields the following profinite version of theorem 4.18

Theorem 4.19 *Let G be a finite group and p a prime number dividing $|G|$. Assume G contains two tuples $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$, $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$ verifying* (**H**1.1$^+$), (**H**1.2$^+$) *and* (**H**2) *from proposition 4.8 (for instance, assume G, A, $\mathbf{B}$ verify conditions (i), (ii) and (iii) of corollary 4.5). Set $k_{\mathbf{A}} := \mathbb{Q}(\zeta_{o(A_1)}, ..., \zeta_{o(A_m)})$ and write*

$$\mathbf{C}_s := ([\mathbf{A}], \mathrm{Rat}_{\underline{m}}(\mathbf{B}^s)) \quad r_s := l(\mathbf{C}_s)$$

where $\underline{m} = (m_1, ..., m_{ns}) \in \mathbb{N} \setminus \{0\}^{ns}$ is such that $o(B_i)^{m_{i+kn}} \neq o(B_j)^{m_{j+ln}}$, $(i,k) \neq (j,l)$, $0 \leq i, j \leq n$, $1 \leq k, l \leq s-1$. Then, for s large enough, the HM-modular tower $(\mathcal{H}'^{HM}_{r_s,p^{k+1}\tilde{G}}(\mathbf{C}_{k+1,s}) \to \mathcal{H}'^{HM}_{r_s,p^k\tilde{G}}(\mathbf{C}_{k,s}))_{k \geq 0}$ is a tower of geometrically irreducible varieties and, for any $\mathbf{t}' \in \mathcal{U}^{r_s-(2m-1)}(\overline{\mathbb{Q}})$,

$(\mathcal{H}'^{HM}_{r_s,\overset{k+1}{p}\tilde{G}}(\mathbf{C}_{k+1,s})_{\mathbf{t}'} \to \mathcal{H}'^{HM}_{r_s,\overset{k}{p}\tilde{G}}(\mathbf{C}_{k,s})_{\mathbf{t}'})_{k\geq 0}$ is a tower of HM-curves which are still geometrically irreducible. Furthermore, for any finite set Σ of (non archimedean) places of $k_{\mathbf{A}}$ of residue characteristic not dividing $|G|$,

(1) If there exists $a_1, ..., a_m \in \mathbb{Q}$ such that $|a_i - a_j|_p = 1$, $1 \leq i \neq j \leq m$ for any residue characteristic p of $P \in \Sigma$ then there exists $\mathbf{t}'_\Sigma \in \mathcal{U}^{r_s-(2m-1)1}(\overline{\mathbb{Q}})$ with $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-(2m-1)}(\mathbb{Q})$ and such that the corresponding tower of $(2m-1)$-dimensional symmetrised HM-subvarieties $(\mathcal{H}^{HM}_{r_s,\overset{k+1}{p}\tilde{G}}(\mathbf{C}_{k+1,s})_{\mathbf{t}'_\Sigma} \to \mathcal{H}^{HM}_{r_s,\overset{k}{p}\tilde{G}}(\mathbf{C}_{k,s})_{\mathbf{t}'_\Sigma})_{k\geq 0}$ is defined over $k_{\mathbf{A}}$ with the property that

$$\varprojlim_{k\geq 0} \mathcal{H}^{HM}_{r_s,\overset{k}{p}\tilde{G}}(\mathbf{C}_{k,s})_{\mathbf{t}'_\Sigma}((k_A)_P)^{noob} \neq \emptyset,\ P \in \Sigma \quad \text{and} \quad \mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}(k_A^\Sigma)^{noob} \neq \emptyset.$$

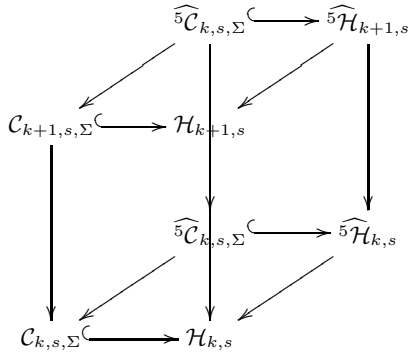
(2) Else, choose furthermore $\underline{m}^0 :== (m_1^0, ..., m_m^0) \in \mathbb{N}^m$ such that $o(A_i)^{m_i^0} \neq o(A_j^{m_j^0})$, $1 \leq i \neq j \leq m$ and $o(A_i)^{m_i^0} \neq o(B_j^{m_{j+kn}})$, $1 \leq i \leq m$, $1 \leq j \leq n$, $0_l eqk \leq s-1$ and set $k_{\mathbf{A},\underline{m}^0} := \mathbb{Q}(\zeta_{o(A_1^{m_1^0})}, ..., o(A_m^{m_m^0})$. Then the above assertion remains true replacing $k_{\mathbf{A}}$ by $k_{\mathbf{A},\underline{m}^0}$.

These conclusions still hold (with the same s and $\mathbf{t}'_\Sigma$) for any associated q-central tower (for primes $q \neq p$ dividing $|G|$ and such that G is q perfect) replacing $e(G)$ by $e(G)e(G)_q$.

Proof. Assume (1). According to proposition 4.8, for s large enough and for all $k \geq 0$, $\mathbf{C}_{k,s}$ (resp. $\widehat{{}^q\mathbf{C}_{k,s}}$) verifies (**C**1), (**C**2) that is, $\mathcal{H}'^{HM}_{r_s,\overset{k}{p}\tilde{G}}(\mathbf{C}_{k,s})_{\mathbf{t}'_\Sigma}$ (resp. $\mathcal{H}'^{HM}_{r_s,\widehat{{}^q\overset{k}{p}\tilde{G}}}(\widehat{{}^q\mathbf{C}_{k,s}})_{\mathbf{t}'_\Sigma}$) is a geometrically irreducible HM-curve. Consider the $\mathbf{t}' \in \mathcal{U}^{r_s}(\mathbb{Q})$, $\mathbf{t}'_\Sigma \in \mathcal{U}^{r_s-(2m-1)}(\overline{\mathbb{Q}})$ built in the proof of theorem 4.18. Then, for any $P \in \Sigma$, $\mathcal{H}^{HM}_{r_s,\overset{k}{p}\tilde{G}}(\mathbf{C}_{k,s})_{\mathbf{t}'_\Sigma}(k_P)^{noob} \neq \emptyset$ (resp. $\mathcal{H}^{HM}_{r_s,\widehat{{}^q\overset{k}{p}\tilde{G}}}(\widehat{{}^q\mathbf{C}_{k,s}})_{\mathbf{t}'_\Sigma}(k_P)^{noob} \neq \emptyset$) and these sets being finite, one has $\varprojlim_{k\geq 0}\mathcal{H}^{HM}_{r_s,\overset{k}{p}\tilde{G}}(\mathbf{C}_{k,s})_{\mathbf{t}'_\Sigma}(k_P)^{noob} \neq \emptyset$, $P \in \Sigma$ (resp. $\varprojlim_{k\geq 0}\mathcal{H}^{HM}_{r_s,\widehat{{}^q\overset{k}{p}\tilde{G}}}(\widehat{{}^q\mathbf{C}_{k,s}})_{\mathbf{t}'_\Sigma}(k_P)^{noob} \neq \emptyset$, $P \in \Sigma$) and the second part of the conclusion is obtained, once again, using the local-global principle and the global descent varieties. One obtains assertion (2) in a similar way. □

In terms of G-covers, theorem 4.19 means that for s large enough and for all $k \geq 0$ there exists HM-G-covers (f_k, α_k) defined over $k_{\mathbf{A}}^\Sigma$, with invariants $\overset{k}{p}\tilde{G}$, $\mathbf{C}_{k,s}$, $\mathbf{t}_{f_k}$ where $\mathbf{t}_{f_k}$ can be written $\mathbf{t}_{f_k} = \mathbf{t}_{1,f_k} + \mathbf{t}_\Sigma$ with $|\mathbf{t}_{1,f_k}| = 2m-1$ and $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-(2m-1)}(\mathbb{Q})$.

Example 4.20 Let us consider for instance M_{11} (*cf.* section 4.2.3.2 (2)). Take $\mathbf{A} = (8A)$, $\mathbf{B} = (11A)$ and, with the notation of theorem 4.19, let $(\mathcal{H}_{k+1,s} \to \mathcal{H}_{k,s})_{k\geq 0}$ be the HM-modular tower associated with the data $(M_{11}, \mathbf{C}_s, 3)$ and write $\mathcal{C}_{k,s,\Sigma} := (\mathcal{H}_{k,s})_{\mathbf{t}'_\Sigma}$, $k \geq 0$ for the resulting symmetrised HM-curves. Since 5 does not divide 8, 11, by Schur-Zassenhauss, there exists a unique conjugacy class $\widehat{{}^5(8A)_k}$ (resp. $\widehat{{}^5(11A)_k}$) lifting $(8A)_k$ (resp. $(11A)_k$) in $\widehat{{}^5\overset{k}{p}\tilde{G}}$ with $o(\widehat{{}^5(8A)_k}) = 8$ (resp. $o(\widehat{{}^5(11A)_k}) = 11$). This defines uniquely an associated 5-central tower $(\widehat{{}^5\mathcal{H}}_{k+1,s} \to \widehat{{}^5\mathcal{H}}_{k,s})_{k\geq 0}$ defined over the same field $k := \mathbb{Q}(i\sqrt{2})$ as $(\mathcal{H}_{k+1,s} \to \mathcal{H}_{k,s})_{k\geq 0}$; write $\widehat{{}^5\mathcal{C}}_{k,s,\Sigma} := (\widehat{{}^5\mathcal{H}}_{k,s})_{\mathbf{t}'_\Sigma}$, $k \geq 0$ for the resulting curves. The following commutative diagram defined over k summarizes the situation



Theorem 4.19 then means that the non obstruction locus of the left side of this diagram carries (double) projective systems of k_P-points for each $P \in \Sigma$ and that $\mathcal{C}_{k,s,\Sigma}(k^\Sigma)^{noob} \neq \emptyset$, $\widehat{{}^5\mathcal{C}}_{k,s,\Sigma}(k^\Sigma)^{noob} \neq \emptyset$, $k \geq 0$.

4.4.2.3 Working over fields with no roots of 1

Refining lemma 4.17 and the method of section 4.4.2.2 yields analogs of theorems 4.18, 4.19 with $k_{\mathbf{A}}$, $k_{\mathbf{A},\underline{m}}$ replaced by $\mathbb{Q}$. In counterpart, the dimension of the (symmetrised) HM-subvarieties we have to use will be in general larger than the one of the (symmetrised) HM-subvarieties that appear in theorems 4.18, 4.19. Indeed, the branch cycle argument gives a necessary condition to obtain symmetrised HM-subvarieties defined over $\mathbb{Q}$: $\mathbf{C}_s$ (resp. $\mathbf{C}_{s,k}$, $k \geq 0$) have to be replaced by the rational union of conjugacy classes $\mathbf{C}_s := \mathrm{Rat}_{\underline{m}}(\mathbf{A}, \mathbf{B}^s)$ (resp. $\mathbf{C}_{s,k} := \mathrm{Rat}_{\underline{m}}(\mathbf{A}_k, \mathbf{B}_k^s)$, $k \geq 0$) and thus $2m-1$ by $r := l(\mathrm{Rat}_{(m_1,...,m_m)}(\mathbf{A}))$, r_s by $r_s := r_s + r - 2m$. We also have to check $\mathbf{t}'_\Sigma$ can be built in such a way that the r-dimensional geometrically irreducible symmetrised HM-variety $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}$ (resp. $\mathcal{H}^{HM}_{r_s,{}^k_p\tilde{G}}(\mathbf{C}_{k,s})_{\mathbf{t}'_\Sigma}$, $k \geq 0$) is defined over $\mathbb{Q}$ and carries $\mathbb{Q}_p$-points for each $P \in \Sigma$. This can be done using (2-2), lemma 4.17, which also explains how to choose $m_1, ..., m_m$. These results can be improved depending on the rationality properties of $\mathbf{A}$ and the value of the integer m compared with the one of the residue characteristic of the places in Σ.

Theorem 4.21 *Let G be a finite group containing two tuples $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$, $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$ verifying (**H**1) and (**H**2) from theorem 4.4. Set*

$$\mathbf{C}_s := (\mathrm{Rat}_{\underline{m}}(\mathbf{A}, \mathbf{B}^s)) \quad r := l(\mathrm{Rat}_{(m_1,...,m_m)}(\mathbf{A})) \quad r_s := l(\mathbf{C}_s)$$

where $\underline{m} = (m_1, ..., m_{ns+m}) \in \mathbb{N} \setminus \{0\}^{ns}$ is any tuple such that the $o(A_i)^{m_i}$, $o(B_j)^{m_{j+ln}}$, $1 \leq i \leq m$, $1 \leq j \leq n$, $0 \leq l \leq s-1$ are all distincts. Then, for s large enough, $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)$ is a geometrically irreducible variety and, for any $\mathbf{t}' \in \mathcal{U}^{r_s-(2m-1)}(\overline{\mathbb{Q}})$ the $(2m-1)$-dimensional HM-subvariety $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'}$ remains geometrically irreducible. Furthermore, for any finite set Σ of (non archimedean) places of $\mathbb{Q}$ of residue characteristic not dividing $|G|$, there exists $\mathbf{t}'_\Sigma \in \mathcal{U}^{r_s-r}(\overline{\mathbb{Q}})$ with $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-r}(\mathbb{Q})$ and such that the corresponding r-dimensional symmetrised HM-subvariety $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}$ is defined over $\mathbb{Q}$ with the property that

$$\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}(\mathbb{Q}^\Sigma)^{noob} \neq \emptyset.$$

In terms of G-covers, theorem 4.21 means that for s large enough there exists HM-G-covers (f, α) defined over $\mathbb{Q}^\Sigma$, with invariants G, $\mathbf{C}_s$, $\mathbf{t}_f$ where $\mathbf{t}_f$ can be written $\mathbf{t}_f = \mathbf{t}_{1,f} + \mathbf{t}_\Sigma$ with $|\mathbf{t}_{1,f}| = r$, $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-r}(\mathbb{Q})$.

If A_m is a rational conjugacy classes, $\mathbf{t}'_\Sigma \in \mathcal{U}^{r_s-r}(\overline{\mathbb{Q}})$ can be replaced by $\mathbf{t}'_\Sigma \in \mathcal{U}^{r_s-(r+1)}(\overline{\mathbb{Q}})$. If $\mathbf{A}$ is a tuple of rational conjugacy classes and if there exists $a_1, ..., a_m \in \mathbb{Q}$ such that $|a_i - a_j|_p = 1$, $1 \leq i \neq j \leq m$ for any residue characteristic p of $P \in \Sigma$, $p \in \Sigma$, the statement of theorem 4.21 remains true with $\mathrm{Rat}_{\underline{m}}(\mathbf{A})$ replaced by $[\mathbf{A}]$. In that case, the (symmetrised) HM-subvariety $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}$ in theorem 4.21 has the same dimension as the (symmetrised) HM-subvariety in theorem 4.18. When $m = 1$ and A_1 is rational, the statement of theorem 4.21 is actually true for any finite set Σ of prime not dividing $|G|$ since, in that case, the condition $|a_i - a_j|_p = 1$, $1 \leq i \neq j \leq m$ (which is the main obstruction as explained in the comment about condition (*)) is empty.

Example 4.22 Take $G := L_2(p)$ with $p \equiv 3$ [mod4], $p \geq 7$ is a prime, $\mathbf{A} := (2A)$, $\mathbf{B} := (pA)$. Then since $m = 1$ and $2A$ is rational, for s large enough and for any finite set of prime not dividing $p(p^2-1)/2$ there exists HM-G-covers (f, α) defined over $\mathbb{Q}^\Sigma$, with invariants $L_2(p)$, $\mathbf{C}_s$, $\mathbf{t}_f$ where $\mathbf{t}_f$ can be written $\mathbf{t}_f = \mathbf{t}_{1,f} + \mathbf{t}_\Sigma$ with $|\mathbf{t}_{1,f}| = 1$, $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-1}(\mathbb{Q})$.

Profinite versions of theorem 4.21 and its improvements under the above rationality assumptions can be given. We leave this to the reader who can show, for instance, that for any odd primes $p < q$ and for all $n \geq 0$ there exists HM-G-covers (f_n, α_n) defined over $\mathbb{Q}^\Sigma$ with group ${}^n_p\tilde{\mathcal{A}}_q$ and a branch point divisor $\mathbf{t}_{f_n} = \mathbf{t}_{1,f_n} + \mathbf{t}_\Sigma$ where $|\mathbf{t}_{1,f_n}| = 1$ and $\mathbf{t}_\Sigma$ is rational (where Σ is any finite set of primes $> q$).

4.4.3 $(\mathbf{RIGP}/\mathbf{t}_2 \subset \mathbf{t})$ over $\mathbb{Q}^{tr}$

4.4.3.1 G-covers defined over $\mathbb{R}$

We first recall succintly the description of G-covers defined over $\mathbb{R}$ with prescribed invariants given in [DF94]. We will use it in the next paragraph.

Let $\mathbf{t}' \in \mathcal{U}^r(\overline{\mathbb{Q}})$ be an r-tuple consisting of $r = r_1 + 2r_2$ branch points in configuration (r_1, r_2), that is with - r_1 real branch points $t_1, ..., t_{r_1}$.
- r_2 complex conjugated pairs $\{z_i, \overline{z}_i\} \subset \mathbb{P}^1(\mathbb{C})\backslash\mathbb{P}^1(\mathbb{R})$ with $z_i = t_{r_1+i-1}$, $\overline{z}_i = t_{r_1+i}$, $i = 1, ..., r_2$.

and assume that $t_1 < ... < t_{r_1}$, $\mathrm{Re}(z_1) < ... < \mathrm{Re}(z_{r_2})$. Then there exists a standard ordered topological bouquet $\underline{\gamma} = (\gamma_1, ..., \gamma_r)$ for $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ such that complex conjugation $c \in \Gamma_{\mathbb{R}}$ acts by
- ${}^c\gamma_i = (\gamma_i^{-1})^{(\gamma_1 \cdots \gamma_{i-1})}$, $i = 1, ..., r_1$
- ${}^c\gamma_{r_1+2i-1} = (\gamma_{r_1+2i}^{-1})^{(\gamma_1 \cdots \gamma_{r_1})}$, $i = 1, ..., r_2$

Let G be a finite group and $\mathbf{C} = (C_1, ..., C_r) \in \mathcal{C}_r(G)$. Define the subset $\mathrm{sni}^{\mathbb{R}}(\mathbf{C}; \mathrm{r}_1, \mathrm{r}_2)$ of $\mathrm{sni}(\mathbf{C})$ consisting of those $(g_1, ..., g_r)$ in $\mathrm{sni}(\mathbf{C})$ verifying the additional condition :
(4) there exists an involution $g_0 \in G$ such that - $g_i^{g_0} = (g_i^{-1})^{(g_1 \cdots g_{i-1})^{-1}}$, $i = 1, ..., r_1$
- $g_{r_1+2i-1}^{g_0} = (g_{r_1+2i}^{-1})^{(g_1 \cdots g_{r_1})}$, $i = 1, ..., r_2$

Write $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ for the corresponding quotient set modulo the componentwise action of Inn(G). Then, $BCD_{\underline{\gamma}}$ defines an identification $(\Psi'_{r,G})^{-1}(\mathbf{t}') \simeq \overline{\mathrm{sni}}(\mathbf{C})$ such that $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ corresponds to those G-covers in $\overline{\mathrm{sni}}(\mathbf{C})$ which are defined over $\mathbb{R}$.

4.4.3.2 Statements and applications

We will use here a variant Rat of the rationalization operator Rat_0 introduced in paragraph 4.4.2.1. Namely, $\mathrm{Rat}(C) := (C^{u_1}, C^{-u_1}, ..., C^{u_r}, C^{-u_r})$ if $\{C^u\}_{u \in (\mathbb{Z}/o(C)\mathbb{Z})^\star} = \{C^{\pm u_i}\}_{i=1,...,r}$

Theorem 4.23 *Let G be a finite group containing two tuples $\mathbf{A} = (A_1, ..., A_m)$, $\mathbf{B} = (B_1, ..., B_n)$ verifying* $(\mathbf{H}1)$ *and* $(\mathbf{H}2)$. *Write $\mathbf{C}_s := (\mathrm{Rat}(\mathbf{A}), \mathrm{Rat}(\mathbf{B})^s)$ and $r := \sum_{k=1}^m |\mathrm{Rat}(A_k)|$, $r_s := s\sum_{k=1}^n |\mathrm{Rat}(B_k)|$. Then, for s large enough, $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)$ is a geometrically irreducible $\mathbb{Q}$-variety and there exists $\mathbf{t}'_{\mathbb{R}} \in \mathcal{U}^{r_s-r}(\overline{\mathbb{Q}})$ with a $\mathbb{Q}$-rational associated divisor $\mathbf{t}_{\mathbb{R}} \in \mathcal{U}_{r_s-r}(\mathbb{Q})$ and such that the symmetrised HM-subvariety $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_{\mathbb{R}}}$ is a geometrically irreducible r-dimensional $\mathbb{Q}$-variety with,*

$$\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_{\mathbb{R}}}(\mathbb{Q}^{tr})^{noob} \neq \emptyset$$

Proof. As in the proof of theorem 4.18, we are only to show $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_{\mathbb{R}}}(\mathbb{R})^{noob} \neq \emptyset$. For this, apply the following procedure (with the notation of section 4.4.2.1) : given a non trivial conjugacy class C
(1) - If $o(C) = 2$, associate to C the tuple $\mathbf{t}'_C := (i, -i)$.
- If $o(C > 2)$, associate to C the tuple $\mathbf{t}'_C := (\zeta_{o(C)}^{u_1}, \zeta_{o(C)}^{-u_1}, ..., \zeta_{o(C)}^{u_{\phi(o(C))/2}}, \zeta_{o(C)}^{-u_{\phi(o(C))/2}})$.

(2) Set $\mathbf{t}' := (\mathbf{t}'_{1,r}, \mathbf{t}'_{r+1,r_s})$ with $\mathbf{t}'_{1,r} = (\mathbf{t}'_{A_i} + 4(i-1))_{i=1,...,m}$ and $\mathbf{t}'_{r+1,r_s} = ((\mathbf{t}'_{B_i} + 4(i-1))_{i=1,...,n}) + 4(m + jn))_{j=0,...,s-1}$.
Then, $\mathbf{t}' \in \mathcal{U}^{r_s}(\overline{\mathbb{Q}})$ is in configuration $(0, r_s/2)$ and since $\emptyset \neq \overline{\mathrm{hm}}(\mathbf{C}_s) \subset \mathrm{sni}^{\mathbb{R}}(\mathbf{C}_\mathrm{s}; 0, \mathrm{r_s}/2)$, we obtain $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'}(\mathbb{R})^{noob} \neq \emptyset$. Set $\mathbf{t}'_{\mathbb{R}} := \mathbf{t}'_{r+1,r_s}$, which satisfies $\mathbf{t}'_{\mathbb{R}} \in \mathcal{U}_{r_s-r}(\mathbb{Q})$. Then, by the branch cycle argument, $\mathcal{H}^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_{\mathbb{R}}}$ is defined over $\mathbb{Q}$ and conclude applying the local-global principle to the associated global descent variety as in the proof of proposition 4.13. □

As in section 4.4.2.2, one can state a profinite version of theorem 4.23 for modular towers and associated q-central towers ; we leave this to the reader and give another application of our method to the profinite regular inverse Galois problem over $\mathbb{Q}^{tr}$ (see also [**?**]).

Let $(s_{k+1} : G_{k+1} \twoheadrightarrow G_k)$ be a complete projective system of finite groups and $(\mathbf{C}_k = (C_{k,1}, ..., C_{k,r}))_{k\geq 0}$ a projective system of tuples $\mathbf{C}_k \in \mathcal{C}_r(G_k)$. Assume there exists $r_1, r_2 \geq 0$ with $r = r_1 + 2r_2$ and

$$(*) \text{ For all } m \geq 1 \text{ such that } (m, e(G)) = 1,\ s_{k+1}^{-1}(\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}_k; r_1, r_2)) \subset \overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}_{k+1}; r_1, r_2)$$

Lemma 4.24 *Assume there exists a $\mathbb{Q}^{tr}$-G-cover (f_0, α_0) with invariants G_0, $\mathbf{C}_0$, $\mathbf{t}'$ such that ${}^{\sigma}\mathbf{t}'$ is in configuration (r_1, r_2), $\sigma \in \Gamma_{\mathbb{Q}}$. Then there exists a regular realization of $\varprojlim_{k\geq 0} G_k$ over $\mathbb{Q}^{tr}$ with invariants $\varprojlim_{k\geq 0} \mathbf{C}_k$, $\mathbf{t}'$.*

Proof. Let $\mathbf{p}_0 \in \mathcal{H}_{r,G_0}(\mathbf{C}_0)_{\mathbf{t}}(\mathbb{Q}^{tr})^{noob}$ and $(f_k, \alpha_k)_{k\geq 0}$ a projective system of G-covers corresponding to a projective system of points $(\mathbf{p}_k)_{k\geq 0} \in \varprojlim_{k\geq 0} \mathcal{H}_{r,G_k}(\mathbf{C}_k)_{\mathbf{t}}$ above $\mathbf{p}_0$. For any $\sigma \in \Gamma_{\mathbb{Q}}$, by the branch cycle argument, ${}^{\sigma}(\mathbf{p}_k)_{k\geq 0} \in \varprojlim_{k\geq 0} \mathcal{H}_{r,G_k}(\mathbf{C}_k^{\chi(\sigma)})_{\mathbf{t}}$. Furthermore, since (f_0, α_0) is defined over $\mathbb{Q}^{tr}$, ${}^{\sigma}(f_0, \alpha_0)$ is defined over $\mathbb{R}$ with branch points ${}^{\sigma}\mathbf{t}'$ in configuration (r_1, r_2) so, its branch cycle description lies in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}_0; r_1, r_2)$. The branch cycle description of ${}^{\sigma}(f_k, \alpha_k)$ lies in $\overline{\text{sni}}(\mathbf{C}_k)$ above the one of ${}^{\sigma}(f_0, \alpha_0)$ so, according to (*), in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}_k; r_1, r_2)$. As a result, ${}^{\sigma}(f_k, \alpha_k)$ is defined over $\mathbb{R}$. Now, let $D(f_k, \alpha_k)$ be the descent variety of (f_k, α_k) [DDoMo04] ; it is a smooth geometrically irreducible $\mathbb{R}$-variety such that for any $\sigma \in \Gamma_{\mathbb{Q}}$ ${}^{\sigma}D(f_k, \alpha_k)(\mathbb{R}) = D({}^{\sigma}(f_k, \alpha_k))(\mathbb{R}) \neq \emptyset$. Apply then the local-global principle to show $D(f_k, \alpha_k)(\mathbb{Q}^{tr}) \neq \emptyset$; that is, (f_k, α_k) is defined over $\mathbb{Q}^{tr}$. □

Example 4.25 Let $D_{2a^\infty} := \varprojlim_{k\geq 1} D_{2a^k}$ be the prodihedral group of order $2a^\infty$ where

$$D_{2a^k} :=< u, v |\ u^{a^k} = v^2 = 1,\ \ vuv = u^{-1} >$$

For any $k \geq 1$, let $A_{k,i}$ be the conjugacy class of u^i in D_{2a^k}, $i = 1, ..., E(a^k + 1)/2$ and B_k be the conjugacy class of v in D_{2a^k}.

First step : For any $1 \leq i_1, ..., i_t \leq E(a^k + 1)/2$ (*) is fulfilled with $\mathbf{C}_k := ([B_k], [A_{k,i_1}, ..., A_{k,i_t}])$, $k \geq 1$.

Proof. One checks that, given $n \geq 1$, any element of $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{C}_n; 2, s-1)$ is either of the form $\mathbf{g}_1 = [v_n, u_n^{i_1}, ..., u_n^{i_t}]$ $(g_0 = 1)$ or of the form $\mathbf{g}_{2,k_n,\epsilon} = (v_n, v_n u_n^{k_n}, u_n^{\epsilon i_1}, u_n^{\epsilon i_1}, ..., u_n^{\epsilon i_t}, u_n^{\epsilon i_t})$ with $\epsilon = \pm 1$ and $k_n + 2\epsilon(i_1 + \cdots i_t) \equiv 0\ [\text{mod} a^n]$ $(g_0 = v_n)$. But, on $A_{i_k,n+1}$, $k = 1, ..., t$, s_n is bijective so - due to relation (2) in the definition of $\overline{\text{sni}}(\mathbf{C}_{n+1})$ - the preimage of $\mathbf{g}_1$ is necessarily $[v_{n+1}, u_{n+1}^{i_1}, ..., u_{n+1}^{i_t}]$ whereas the one of $\mathbf{g}_{2,k_n,\epsilon}$ consists of elements of the form $(v_{n+1}, v_{n+1}u_n^{k_n+la^n}, u_{n+1}^{\epsilon i_1}, u_{n+1}^{\epsilon i_1}, ..., u_{n+1}^{\epsilon i_t}, u_{n+1}^{\epsilon i_t})$ with $0 \leq l \leq a-1$ such that $k_n + la^n + 2\epsilon(i_1 + \cdots i_t) \equiv 0\ [\text{mod} a^{n+1}]$. The proof remains the same when replacing $\mathbf{C}$ by $\mathbf{C}^m$. Conclude using §5.3.1. □

Second step : To prove the existence of (f_1, α_1) as in the lemma, we re-use the idea (and the notation !) of the proof of theorem 4.23 as follows : observe that $\mathbf{A} := (B_1)$, $\mathbf{B} := (A_{1,1})$ verify (**H**1) and (**H**2) so, with $\mathbf{C}_1 := \mathbf{C}_s$, for s large enough and for any $\mathbf{t}'_{3,r_s} \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$, $\mathcal{H}^{HM}_{r_s,D_{2a}}(\mathbf{C}_1)_{\mathbf{t}'_{3,r_s}}$ is a geometrically irreducible curve. Let $\mathbf{t}'_{3,r_s} \in \mathcal{U}^{r_s-2}(\overline{\mathbb{Q}})$ built as in the proof of theorem 4.23 then, since B is rational $(o(B) = 2)$, $\mathcal{H}^{HM}_{r_s,D_{2a}}(\mathbf{C}_1)_{(0,\mathbf{t}'_{3,r_s})}$ is defined over $\mathbb{Q}$. According to section 4.4.3.1, $\mathcal{H}^{HM}_{r_s,D_{2a}}(\mathbf{C}_1)_{(0,\mathbf{t}'_{3,r_s})}(\mathbb{R})^{noob} \neq \emptyset$ so, applying once again the local-global principle to the global descent variety, $\mathcal{H}^{HM}_{r_s,D_{2a}}(\mathbf{C}_1)_{(0,\mathbf{t}'_{3,r_s})}(\mathbb{Q}^{tr})^{noob} \neq \emptyset$ and, if (f_1, α_1) is a G-cover corresponding to a point $\mathbf{p}_1 \in \mathcal{H}^{HM}_{r_s,D_{2a}}(\mathbf{C}_1)_{(0,\mathbf{t}'_{3,r_s})}(\mathbb{Q}^{tr})^{noob}$, its branch point divisor is of the form $(t_1, 0,)\mathbf{t}'_{2,r_s}$ that is in configuration $(2, r_s/2 - 1)$ and satisfying the hypothesis of lemma 4.24.

Conclude, by applying this lemma, that there exists regulr realization of D_{2a^∞} over $\mathbb{Q}^{tr}$ with invariants $\varprojlim_{k\geq 0}([B_k], [A_{k,1}^{u_1}, ..., A_{k,1}^{u_{\phi(a)/2}}])$, $(t_1, 0, \mathbf{t}'_{3,r_s})$.

4.4.4 Concluding remarks

The preceding constructions give rise to two natural questions :

Problem 4.26 *Is there an analog of theorem 4.18 for large fields ?*

Problem 4.27 *Is it possible to carry out the construction of geometrically irreducible HM-subvarieties* $\mathcal{H}'^{HM}_{r,G}(\mathbf{C})_{\mathbf{t}'}$ *in such a way that* $\mathcal{H}'^{HM}_{r,G}(\mathbf{C})_{\mathbf{t}'}(k_P) \neq \emptyset$ *for almost all places* P *of* k *? (where* $k := \mathbb{Q}(e^{\frac{2\pi i}{e(G)}})$

Both problems have a partial answer if we assume the ground field has enough roots of 1 but with losing the control of the dimension of the HM-subvarieties we obtain.

More precisely, for problem 4.26, let G be a finite group and let k be a large field of characteristic 0 containing all the $e(G)$th roots of 1. Assume G contains two tuples $\mathbf{A} = (A_1, ..., A_m)$, $\mathbf{B} = (B_1, ..., B_n)$ verifying (**H1**) and (**H2**) and, as usual, set $\mathbf{C}_s = ([\mathbf{A}], [\mathbf{B}]^s)$, $r_s := 2(m + ns)$). Then, for s large enough and for any $\mathbf{t}'_{2m,r_s} \in \mathcal{U}^{r_s-(2m-1)}$, $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)_{\mathbf{t}'_{2m,r_s}}$ remains geometrically irreducible defined over $k(\mathbf{t}'_{2m,r_s})$; thus, for any closed subvariety $V \hookrightarrow \mathcal{U}^{r_s}$ containing $\mathbf{t}'_{2m,r_s}$, $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)_V$ also remains geometrically irreducible. In particular, consider the case when $V^{odd}_{\mathbf{t}'_{2m,r_s}} = \{\mathbf{u}' \in \mathcal{U}^{r_s} \mid \mathbf{u}'_{2i+1,2i+1} = \mathbf{t}'_{2i+1,2i+1},\ i = m, ..., ns\}$ that is, we assume the odd entries of indices $\geq 2m+1$ are those of $\mathbf{t}'_{2m,r_s}$. Now, take $\mathbf{t}' = (t_1, ..., t_{r_s}) \in \mathcal{U}^{r_s}(k(T))$ with $t_{2i-1} \in k$, and $t_{2i} = t_{2i-1} + T$, $i = 1, ..., m + ns$; $\mathbf{t}' \in \mathcal{U}^{r_s}(k(T))$ and verifies (*) for the complete field $k((T))$ so, we can apply (1) of lemma 4.17 to build HM-G-covers defined over $k((T))$ with invariants $\mathbf{C}$, $\mathbf{t}'$. In other words, the geometrically irreducible k- HM-subvariety $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)_{V^{odd}_{\mathbf{t}'_{2m,r_s}}}$ carries $k((T))$-points corresponding to G-covers defined over $k((T))$ so its global descent variety, which is also geometrically irreducible defined over k carries $k((T))$-points ; conclude, using the fact k is large, that $\mathcal{H}'^{HM}_{r,G}(\mathbf{C}_s)_{V^{odd}_{\mathbf{t}'_{2m,r_s}}}(k)^{noob} \neq \emptyset$.

Likewise, for problem 4.27, consider any $\mathbf{t}' \in \mathcal{U}^{r_s}(\mathbb{Q})$ then the set Σ of places of k diving $|G|$ or where $V^{odd}_{\mathbf{t}'_{2m,r_s}}$ has bad reduction is finite. Thus, for any place $P \notin \Sigma$, one can always build $\mathbf{t}'_P \in V^{odd}_{\mathbf{t}'_{2m,r_s}}(k)$ verifying (*) for the complete field k_P thus, HM-G-covers defined over k_P with invariants $\mathbf{C}_s$, $\mathbf{t}'_P$. Conclude as above that $\mathcal{H}'^{HM}_{r_s,G}(\mathbf{C}_s)_{V^{odd}_{\mathbf{t}'_{2m,r_s}}}(k_P)^{noob} \neq \emptyset$ for all places $P \notin \Sigma$.

Obviously, the main drawback of these constructions is that we obtain $2m + ns$-dimensional HM-subvarieties where s is hard to control and a priori very large.

The following conjecture is a variant of problem 4.27 which is a stronger version of the results of [Des95] or [DE03]. We give a track to investigate it.

Conjecture 4.28 *Let* G *be a finite group, then there exists a geometrically irreducible* $\mathbb{Q}$*-component* $\mathcal{H}^0_G$ *of some Hurwitz space* $\mathcal{H}_G$ *associated with* G *containing a geometrically irreducible* $\mathbb{Q}$*-curve* $\mathcal{C}^0_G \subset \mathcal{H}^0_G$ *verifying* $\mathcal{C}^0_G(\mathbb{Q}_p)^{noob} \neq \emptyset$ *for all places* $p \notin \Sigma_G$*, where* Σ_G *is a finite set of places* ***explicitly computable*** [4].

An idea to tackle this conjecture would be to use other rational base curves than the standard $\mathbf{t}' : \mathbb{P}^1 \setminus \{t_2, ..., t_r\} \hookrightarrow \mathcal{U}^r$, $t \to (t, t_2, ..., t_r)$ we use to define HM-curves. Considering (1) of lemma 4.17 (we still work over $k := \mathbb{Q}(e^{\frac{2\pi i}{e(G)}})$ to avoid rationality matters), let $\mathcal{C} : \mathbb{P}^1 \setminus \{0, \infty \pm 1, ..., \pm(s-1)\} \hookrightarrow \mathcal{U}^r$, $t \to (t, 3t, t+2, 3t+2, ..., t+2(s-1), 3t+2(s-1)) =: \mathbf{t}'(t)$. Then, for any places P of k of residue characteristic p such that $p \neq 2$ and $p \not| \, l - k$, $0 \leq k < l \leq s-1$, $\mathbf{t}'(p)$ verifies condition (*) thus, for any s-tuple $\mathbf{C} = (C_1, ..., C_s) \in \mathcal{C}_s(G)$,

$$\emptyset \neq \mathcal{H}'^{HM}_{2s,G}([\mathbf{C}])_{\mathbf{t}'(p)}(k_P)^{noob} \subset \mathcal{H}'^{HM}_{2s,G}([\mathbf{C}])_{\mathcal{C}}(k_P)^{noob}$$

Since $\mathcal{C}$ is defined over $\mathbb{Q}$, $\mathcal{H}'^{HM}_{2s,G}([\mathbf{C}])_{\mathcal{C}}$ is a k-curve. Provided $\mathcal{H}'^{HM}_{2s,G}([\mathbf{C}])$ is geometrically irreducible, the problem is to show $\mathcal{H}'^{HM}_{2s,G}([\mathbf{C}])_{\mathcal{C}}$ is too that is the monodromy group of $\mathcal{H}'^{HM}_{2s,G}([\mathbf{C}])_{\mathcal{C}} \to \mathbb{P}^1 \setminus \{0, \infty, \pm 1, ..., \pm(s-1)\}$ acts transitively on $O^{HM}([\mathbf{C}])$. We would like an equivalent of [F95a] Th. 3.21. (that is to control s so as to control Σ_G) but if this seems more likely to occur for curves like $\mathcal{C}$

[4] We insists on the fact one must be able to define precisely Σ_G since Hensel's lemma and Hasse-Weil bounds for curves over finite fields imply any $\mathbb{Q}$-curve carries $\mathbb{Q}_p$-rational points for almost all places p of $\mathbb{Q}$! Actually, one can even expect Σ_G to be contained in the set of all primes p dividing $|G|$.

(more ramification points) than for standard curves, the monodromy is also more difficult to compute ; however, choosing a more appropriate $\mathcal{C}$ and a clever topological bouquet for $\mathbb{P}^1\setminus\{0,\infty,\pm1,...,\pm(s-1)\}$ might lead to at least partial results.

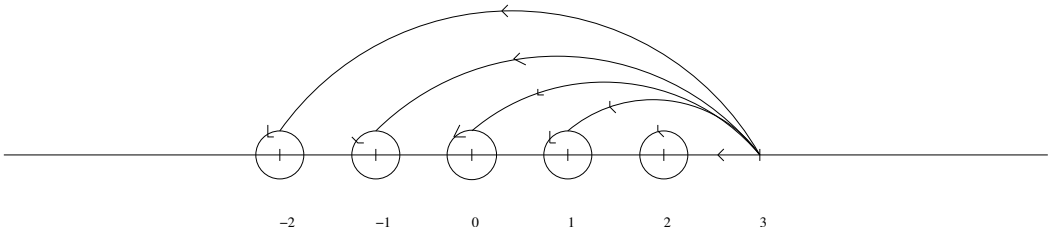


FIG. 4.1 –

Example 4.29 With $s=3$, we can compute the monodromy starting from the topological bouquet of figure 1 for $\mathbb{P}^1\setminus\{0,\infty\pm1,\pm2\}$. We obtain the subgroup of SH_6 generated by

- γ_{-2} :$Q_5Q_4Q_3Q_2Q_1^{-2}Q_2^{-1}Q_3^{-1}Q_4^{-1}Q_5^{-1}$.
- γ_{-1} :$Q_4Q_3Q_2Q_5Q_4Q_3^{-2}Q_4^{-1}Q_5^{-1}Q_1^{-2}Q_2^{-1}Q_3^{-1}Q_4^{-1}$
- γ_0 :$Q_3Q_2Q_4Q_5^{-2}Q_3^{-2}Q_4^{-1}Q_1^{-2}Q_2^{-1}Q_3^{-1}$
- γ_1 :$Q_3Q_4^{-2}Q_2^{-2}Q_3^{-1}$
- γ_2 :Q_3^{-2}.
- γ_∞ :$(\gamma_{-2}\cdots\gamma_2)^{-1}$

If we take for instance $G:=D_8=<u,v\mid u^4=v^2=1,\ vuv=u^{-1}>$ and $\mathbf{C}:=[B_1,B_2,B_2]$ where B_1 is the conjugacy class of v and B_2 the one of vu, we obtain a degree 8 connected cover $\mathcal{H}_{6,D_8}([\mathbf{C}])_{\mathcal{C}}\to\mathbb{P}^1\setminus\{0,\infty\pm1,\pm2\}$ with ramification type $((2)^4,(2)^4,(2)^4,(2)^4,(1)^8,(2)^4)$ that is $\mathcal{H}_{6,D_8}([\mathbf{C}])_{\mathcal{C}}$ is a genus 3 geometrically irreducible $\mathbb{Q}$-curve with $\mathcal{H}_{6,D_8}([\mathbf{C}])_{\mathcal{C}}(\mathbb{Q}_p)^{noob}\neq\emptyset$ for all primes $p\neq2$ and $\mathcal{H}_{6,D_8}([\mathbf{C}])_{\mathcal{C}}(\mathbb{R})^{noob}\neq\emptyset$.

Chapitre 5

Rational points on Hurwitz towers

Il s'agit de l'article [C04d].

Sommaire

Introduction

The problem motivating this paper is the regular inverse Galois problem RIGP for profinite groups over number fields and its translation in terms of rational points on towers of Hurwitz spaces. Though strongly related to the RIGP for finite groups, additional obstructions - such as the lack of roots of 1 - are attached to the RIGP for profinite groups. For instance, the branch cycle argument (lemma 5.5) rules out the regular realization of such elementary profinite groups as $\mathbb{Z}_p$ or D_{2p^∞} over any number field [F95b]. On the contrary, groups as $\mathrm{GL}_n(\mathbb{Z}_p)$ have been recently regularly realized over $\mathbb{Q}$ by Katz's algorithm for the rigidity method. So, there is no hope to obtain a global answer to the RIGP for profinite groups over number fields.

In this paper, we generalize a result of [BF02] which states that, given a number field k and a centerless p-perfect finite group G_0, there is no regular realization of its universal p-Frattini cover ${}_p\tilde{G}_0$ over k with only inertia groups of finite prime-to-p order. More precisely, we replace the universal p-Frattini cover ${}_p\tilde{G}_0$ of G_0 by any profinite group G which is an extension of a finite group G_0 by a pronilpotent projective group P of finite rank and we impose no restriction on the ramification. We thus obtain

Theorem 5.1 *Let $1 \to P \to G \to G_0 \to 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a pronilpotent projective group of finite rank and k be either a number field or a finite field of characteristic $q > 0$ not dividing $|G_0|$ and not dividing p if P is a pro-p group*[1]*. Then there is no regular realization of G over $k(T)$ for any number field k.*

In terms of towers of Hurwitz moduli spaces of covers, this means that, for any number field k (or any finite field as in the statement), there is no projective system of k-rational points lying in the non-obstruction locus (that is, corresponding to projective systems of G-covers not only with field of moduli k but defined over k compatibly) of any tower of Hurwitz spaces associated with such a profinite group G. It is rather natural to ask whether there may exist projective systems of k-rational points outside this non-obstruction locus. We show the answer is no.

Theorem 5.2 *Under the hypotheses of theorem 5.1, there is no Galois extension $K/\overline{k}(T)$ with group G and field of moduli k. In other words, there is no projective system of k-rational points on any tower of Hurwitz spaces $(\mathcal{H}_{r_{n+1},G_{n+1}} \to \mathcal{H}_{r_n,G_n})_{n\geq 0}$ associated with any complete projective system $(G_{n+1} \to G_n)_{n\geq 0}$ of finite groups such that $G = \varprojlim G_n$.*

The proof of theorem 5.1 has two parts : the first one (lemma 5.6) generalizes some argument from [F95b], the second one (lemma 5.7) rests on the branch cycle argument. Both involve some abelianization procedure that will be more systematically discussed in section 5. Theorem 5.2 is a consequence of both theorem 5.1 and the following result

Theorem 5.3 *Under the hypotheses of theorem 5.1 but with P a free pro-p group of finite rank, any regular Galois extension $K/\overline{k}(T)$ with group G and field of moduli k is defined over a finite extension k_0/k.*

For finite G-covers, there is a classical obstruction to the field of moduli being a field of definition. The proof of theorem 5.3 uses a generalization of this obstruction. This theorem also extends to the case P is a pronilpotent projective group of finite rank with only finitely many rank 1 p-Sylow subgroups, as we explain in §5.3.2.2.

A related problem is Fried's conjecture about the disappearance of rational points on modular towers beyond a certain level. We discuss this conjecture in the last section of our paper, showing in particular

Theorem 5.4 *Fried's conjecture is a consequence of the strong torsion conjecture for abelian varieties.*

The paper is organized as follows : section 1 recalls the basic notions and introduces the notation, section 2 is devoted to the proof of theorem 5.1, section 3 to the one of theorem 5.3. Section 4 gives some applications and section 5 is about Fried's conjecture.

Aknowledgment : This work originates in Fried's papers [F95b], [FK97], [BF02] where some of the ideas we generalize here already appear. I am also very grateful to P. Dèbes for his many re-readings and helpful comments.

5.1 Notation and basic notions

Given a field k, we will always denote by Γ_k its absolute Galois group. For any $r \geq 3$, set $\mathcal{U}^r = \text{spec}(\mathbb{Z}[T_1, ..., T_r]_{\prod_{1\leq i<j\leq r}(T_i-T_j)})$ and let $\mathcal{U}_r = \mathcal{U}^r/\mathcal{S}_r$ be the quotient of $\mathcal{U}^r$ by the natural action of the symmetric group $\mathcal{S}_r$.

[1] The latter condition being empty if at least two distinct primes divide $|P|$

5.1.1 Arithmetic fundamental group and G-covers

Let k be a field of characteristic 0 and $\overline{k(T)}$ an algebraic closure of $k(T)$. We fix a compatible system $(\zeta_n)_{n\geq 2}$ of primitive roots of 1 in k that is, $\zeta_{mn}^m = \zeta_n$, $n, m \geq 2$ (when $k = \mathbb{C}$, the canonical choice is $\zeta_n = \mathrm{e}^{2i\pi/n}$, $n \geq 0$). Given a non singular projective algebraic curve X/k and a divisor $\mathbf{t}$ on it, let $M_{k,X,\mathbf{t}}/\overline{k}(X)$ be the maximal algebraic extension of $\overline{k}(X)$ (in a fixed algebraic closure $\overline{k(X)}$) unramified outside $\mathbf{t}$. Then $M_{k,X,\mathbf{t}}/\overline{k}(X)$ and $M_{k,X,\mathbf{t}}/k(X)$ are Galois extensions with groups we denote by $\pi_{1,k}^{\mathrm{alg}}(X \setminus \mathbf{t})$ and $\pi_{1,k}^{\mathrm{ar}}(X \setminus \mathbf{t})$ respectively.

If $X = \mathbb{P}_k^1$ and $\mathbf{t} = \{t_1, ..., t_r\} \in \mathcal{U}_r(k)$, we write $M_{k,\mathbf{t}}$, $\pi_{k,\mathbf{t}}^{\mathrm{alg}}$, $\pi_{k,\mathbf{t}}^{\mathrm{ar}}$ instead of $M_{k,X,\mathbf{t}}$, $\pi_{1,k}^{\mathrm{alg}}(X \setminus \mathbf{t})$, $\pi_{1,k}^{\mathrm{ar}}(X \setminus \mathbf{t})$. In particular, we have the fundamental short exact sequence from Galois theory

$$1 \longrightarrow \pi_{k,\mathbf{t}}^{\mathrm{alg}} \longrightarrow \pi_{k,\mathbf{t}}^{\mathrm{ar}} \underset{s}{\longrightarrow} \Gamma_k \longrightarrow 1 \,.$$

which splits since $\mathbb{P}^1(k) \neq \emptyset$. By Riemann Existence Theorem, $\pi_{k,\mathbf{t}}^{\mathrm{alg}}$ is the profinite completion of the group defined by the generators $\gamma_{t_1}, ..., \gamma_{t_r}$ with the single relation $\gamma_{t_1} \cdots \gamma_{t_r} = 1$ ($\gamma_{t_1}, ..., \gamma_{t_r}$ arise from a standard topological bouquet of loops around the branch points for $\mathbb{P}_k^1 \setminus \mathbf{t}$ and, in the following, we will always assume such a topological bouquet has been fixed). For each $t \in \mathbf{t}$, the element γ_t is a *distinguished generator* of the inertia group $I(\mathcal{P}_t|t)$ of some place $\mathcal{P}_t$ of $M_{k,\mathbf{t}}$ above t. By distinguished, we mean the following. There is a group isomorphism between $I(\mathcal{P}_t|t)$ and the group of ${e_t}^2$-roots of 1 in the residue field $\kappa(\mathcal{P}_t) \simeq \overline{k}$: it maps each $\omega \in I(\mathcal{P}_t|t)$ to $\frac{\omega(u_t)}{u_t}$ mod $\mathcal{P}_t$ where u_t is an uniformizing parameter for $\mathcal{P}_t$. Then γ_t is the preimage of ζ_{e_t} via this isomorphism. The action of Γ_k on $\pi_{k,\mathbf{t}}^{\mathrm{alg}}$ has the following property [V99] lemma 2.8.

Lemma 5.5 (Branch cycle argument) *For any $\sigma \in \Gamma_k$, $t \in \mathbf{t}$, ${}^{s(\sigma)}\gamma_t$ is conjugate in $\pi_{k,\mathbf{t}}^{\mathrm{alg}}$ to $\gamma_{\sigma(t)}^{\chi(\sigma)}$ where $\chi : \Gamma_k \to \hat{\mathbb{Z}}$ denotes the cyclotomic character.*

A classical consequence of lemma 5.5 is that many branch points are necessary to realize regularly cyclic groups over number fields (for instance at least $\phi(n)$ branch points are necessary for $\mathbb{Z}/n\mathbb{Z}$ over $\mathbb{Q}$, where ϕ is the Euler function). We will re-use lemma 5.5 to obtain a similar conclusion but in a non abelian context. This will be a key ingredient of our proof (*cf.* lemma 5.7).

A k G-cover is a pair (f, α) where $f : X \to \mathbb{P}_k^1$ is an algebraic Galois cover and $\alpha : \mathrm{Aut}(f) \to G$ is a group isomorphism; k G-extensions $(K/k(T), \alpha)$ are defined similarly. We often drop the reference to α in the following.

One can attach to any G-cover f defined over an algebraically closed field $\overline{k}$ of characteristic 0 three invariants : the Galois group G, the branch point divisor $\mathbf{t} = \{t_1, ..., t_r\} \in \mathcal{U}_r(\overline{k})$ and, for each $t \in \mathbf{t}$, the corresponding inertia canonical conjugacy class C_t. This last invariant can be defined as follows : consider the restriction $\gamma_t|_{\overline{k}(X)}$ and its conjugates in $\mathrm{Gal}(\overline{k}(X)|\overline{k}(T))$. They are called the *distinguished inertia generators* of $\overline{k}(X)/\overline{k}(T)$ above t and they form a conjugacy class which is the class C_t.

Let G be a finite group, $\mathbf{t} = \{t_1, ..., t_r\} \in \mathcal{U}_r(k)$ and $\mathbf{C} = (C_t)_{t\in\mathbf{t}}$ an r-tuple of non trivial conjugacy classes of G. The following categories are classically equivalent :

- (C1) the category of k-G-covers with invariants G, $\mathbf{t}$, $\mathbf{C}$.
- (C2) the category of k-G-extensions with invariants G, $\mathbf{t}$, $\mathbf{C}$.
- (C3) the category of group epimorphisms $\Phi : \pi_{k,\mathbf{t}}^{\mathrm{ar}} \twoheadrightarrow G$ such that $(C_{\Phi(\gamma_1)}^G, ..., C_{\Phi(\gamma_r)}^G) = \mathbf{C}$ and $\Phi(\pi_{k,\mathbf{t}}^{\mathrm{alg}}) = G$, where C_g^G is the conjugacy class of g in G.

In the category (C1) a morphism from $(f_1 : X_1 \to \mathbb{P}_k^1, \alpha_1)$ to $(f_2 : X_2 \to \mathbb{P}_k^1, \alpha_2)$ is the data of a morphism of covers $u : f_1 \to f_2$ such that for any $g \in \mathrm{Aut}(f_1)$ we have $\alpha_2(u \circ g \circ u^{-1}) = \alpha_1$; in the

[2] here, e_t denotes the profinite order of the cyclic group $I(\mathcal{P}_t|t)$

category (C3), a morphism from Φ_1 to Φ_2 is an inner automorphism $i_g \in \mathrm{Inn}(G)$ such that $i_g \circ \Phi_1 = \Phi_2$.

The usual notions of field of moduli and field of definition can be easily described in the category (C3). Indeed, let $f : X \to \mathbb{P}^1_{\overline{k}}$ be a $\overline{k}$ G-cover corresponding to $\Phi_f : \pi^{\mathrm{alg}}_{k,\mathbf{t}} \twoheadrightarrow G$ then

- **(fod)** k is a field of definition for f if the two following equivalent conditions are fulfilled :
(i) There exists a k G-cover f_k such that $f \simeq f_k \times_k \overline{k}$.
(ii) $\Phi_f : \pi^{\mathrm{alg}}_{k,\mathbf{t}} \twoheadrightarrow G$ extends to a group epimorphism $\Phi_{f,k} : \pi^{\mathrm{ar}}_{k,\mathbf{t}} \twoheadrightarrow G$.

- **(fom)** k is the field of moduli for f (relatively to the extension $\overline{k}/k$) if the two following equivalent conditions are fulfilled :
(i) $k = \overline{k}^{M_{f,k}}$ where $M_{f,k} = \{\sigma \in \Gamma_k \mid f \simeq {}^{\sigma}f\} \subset \Gamma_k$ is the closed subgroup (of finite index) of Γ_k fixing the isomorphism class of f.
(ii) There exists an application $h_{f,k} : \Gamma_k \to G$ such that $\Phi_f({}^{s(\sigma)}\gamma) = h_{f,k}(\sigma) \cdot \Phi_f(\gamma) \cdot (h_{f,k}(\sigma))^{-1}$, for all $\gamma \in \pi^{\mathrm{alg}}_{k,\mathbf{t}}$, $\sigma \in \Gamma_k$. (Observe that the map $h_{f,k}$ depends on the section $s : \Gamma_k \hookrightarrow \pi^{\mathrm{ar}}_{k,\mathbf{t}}$ but the notion of field of moduli does not).

Clearly (fod) implies (fom) but the converse is false in general. One can define a cohomological obstruction $[\omega_{f,k}] \in \mathrm{H}^2(k, Z(G))$ for a G-cover f with group G and field of moduli k to be defined over k [DDo97] : with the notation above, the map

$$\begin{array}{rccc} \overline{\phi}_{f,k} : & \Gamma_k & \to & G/Z(G) \\ & \sigma & \to & h_{f,k}(\sigma) \ [\mathrm{mod\ Z}(G)] \end{array}$$

is a well-defined group morphism, which only depends on s and not on the particular representative $h_{f,k}$. Considering $Z(G)$ as a trivial Γ_k-module, the cochain

$$\begin{array}{rccc} \omega_{f,k} : & \Gamma_k \times \Gamma_k & \to & Z(G) \\ & (\sigma, \tau) & \to & h_{f,k}(\sigma\tau)^{-1} h_{f,k}(\sigma) h_{f,k}(\tau) \end{array}$$

defines a class $[\omega_{f,k}] \in \mathrm{H}^2(k, Z(G))$ which does not depend on s. Classically, $[\omega_{f,k}] \in \mathrm{H}^2(k, Z(G))$ is 0 in $\mathrm{H}^2(k, Z(G))$ iff f is defined over k and this, in turn, is equivalent to the existence of a group morphism $\phi_{f,k} : \Gamma_k \to G$ making the following diagram commute

$$\begin{array}{ccccccccc} 1 & \longrightarrow & Z(G) & \longrightarrow & G & \longrightarrow & G/Z(G) & \longrightarrow & 1 \\ & & & & & \nwarrow^{\exists \phi_{f,k}} & \uparrow{\scriptstyle \overline{\phi}_{f,k}} & & \\ & & & & & & \Gamma_k & & \end{array}$$

(this occurs in particular if $Z(G) = \{1\}$ or if $Z(G)$ is a direct factor of G). We call $[\omega_{f,k}] \in \mathrm{H}^2(k, Z(G))$ the *cohomological obstruction* for f to be defined over k.

5.1.2 Hurwitz spaces and modular towers

5.1.2.1 Notations for Hurwitz spaces

Given a finite group G and an integer $r \geq 3$, denote by $\psi_{r,G} : \mathcal{H}_{r,G} \to \mathcal{U}_r$ the coarse moduli space (fine assuming $Z(G) = \{1\}$) for the category of G-covers of $\mathbb{P}^1$ with group G and r branch points, where $\psi_{r,G}$ is the application which to a given isomorphism class of G-covers associates its branch point set. For any r-tuple $\mathbf{C} = (C_1, ..., C_r)$ of non trivial conjugacy classes of G let $\mathcal{H}_{r,G}(\mathbf{C})$ be the corresponding *Hurwitz space* [FV91], that is the union of all irreducible components of $\mathcal{H}_{r,G}$ parametrizing the isomorphism classes of G-covers with r branch points, group G and inertia canonical invariant $\mathbf{C}$. We will freely use the general theory of Hurwitz spaces (*cf.* for instance [FV91], [V99],

[W98], *etc.*).

In particular, given a field k of characteristic 0, $\mathcal{H}_{r,G}(k)$ corresponds to G-covers with field of moduli k and we write $\mathcal{H}_{r,G}(k)^{noob}$ for the k-non obstruction locus that is, the (possibly empty) subset of $\mathcal{H}_{r,G}(k)$ corresponding to G-covers defined over k (equivalently, to regular realizations of G over k). The construction of Hurwitz spaces being functorial in G, any complete projective system of finite groups and tuples of conjugacy classes $((G_{n+1}, \mathbf{C}_{n+1}) \twoheadrightarrow (G_n, \mathbf{C}_n))_{n\geq 0}$ defines a tower of Hurwitz spaces $\underline{\mathcal{H}} = (\mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r_n,G_n}(\mathbf{C}_n))_{n\geq 0}$ (where r_n is the length of the tuple $\mathbf{C}_n$, $n \geq 0$). As we did for Hurwitz spaces, we can define the k-non obstruction locus $\underline{\mathcal{H}}(k)^{noob}$ of the tower $\underline{\mathcal{H}}$ to be the set of all projective systems of k-rational points corresponding to regular realizations of the profinite group $\varprojlim G_n$ over k or, equivalently, to projective systems of G-covers defined over k and with compatible models over k. In general, $\underline{\mathcal{H}}(k)^{noob}$ is strictly contained in $\varprojlim \mathcal{H}_{r_n,G_n}(k)^{noob}$ (*cf.* §5.3.1).

5.1.2.2 Modular towers

In the following, given a short exact sequence of profinite groups $1 \to P \to G \to G_0 \to 1$ with G_0 a finite group and P a finitely generated pro-p-group, we will write $P_0 = P$, $P_1 = P_0^p[P_0, P_0]$, ..., $P_{n+1} = P_n^p[P_n, P_n]$, *etc.* for the Frattini series of P, which constitutes a fundamental system of open neighborhoods of 1 in P by [RZ00], proposition 2.8.13. We will also write G_n for the characteristic quotient G/P_n and $s_n : G \twoheadrightarrow G_n$ for the canonical projection, $n \geq 0$.

An important special case of the above situation is this. Fix a finite group G_0 and a prime number p dividing $|G_0|$. Let $G := {}_p\tilde{G}_0$ be the universal p-Frattini cover of G_0 [F95a] §II.A, II.B. Then the kernel P of $G \twoheadrightarrow G_0$ is a free pro-p group of finite rank. In this special case, we will write ${}_p^n\tilde{G}$ instead of G_n, $n \geq 0$. We thus obtain a complete projective system of finite groups $({}_p^{n+1}\tilde{G} \to {}_p^n\tilde{G})_{n\geq 0}$ with the property that for any p'-conjugacy class (that is, of prime-to-p order, where we define the order of a conjugacy class as the order of any element in it) C_n of ${}_p^n\tilde{G}$ there exists a unique conjugacy class C_{n+1} of ${}_p^{n+1}\tilde{G}$ above C_n with the same order as C_n([F95a], lemma 3.7). Assume furthermore that G is p-perfect, that is generated by p'-elements, then any r-tuple $\mathbf{C} = (C_1, ..., C_r)$ of non trivial p'-conjugacy classes of G such that the set - we call the *straight Nielsen class* and denote by $\mathrm{sni}(\mathbf{C})$ - of all $g_1, ..., g_r \in G$ verifying (i) $G =< g_1, ..., g_r >$, (ii) $g_1 \cdots g_r = 1$ and (iii) $g_i \in C_i$ is non empty defines a unique projective system of tuples $(\mathbf{C}_n)_{n\geq 0}$ and the corresponding system of Hurwitz spaces

$$(\mathcal{H}_{r,{}_p^{n+1}\tilde{G}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r,{}_p^n\tilde{G}}(\mathbf{C}_n))_{n\geq 0}$$

is called *the modular tower associated with the data* $(G, \mathbf{C}, p)$. These objects were introduced and studied by M. Fried ([F95a], [FK97], [BF02], [D04] *etc.*) and were the starting point of this work.

5.2 Proof of theorem 5.1

For simplicity, we only give here the proof for the case $k = \mathbb{Q}$, leaving to the reader the details of the generalization to the number field case. As for the finite field case, we make some comments in 5.2.3.

We first explain how the general case for which P is a pronilpotent projective group of finite rank can be reduced to the case P is a free pro-p group of finite rank. If P is a pronilpotent group, it can be written as the direct product of its Sylow subgroups : $P \simeq \prod_{p|\,|P|} S_p$ and, P being projective, each group S_p is a free pro-p group [RZ00] proposition 7.6.7 and corollary 7.7.6, $(p|\,|P|)$. As a result, considering the characteristic subgroup $S'_p = \prod_{p'|\,|P|, p'\neq p} S_{p'}$ of P, one gets the quotient short exact

sequence of profinite groups :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P & \longrightarrow & G & \longrightarrow & G_0 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & S_p & \longrightarrow & G/S_p' & \longrightarrow & G_0 & \longrightarrow & 1 \end{array}$$

So, it is enough to consider the case when P is a free pro-p group[3].

The proof of theorem 5.1 then follows from the two following lemmas.

Lemma 5.6 *There is no regular realization of G over $k(T)$ with only inertia groups of finite order.*

Lemma 5.7 *There is no regular realization of G over $k(T)$ with an inertia group of infinite order.*

5.2.1 Proof of lemma 5.6

Let $K/\mathbb{Q}(T)$ be a regular Galois extension with group G and only inertia groups of finite order. Since P is torsion free the extension K/K^P is unramified and the places which ramify in $K/\mathbb{Q}(T)$ are those which ramify in $K^P/\mathbb{Q}(T)$, in particular there are only a finite number - say r - of such places. Let $\mathbf{t} \in \mathcal{U}_r(k)$ be the branch point divisor of $K/\mathbb{Q}(T)$ and $\mathbf{C} = (C_1, ..., C_r)$ the corresponding canonical inertia invariant. Our proof now generalizes a reduction argument of [F95b] for the prodihedral groups.

The characteristic subgroup $[P, P]$ being normal in G, the regular extension $K^{[P,P]}/\mathbb{Q}(T)$ is Galois with invariants $\overline{G} := G/[P, P]$, $\overline{\mathbf{C}} := (\overline{C}_1, ..., \overline{C}_r)$, $\mathbf{t}$ (where $\overline{C}_i$ denotes the image of C_i in $G \twoheadrightarrow G/[P, P]$). Since P is a free pro-p group of finite rank ρ, $P^{ab} := P/[P, P]$ is a free abelian pro-p group of rank ρ that is, [RZ00], theorem 4.3.4, $P^{ab} \simeq \mathbb{Z}_p^\rho$ and, as a result, the nth term of the Frattini series of P^{ab} is $(P^{ab})_n = p^n P^{ab}$, $n \geq 0$. The tower of regular G-extensions $\mathbb{Q}(T) < K^{(P^{ab})_0} < K^{(P^{ab})_1} < ... < K^{(P^{ab})_n^{ab}} < K^{(P^{ab})_{n+1}} < ...$ corresponds to a tower of $\mathbb{Q}$-G-covers $... \to X_{n+1} \to X_n \to ... \to X_0 \to \mathbb{P}^1_{\mathbb{Q}}$. Let $k/\mathbb{Q}$ be a finite extension such that $X_0(k) \neq \emptyset$ then, $X_n \times_{\mathbb{Q}} k \to X_0 \times_{\mathbb{Q}} k$ being an unramified G-cover defined over k with group $P^{ab}/(P^{ab})_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^\rho$, it comes from an unramified G-cover $A_n \to \mathrm{Jac}(X_0 \times_{\mathbb{Q}} k)$ defined over k with group $(\mathbb{Z}/p^n\mathbb{Z})^\rho$. Thus, since $\mathrm{End}(A_n)$ is torsion free, A_n carries a k-torsion point of order p^n. Let $\mathcal{Q}$ be a place of k not dividing p where $\mathrm{Jac}(X_0 \times_{\mathbb{Q}} k)$ has good reduction then, A_n and $\mathrm{Jac}(X_0 \times_{\mathbb{Q}} k)$ being isogenous, their reductions modulo $\mathcal{Q} : \overline{A_n}$ and $\overline{\mathrm{Jac}(X_0 \times_{\mathbb{Q}} k)}$ have the same number of $\mathbb{F}_{q^m}$-points (where $[k : \mathbb{Q}] = m$). Consequently, the reduction modulo $\mathcal{Q}$ map being injective on the p^n-torsion subgroup of A_n, p^n divides $|\overline{\mathrm{Jac}(X_0 \times_{\mathbb{Q}} k)}(\mathbb{F}_{q^m})|$ for all $n \geq 1$: a contradiction. □

5.2.2 Proof of lemma 5.7

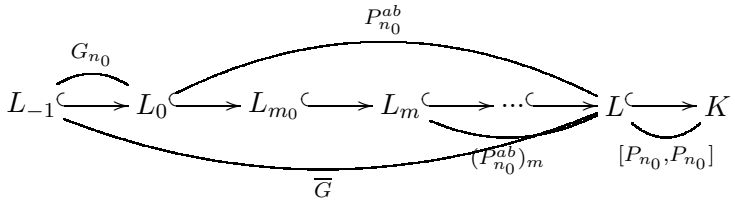
Assume there exists a regular Galois extension $K/\mathbb{Q}(T)$ with group G and an inertia group $< g >$ of infinite order. Denote by α the order of the element $s(g) \in G_0$ (so, in particular, $g^\alpha \in P$) and by $n_0 \geq 0$ the smallest integer such that $g^\alpha \in P_{n_0} \setminus P_{n_0+1}$. Consider the quotient short exact sequence of profinite groups :

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P_{n_0} & \longrightarrow & G & \overset{s_{n_0}}{\longrightarrow} & G_{n_0} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & P_{n_0}^{ab} & \longrightarrow & G/[P_{n_0}, P_{n_0}] & \longrightarrow & G_{n_0} & \longrightarrow & 1 \end{array}$$

[3]Note also that if at least two distinct primes divide the order of the pronilpotent group P, then one is different from the characteristic q of k in the finite field situation, so our reduction argument shows that the assumption on q in this case is just that it does not divide $|G_0|$.

By [RZ00], corollary 3.6.4, P_{n_0} is a free pro-p group of finite rank - say ρ. Thus $P_{n_0}^{ab}$ is a free abelian pro-p group of rank ρ that is, $P_{n_0}^{ab} \simeq \mathbb{Z}_p^\rho$ (and thus $(P_{n_0}^{ab})_m \simeq (p^m\mathbb{Z}_p)^\rho$, $m \geq 0$).

Now, set $L = K^{[P_{n_0},P_{n_0}]}$, $L_{-1} = \mathbb{Q}(T)$ and $L_m = L^{(P_{n_0}^{ab})_m}$, $m \geq 0$. For any place $\mathcal{P}$ of L, denote by $\mathcal{P}_m$ the restriction of $\mathcal{P}$ to L_m and by $I(\mathcal{P}|\mathcal{P}_m)$ the corresponding inertia group , $m \geq -1$. Finally, set $\overline{G} := G/[P_{n_0}, P_{n_0}]$. The following diagram of regular Galois extensions sums up the situation,



Since $g^\alpha \in P_{n_0}$ is non zero modulo P_{n_0+1} and that $[P_{n_0}, P_{n_0}] < P_{n_0+1}$, its image in $G \twoheadrightarrow \overline{G}$ is non zero that is, of infinite order and so is the image of g. But the image of g modulo $[P_{n_0}, P_{n_0}]$ generates an inertia group of L/L_{-1} and, L_0/L_{-1} being finite, the Galois extension L/L_0 is necessarily ramified. More precisely, if $\mathcal{P}$ is a place of L/L_{-1} with inertia group $I(\mathcal{P}|\mathcal{P}_{-1}) =< g >$, we deduce from the canonical short exact sequence

$$1 \to I(\mathcal{P}|\mathcal{P}_0) \to I(\mathcal{P}|\mathcal{P}_{-1}) \to I(\mathcal{P}_0|\mathcal{P}_{-1}) \to 1$$

that $I(\mathcal{P}|\mathcal{P}_0) =< g^\alpha >$. Write $g_m := g|_{L_m}$, $m \geq -1$ and let $m_0 \geq 0$ be the smallest integer $m \geq 0$ such that $g_m^\alpha \neq 0$. Finally, for all $m \geq m_0$, denote by $\Psi(m)$ the set of all integers $1 \leq l \leq p^{m-m_0} - 1$ such that $(l, p|G_{n_0}|) = 1$ (where p^{m-m_0} is, by definition of m_0, the order of g_m^α). Then, by lemma 5.5, for any $m \geq m_0$, $l \in \Psi(m)$, the element g_m^l is conjugate to a distinguished inertia generator of L_m/L_{-1}.

But an element of $P_{n_0}^{ab}/(P_{n_0}^{ab})_m$ has at most $|G_{n_0}|$ conjugates in $\overline{G}/(P_{n_0}^{ab})_m$. Indeed, consider the short exact sequence

$$1 \to P_{n_0}^{ab}/(P_{n_0}^{ab})_m \to \overline{G}/(P_{n_0}^{ab})_m \xrightarrow{\pi} G_{n_0} \to 1$$

Given any set-theoretic section $\sigma : G_{n_0} \to \overline{G}/(P_{n_0}^{ab})_m$ of π, any element $u \in \overline{G}/(P_{n_0}^{ab})_m$ can be written in a unique way $u = \sigma(\pi(u))z_u$ with $z_u \in P_{n_0}^{ab}/(P_{n_0}^{ab})_m$, which implies that $uzu^{-1} = \sigma(\pi(u))z\sigma(\pi(u))^{-1}$ for any $z \in P_{n_0}^{ab}/(P_{n_0}^{ab})_m$.

In particular, $g_m^{\alpha l}$ has at most $|G_{n_0}|$ conjugates in $\overline{G}/(P_{n_0}^{ab})_m$, $l \in \Psi(m)$. So given r distinct integers $l_1, ..., l_r \in \Psi(m)$, if $g_m^{l_1}, ..., g_m^{l_r}$ are conjugate in $\overline{G}/(P_{n_0}^{ab})_m$ then so are the $g_m^{\alpha l_1}, ..., g_m^{\alpha l_r}$, which are all distinct by definition of $\Psi(m)$. Conclude : $r \leq |G_{n_0}|$. As a result there are at least $|\Psi(m)|/|G_{n_0}|$ places of L_{-1} that ramify in L_m/L_{-1} with a distinguished inertia generator conjugate to an element of the form g_m^l, $l \in \Psi(m)$. Such places also ramify in L_{m_0}/L_{-1}. Indeed, the canonical image of g_m^l in $\overline{G}/(P_{n_0}^{ab})_{m_0}$ is $g_{m_0}^l$, which has the same order as g_{m_0}, which, in turn, is non zero (since, by definition of m_0, $g_{m_0}^\alpha$ is non zero) , $l \in \Psi(m)$. But $\lim_{m\to+\infty} |\Psi(m)|/|G_{n_0}| = +\infty$: a contradiction. □

5.2.3 Comments about the finite field case

The proof of lemma 5.6 relies on a reduction modulo $\mathcal{Q}$ argument and, actually, it also works for any finite field of characteristic not dividing $p|G_0|$; its adjustment is straightforward. Likewise, in lemma 5.7, the obstruction to the regular realization of G over $k(T)$ rises from the lack of roots of 1 in k and, as a result, lemma 5.7 also works for any field k of characteristic 0 such that $[k \cap \mathbb{Q}^{ab} : \mathbb{Q}]$ is finite or any finite field of characteristic $q \neq |G|$. This yields the finite field assertion of theorem 5.1.

One could ask what occurs for the missing characteristics. The following theorem shows - at least for the characteristics p dividing $|P|$ - this situation is quite different.

Theorem 5.8 *Let G be a finite group, p a prime dividing $|G_0|$ and ${}_p\tilde{G}_0$ the universal p-Frattini cover of G_0. Then, given a finite field F of characteristic p, any regular realization of G_0 over F yields a regular realization of ${}_p\tilde{G}_0$ over F.*

Proof. Starting from a regular realization $N_0/F(T)$ of G_0, we construct inductively a projective system $(N_n/F(T))_{n\geq 0}$ of regular Galois extension $N_n/F(T)$ with group ${}_p^n\tilde{G}$, $n \geq 0$. So, assume $N_n/F(T)$ exists, corresponding to a group epimorphism $\phi_n : \Gamma_{F(T)} \twoheadrightarrow {}_p\tilde{G}_n$ and observe that the canonical projection ${}_p\tilde{G}_{n+1} \twoheadrightarrow {}_p\tilde{G}_n$ is a Frattini cover with elementary p-abelian kernel $P_n/P_{n+1} \simeq (\mathbb{Z}/p\mathbb{Z})^{r_n}$ for some $r_n \geq 1$. The corresponding embedding problem

$$\begin{array}{ccccccccc} & & & & & & \Gamma_{F(T)} & & \\ & & & & & & \downarrow{\scriptstyle \phi_n} & & \\ 1 & \longrightarrow & (\mathbb{Z}/p\mathbb{Z})^{r_n} & \longrightarrow & {}_p\tilde{G}_{n+1} & \longrightarrow & {}_p\tilde{G}_n & \longrightarrow & 1 \end{array}$$

is thus a geometric Frattini embedding problem with p-group kernel. Consequently, by [MMa99], theorem IV.8.3, it has a solution $\phi_{n+1} : \Gamma_{F(T)} \twoheadrightarrow {}_p\tilde{G}_{n+1}$. And, by [MMa99], proposition IV.5.1, any solution is a geometric proper solution. So take for N_{n+1} the fixed field of $\ker(\phi_{n+1})$ in $F(T)^s$ (which is regular over F). □

In terms of Hurwitz spaces, theorem 5.1 means that for any complete projective system of finite groups and tuples of conjugacy classes $((G_{n+1}, \mathbf{C}_{n+1}) \twoheadrightarrow (G_n, \mathbf{C}_n))_{n\geq 0}$ such that $G = \varprojlim G_n$, the k-non obstruction locus of the corresponding tower of Hurwitz spaces $\underline{\mathcal{H}} = (\mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r_n,G_n}(\mathbf{C}_n))_{n\geq 0}$ is empty. We wonder now if $\varprojlim \mathcal{H}_{r,G_n}(k)$ is empty as well. This fact (theorem 5.2) will appear as a corollary of theorem 5.1 and theorem 5.3, which we prove in the following section.

5.3 Projective system of rational points

The aim of this section is to prove theorem 5.3. We divide it into two parts. In §5.3.1, we explain how to generalize to a projective system of $\overline{k}$-G-covers the classical cohomological obstruction $[\omega_{f,k}] \in \mathrm{H}^2(k, Z(G))$ for a $\overline{k}$-G-cover f with group G and field of moduli k to be defined over k. We then apply these results to reduce the proof of theorem 5.3 (when P is a free pro-p group of finite rank) to a group theoretical verification. We give the proof for a field k of characteristic 0. Replacing $\pi_{k,\mathbf{t}}^{\mathrm{alg}}$, $\pi_{k,\mathbf{t}}^{\mathrm{ar}}$ by their tame analogues $\pi_1^{\mathrm{tame}}(\mathbb{P}^1_{\overline{F}} \setminus \mathbf{t})$, $\pi_1^{\mathrm{tame}}(\mathbb{P}^1_F \setminus \mathbf{t})$, the proof of theorem 5.3 remains unchanged for a field k of characteristic $q > 0$ not dividing $|G_0|$. In §5.3.2.2, we show how to extend theorem 5.3 to the case P is a pronilpotent projective group of finite rank with only finitely many rank 1 p-Sylow subgroups.

5.3.1 The field of moduli obstruction

5.3.1.1 Notation

Let $(G_{n+1} \twoheadrightarrow G_n)_{n\geq 0}$ be a complete projective system of finite groups and $G := \varprojlim G_n$. For each $n \geq 0$, denote by $s_n : G \twoheadrightarrow G_n$ the canonical projection and by P_n its kernel. Given a field k of characteristic 0, any regular Galois extension $K/\overline{k}(T)$ with group G and field of moduli k yields a projective system $(f_n)_{n\geq 0}$ of $\overline{k}$-G-covers f_n with group G_n and field of moduli k. Indeed, if $K/\overline{k}(T)$ has field of moduli contained in k then so do the f_n, $n \geq 0$. Conversely, if for each $n \geq 0$, f_n has field of moduli contained in k, for each $\sigma \in \Gamma_k$ the set of $\overline{k}$-isomorphisms $f_n \simeq^{\sigma} f_n$ being non-empty and finite, there exists a compatible choice $(\chi_{\sigma,n})_{n\geq 0}$ of $\overline{k}$-isomorphisms $\chi_{\sigma,n} : f_n \to {}^{\sigma}f_n$, which implies that $K/\overline{k}(T)$ also has field of moduli k.

For each $n \geq 0$, let $\mathbf{t}_n \in \mathcal{U}_{r_n}(k)$ be the branch point divisor of f_n and $\Phi_n : \pi_{k,\mathbf{t}_n}^{\mathrm{alg}} \twoheadrightarrow G_n$ the

corresponding group epimorphism. We get the commutative diagrams

$$\begin{array}{ccc} \pi^{\mathrm{alg}}_{k,\mathbf{t}_{n+1}} & \xrightarrow{e_n} & \pi^{\mathrm{alg}}_{k,\mathbf{t}_n} \\ {\scriptstyle \Phi_{n+1}}\downarrow & & \downarrow{\scriptstyle \Phi_n} \\ G_{n+1} & \twoheadrightarrow & G_n \end{array}$$

where $e_n : \pi^{\mathrm{alg}}_{k,\mathbf{t}_{n+1}} \twoheadrightarrow \pi^{\mathrm{alg}}_{k,\mathbf{t}_n}$ is the canonical restriction epimorphism defined by the Galois extensions $\overline{k}(T) < M_{k,\mathbf{t}_n} < M_{k,\mathbf{t}_{n+1}}$, $n \geq 0$ (see §5.1.1 for the notation).

5.3.1.2 Projective system of splitting morphisms

Next, considering the projective system of fundamental short exact sequences

$$\begin{array}{ccccccccc} & & & & \overset{s_{\mathbf{t}_{n+1}}}{\curvearrowleft} & & & & \\ 1 & \longrightarrow & \pi^{\mathrm{alg}}_{k,\mathbf{t}_{n+1}} & \longrightarrow & \pi^{\mathrm{ar}}_{k,\mathbf{t}_{n+1}} & \longrightarrow & \Gamma_k & \longrightarrow & 1 \\ & & {\scriptstyle e_n}\downarrow & & {\scriptstyle e_n}\downarrow & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ & & & & \underset{s_{\mathbf{t}_n}}{\curvearrowleft} & & & & \\ 1 & \longrightarrow & \pi^{\mathrm{alg}}_{k,\mathbf{t}_n} & \longrightarrow & \pi^{\mathrm{ar}}_{k,\mathbf{t}_n} & \longrightarrow & \Gamma_k & \longrightarrow & 1 \end{array}$$

observe that one can take the splitting morphisms $s_{\mathbf{t}_n}$ in such a way that $e_n \circ s_{\mathbf{t}_{n+1}} = s_{\mathbf{t}_n}$, $n \geq 0$. Indeed, set $M = \cup_{n\geq 0} M_{k,\mathbf{t}_n}$ and choose $t_0 \in k$; the Galois extension $M/\overline{k}(T)$ can be embedded into the field of Puiseux series $\overline{k}\{\{T - t_0\}\}$, on which Γ_k acts naturally. This defines a splitting morphism $s : \Gamma_k \to \mathrm{Gal}(M|k(T))$ and so, via the restriction $\mathrm{Gal}(M|k(T)) \twoheadrightarrow \pi^{\mathrm{ar}}_{k,\mathbf{t}_n}$, a compatible system of splitting morphisms $(s_{\mathbf{t}_n} : \Gamma_k \to \pi^{\mathrm{ar}}_{k,\mathbf{t}_n})_{n\geq 0}$. If $k \setminus (k \cap \cup_{n\geq 0}\mathbf{t}_n) \neq \emptyset$ (which, for instance, always occurs if k is uncountable), one can choose $t_0 \in k \setminus (k \cap \cup_{n\geq 0}\mathbf{t}_n)$, embedding then $M/\overline{k}(T)$ into the field of Laurent series $\overline{k}((T - t_0))$ as usual.

Note also that, as a consequence of $s_{\mathbf{t}_n} = e_n \circ s_{\mathbf{t}_{n+1}}$, we have, for any $\gamma \in \pi^{\mathrm{ar}}_{k,\mathbf{t}_{n+1}}$ and $\sigma \in \Gamma_k$

$$e_n(s_{\mathbf{t}_{n+1}}(\sigma)\gamma s_{\mathbf{t}_{n+1}}(\sigma)^{-1}) = s_{\mathbf{t}_n}(\sigma)e_n(\gamma)s_{\mathbf{t}_n}(\sigma)^{-1}$$

5.3.1.3 Projective system of cohomological obstructions

Now, with the notation of 5.1.1, if k is the field of moduli of f_n, $n \geq 0$ then, for any $n \geq 0$, $\sigma \in \Gamma_k$, there exists $h_n(\sigma) := h_{f_n,k}(\sigma) \in G_n$ such that

$$\Phi_n(s_{\mathbf{t}_n}(\sigma)\gamma s_{\mathbf{t}_n}(\sigma)^{-1}) = h_n(\sigma)\Phi_n(\gamma)h_n(\sigma)^{-1},\ \gamma \in \pi^{\mathrm{ar}}_{k,\mathbf{t}_n}$$

Denote by $H_n(\sigma) \subset G_n$ the set of all such elements. It is straightforward that $(H_{n+1}(\sigma) \to H_n(\sigma))_{n\geq 0}$ is a projective system of finite sets ; as they also are non empty the inverse limit $\varprojlim H_n(\sigma)$ is non empty. Let $h : \Gamma_k \to G$ be the map sending σ to $h(\sigma) = (h_n(\sigma))_{n\geq 0} \in \varprojlim H_n(\sigma)$. Write $\overline{\phi}_n : \Gamma_k \to G_n/Z(G_n)$, $\omega_n : \Gamma_k \times \Gamma_k \to Z(G_n)$ and $[\omega_n] \in \mathrm{H}^2(k, Z(G_n))$, $n \geq 0$ for the group morphism, cochains and cohomological classes associated with $h_n : \Gamma_k \to G_n$, $n \geq 0$ (see §5.1.1).

5.3.1.4 The profinite cohomological obstruction

Using the map $h : \Gamma_k \to G$ defined in §5.3.1.3, we can introduce as in §5.1.1

$$\begin{array}{rccl} \overline{\phi} : & \Gamma_k & \to & G/Z(G) \\ & \sigma & \to & h(\sigma)\ [\mathrm{mod}\ Z(G)] \end{array} \quad , \quad \begin{array}{rccl} \omega : & \Gamma_k \times \Gamma_k & \to & Z(G) \\ & (\sigma,\tau) & \to & h(\sigma\tau)^{-1}h(\sigma)h(\tau) \end{array} \quad , \quad [\omega] \in H^2(k, Z(G))$$

As in the finite case, $[\omega] = 0$ in $H^2(k, Z(G))$ iff the morphism $\overline{\phi} : \Gamma_k \to G/Z(G)$ can be lifted to a morphism $\phi : \Gamma_k \to G$. This is equivalent to the existence of $(\Phi_{n,k} : \pi^{\mathrm{ar}}_{k,\mathbf{t}_n} \twoheadrightarrow G_n)_{n\geq 0}$ such that $\Phi_{n,k}|_{\pi^{\mathrm{alg}}_{k,\mathbf{t}_n}} = \Phi_n$ and the following diagrams commute[4]

$$\begin{array}{ccc} \pi^{\mathrm{ar}}_{k,\mathbf{t}_{n+1}} & \xrightarrow{e_n} & \pi^{\mathrm{ar}}_{k,\mathbf{t}_n} \\ {\scriptstyle \Phi_{n+1,k}}\downarrow & & \downarrow{\scriptstyle \Phi_{n,k}} \\ G_{n+1} & \twoheadrightarrow & G_n \end{array} \quad , \quad n \geq 0$$

that is, to the existence of a projective system $(f_{n,k})_{n\geq 0}$ of k-models of the $(f_n)_{n\geq 0}$ which, in turn, define a regular Galois extension $K_k/k(T)$ with group G such that $K_k.\overline{k} = K$. So we call $[\omega] \in H^2(k, Z(G))$ the cohomological obstruction for the projective system of G-covers $(f_n)_{n\geq 0}$ to be defined over k (*as projective system*).

Proposition 5.9 *Assume one of the three following conditions holds :*

(1) $Z(G)$ *is a direct factor in* G.
(2) $[G : Z(G)]$ *is finite.*
(3) $Z(G) \cap P_{n_0} = \{1\}$ *for some* $n_0 \geq 0$.

Then any projective system $(f_n)_{n\geq 0}$ *of* $\overline{k}$*-*G*-covers* f_n *with group* G_n *and field of moduli* k *can be defined (as projective system) over a finite extension* k_0/k. *Furthermore,* k_0/k *can be taken in such a way that* $k = k_0$ *under condition (1),* $[k_0 : k] \leq [G : Z(G)]$ *under condition (2) and* $[k_0 : k] \leq |G_{n_0}|$ *under condition (3).*

Proof. (1) is straightforward. For (2), take for instance $k_0 = \overline{k}^{\ker(\overline{\phi})}$. To prove (3), suppose that $Z(G) \cap P_{n_0} = \{1\}$. Then there is a canonical commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & s_{n_0}(Z(G)) & \longrightarrow & G_{n_0} & \xrightarrow{\pi_{n_0}} & G_{n_0}/Z(G) & \longrightarrow & 1 \\ & & {\scriptstyle \simeq}\uparrow & & {\scriptstyle s_{n_0}}\uparrow & & {\scriptstyle \overline{s}_{n_0}}\uparrow & & \\ 1 & \longrightarrow & Z(G) & \longrightarrow & G & \xrightarrow[\exists\phi]{} & G/Z(G) & \longrightarrow & 1 \\ & & & & & & {\scriptstyle \overline{\phi}}\uparrow & & \\ & & & & & & \Gamma_k & & \end{array}$$

and the class $[s_{n_0} \circ \omega]$ in $\mathrm{H}^2(k, s_{n_0}(Z(G)))$ is the cohomological obstruction for the existence of a group morphism $\phi : \Gamma_k \to G_{n_0}$ such that $\pi_{n_0} \circ \phi = \overline{s}_{n_0} \circ \overline{\phi}$. As a result, setting $k_0 := \overline{k}^{\ker(\overline{s}_{n_0} \circ \overline{\phi})}$ (which is a degree $\leq [G_{n_0} : Z(G)]$ extension of k) one has $[s_{n_0} \circ \omega] = 0$ in $\mathrm{H}^2(k_0, s_{n_0}(Z(G)))$, that is, $s_{n_0} \circ \omega$ is a coboundary and, since by assumption s_{n_0} is injective on $Z(G)$, so is ω : conclude $[\omega] = 0$ in $\mathrm{H}^2(k_0, Z(G))$. □

5.3.1.5 Concluding remark

We end this section by comparing the global cohomological obstruction $[\omega] \in H^2(k, Z(G))$ and the projective system of cohomological obstructions $([\omega_n])_{n\geq 0} \in \varprojlim H^2(k, Z(G_n))$. Clearly, $i \circ \overline{\phi} = \varprojlim \overline{\phi}_n$ where $i : G/Z(G) \hookrightarrow \varprojlim G_n/Z(G_n)$ is the canonical monomorphism (note that $\varprojlim Z(G_n) = Z(G)$).

[4] Given $\phi : \Gamma_k \to G$, for any $n \geq 0$, define $\Phi_{n,k} : \pi^{\mathrm{ar}}_{k,\mathbf{t}_n} \twoheadrightarrow G_n$ by $\Phi_{n,k}(\gamma s_{\mathbf{t}_n(\sigma)}) = \Phi_n(\gamma) s_n \circ \phi(\sigma)$, $(\gamma \in \pi^{\mathrm{ar}}_{k,\mathbf{t}_{n+1}}, \sigma \in \Gamma_k)$. Conversely, given $(\Phi_{n,k} : \pi^{\mathrm{ar}}_{k,\mathbf{t}_n} \twoheadrightarrow G_n)_{n\geq 0}$ define $\phi = \varprojlim \Phi_{n,k} \circ s_{\mathbf{t}_n}$.

Likewise, $\omega = \varprojlim \omega_n$ and $j([\omega]) = ([\omega_n])_{n\geq 0}$ where $j : H^2(k, Z(G)) \to \varprojlim H^2(k, Z(G_n))$ is the canonical morphism. In general j is not injective and non trivial global cohomological obstructions $[\omega]$ lying in the kernel of j correspond to projective systems of $\overline{k}$ G-covers $(f_n)_{n\geq 0}$ such that for each $n \geq 0$ the set $\mathcal{G}_{f_n}(k)$ of all the k-models of f_n is not empty but the projective limit $\varprojlim \mathcal{G}_{f_n}(k)$ is. In terms of Hurwitz spaces, if j is injective then $\underline{\mathcal{H}}(k)^{noob} = \varprojlim \mathcal{H}_{r_n,G_n}(k)^{noob}$.

A sufficient condition for j to be injective is classically given by the Mittag-Leffler property [L02], III.10 for the projective system of 1-cocycles $(\mathrm{C}^1(k, Z(G_{n+1})) \to \mathrm{C}^1(k, Z(G_n)))_{n\geq 0}$. It holds, for instance, when :

- $Z(G) = \{0\}$.
- The morphism $Z(G_{n+1}) \to Z(G_n)$ is an epimorphim and any morphism $\Gamma_k \to Z(G_n)$ can be lifted to a morphism $\Gamma_k \to Z(G_{n+1})$ (for instance if k is of cohomological dimension ≤ 1), $n \geq 0$.
- k is p-closed for each prime p dividing $|Z(G)|$.

5.3.2 Proof of theorem 5.3

We consider first the case when P is a free pro-p group of finite rank and then prove a more general version of theorem 5.3.

5.3.2.1 Two lemmas

In this paragraph, assume P is a free pro-p group of finite rank. By proposition 5.9, in order to prove theorem 5.3 it is enough to prove that $Z(G) \cap P_{n_0} = \{1\}$ for some $n_0 \geq 0$ or that $[G : Z(G)]$ is finite. We consider separately the case $\mathrm{rank}(P) \geq 2$ and $\mathrm{rank}(P) = 1$.

Lemma 5.10 *If* $\mathrm{rank}(P) \geq 2$ *then* $P \cap Z(G) = \{1\}$.

Proof. Assume there exists $x \in P \cap Z(G) \setminus \{1\}$ and let $n_0 \geq 0$ be the smallest integer such that $x \in P_{n_0} \setminus P_{n_0+1}$. Then, according to [RZ00], corollary 3.6.4, P_{n_0} is a free pro-p group of rank $\mathrm{rank}(P_{n_0}) = 1 + [P_0 : P_{n_0}](\mathrm{rank}(P_0) - 1) \geq 2$. And since $x \in P_{n_0}$ is non zero modulo P_{n_0+1}, corollary 7.6.10 of [RZ00] shows there exists $u_2, ..., u_r \in P_{n_0}$ such that the elements $x, u_2, ..., u_r$ freely generate P_{n_0}. The group P_{n_0} can be viewed as the free product $< x > \coprod < u_2, ..., u_r >$ so, according to [RZ00], theorem 9.1.12, for any $y \in P_{n_0} \setminus < x >$ one has $< x > \cap < x^y >= \{1\}$, in particular $x^{-1}x^y \neq 1$: a contradiction since $x \in Z(G)$. □

Lemma 5.11 *If* $\mathrm{rank}(P) = 1$ *and one of the three following conditions is fulfilled*
(i) $[G : Z(G)]$ *is not finite or,*
(ii) $[G, G]$ *is not finite, or*
(iii) for each $n \geq 0$, $p|\,|G_n|$, G_n *is* p*-perfect and the short exact sequences* $1 \to P_n \to G \stackrel{s_n}{\to} G_n \to 1$ *is unsplit,*
then $P \cap Z(G) = \{1\}$.
Furthermore, if $P \cap Z(G) \neq \{1\}$ *then* $[P : Z(G) \cap P]$ *is finite.*

Proof. If $\mathrm{rank}(P) = 1$ and $P \cap Z(G) \neq \{1\}$ then by [RZ00], proposition 2.7.1, $P \cap Z(G) =< x >$ for some $x \in P \setminus \{1\}$ and $[P :< x >]$ is finite. As a result, $[G : Z(G) \cap P] = [G : P][P :< \underline{x} >] = |G_0|[P :< x >]$ is finite and so, $[G : Z(G)]$ is too, whence (i) and the last assertion of lemma 5.11.

As for (ii) and (iii), observe that $P_n \simeq p^n\mathbb{Z}_p$ $(n \geq 0)$ thus, if n_0 is the smallest integer such that $x \in P_{n_0} \setminus P_{n_0+1}$ we have $P_{n_0} =< x >\subset Z(G)$.

Assume (iii). The key ingredient here will be the Schur multiplier $M(G_{n_0})$ of G_{n_0}. Let $\tilde{g}_1, ..., \tilde{g}_r \in G$ be a generating system of G and set $s_{n_0}(\tilde{g}_i) = g_i$, $i = 1, ..., r$. Denote by F_r the pro-free group with r generators $\gamma_1, ..., \gamma_r$. The universal property of F_r allows us to define uniquely two epimorphisms

$u : F_r \twoheadrightarrow G_{n_0}$ and $\tilde{u} : F_r \twoheadrightarrow G$ mapping γ_i to g_i and $\tilde{g}_i$ respectively ; in particular $s_{n_0} \circ \tilde{u} = u$. Set $N = \ker(u)$ then, since P_{n_0} is central, $\tilde{u}([N, F_r]) < [P_{n_0}, G] = \{1\}$. Thus, we obtain the following commutative diagram of short exact sequences

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N \cap [F_r, F_r]/[N, F_r] & \longrightarrow & [F_r, F_r]/[N, F_r] & \longrightarrow & [G_{n_0}, G_{n_0}] & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & P_{n_0} & \longrightarrow & [G, G] & \longrightarrow & [G_{n_0}, G_{n_0}] & \longrightarrow & 1 \end{array}$$

But, by Schur's theorem, $N \cap [F_r, F_r]/[N, F_r] \simeq M(G_{n_0})$ is the Schur multiplier of G_{n_0} and, in particular, it is of finite exponent which implies, P_{n_0} being torsion free, that $N \cap [F_r, F_r]/[N, F_r]$ is contained in the kernel of the middle vertical arrow. Thus, the above commutative diagram yields the following one

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1 & \longrightarrow & [F_r, F_r]/N \cap [F_r, F_r] & \longrightarrow & [G_{n_0}, G_{n_0}] & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & P_{n_0} & \longrightarrow & [G, G] & \longrightarrow & [G_{n_0}, G_{n_0}] & \longrightarrow & 1 \end{array}$$

where the middle vertical arrow maps a finite group onto a non finite group : a contradiction.

Assume (ii). Here, it is the p-part $M(G_{n_0})_p$ of the Schur multiplier $M(G_{n_0})$ of G_{n_0} that we are going to use. Since G_{n_0} is p-perfect, there exists a central extension $1 \to M(G_{n_0})_p \to \widehat{G_{n_0}}^p \xrightarrow{u} G_{n_0} \to 1$ which is universal for central extensions of G_{n_0} with p-group kernel [BF02], §3.6. Consequently, there exists a canonical commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & M(G_{n_0})_p & \longrightarrow & \widehat{G_{n_0}}^p & \xrightarrow{u} & G_{n_0} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & P_{n_0} & \longrightarrow & G & \xrightarrow{s_{n_0}} & G_{n_0} & \longrightarrow & 1 \end{array}$$

so, the fact that $M(G_{n_0})_p$ is of finite exponent and P_{n_0} is torsion free, implies once again that $M(G_{n_0})_p$ is contained in the kernel of the middle vertical arrow. This leads to the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1 & \longrightarrow & \widehat{G_{n_0}}^p/M(G_{n_0})_p & \xrightarrow{\overline{u}} & G_{n_0} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow v & & \| & & \\ 1 & \longrightarrow & P_{n_0} & \longrightarrow & G & \xrightarrow{s_{n_0}} & G_{n_0} & \longrightarrow & 1 \end{array}$$

where $\overline{u}$ becomes an isomorphism, thus providing a section of s_{n_0} : a contradiction. □

Remark 5.12 Proposition 5.9 and lemmas 5.10, 5.11 actually show that the finite extension k_0/k of theorem 5.3 can be taken to be of degree $[k_0 : k] \leq |G_0|$ if $P \cap Z(G) = \{1\}$ and of degree $[k_0 : k] \leq [G : Z(G)]$ else.

In particular, when considering the universal p-Frattini cover ${}_p\tilde{G}_0 \twoheadrightarrow G_0$ of a finite p-perfect group G_0, for each $n \geq 0$ ${}_p\tilde{G}_0 \twoheadrightarrow {}^n_p\tilde{G}$ is the universal p-Frattini cover of ${}^n_p\tilde{G}$ and, as a result, does not split. Consequently, $Z({}_p\tilde{G}_0) \cap P = \{1\}$ and one obtains

Corollary 5.13 [5] *Let G_0 be a finite group and p a prime dividing $|G_0|$ such that G_0 is p-perfect. Then any regular Galois extension $K/\overline{k}(T)$ with group the universal p-Frattini cover ${}_p\tilde{G}_0$ of G_0 is defined over a field extension k_0/k of degree $[k_0 : k] \leq |G_0|$.*

[5] K.Kimura also obtained corollary 5.13, giving furthermore a precise description of the center $Z({}_p\tilde{G})$ of the universal p-Frattini cover of G.

5.3.2.2 Generalization of theorem 5.3

We will show now theorem 5.3 still holds if P *is a pronilpotent projective group of finite rank with only finitely many rank* 1 p*-Sylow subgroups.*

Write $P \simeq \prod_{p|\,|P|} S_p$ as the direct product of its Sylow subgroups. For each $p|\,|P|$, S_p is a free pro-p group of finite rank. From the fact that S_p is a characteristic subgroup of P one has $S_p \lhd G$, $p|\,|P|$, and so $Z(G) \cap P \simeq \prod_{p|\,|P|} Z(G) \cap S_p$. Denote by $\mathcal{S}_1$ the set of those primes $p|\,|P|$ such that $Z(G) \cap S_p = \{1\}$, by $\mathcal{S}_2$ the set of those primes $p|\,|P|$ such that $Z(G) \cap S_p \neq \{1\}$ (which is finite by lemma 5.10) and write $Q_i = \prod_{p \in \mathcal{S}_i} S_p$, $i = 1, 2$. Then,

• $P/Q_2 \cap Z(G/Q_2) = \{1\}$: indeed, for any $g_1 \in Q_1$, if $g_1 g g_1^{-1} g^{-1} \in Q_2$ for all $g \in G$ then, since Q_1 is a characteristic subgroup of P, one also has $g_1 g g_1^{-1} g^{-1} \in Q_1$ for all $g \in G$ and, as a result, $g_1 \in Z(G) \cap Q_1 = \{1\}$.

So, according to proposition 5.9 (3), $K^{Q_2}/\overline{k}(T)$ is defined over a finite extension k_2/k.

• $[G/Q_1 : Z(G/Q_1)]$ is finite : indeed, since $Z(G) \cap Q_1 = \{1\}$, $Z(G)$ is a subgroup of $Z(G/Q_1)$ and, $[G/Q_1 : Z(G/Q_1)]$ divides $[G/Q_1 : (Z(G) \cap P)/Q_1]$ with $[G/Q_1 : (Z(G) \cap P)/Q_1] = |G_0|[P/Q_1 : (Z(G) \cap P)/Q_1] = |G_0|[Q_2 : Z(G) \cap Q_2]$, which is finite by lemma 5.11.

So, according to proposition 5.9 (2), $K^{Q_1}/\overline{k}(T)$ is defined over a finite extension k_1/k.

• Set $k_0 = k_1.k_2$, then $K^{Q_i}/\overline{k}(T)$ is defined over k_0 that is, there exists a regular Galois extension $K_i/k_0(T)$ with group G/Q_i such that $K_i.\overline{k} = K^{Q_i}$ $(i = 1, 2)$. We will show $K_1.K_2/k_0(T)$ is a model for $K/\overline{k}(T)$. We have, $K_1^{Q_2}.\overline{k} = K^P = K_2^{Q_1}.\overline{k}$, so, up to taking a finite extension of k_0, we may assume that $K_1^{Q_2} = K_2^{Q_1}$; denote this field by K_0. Also set

$$\begin{cases} Q_{i,n} = \prod_{p \in \mathcal{S}_i} S_p^n \text{ (where } S_p^n \text{ is the canonical image of } S_p \text{ in } G \twoheadrightarrow G_n,\ n \geq 0) \\ K_{i,n} = K_i^{Q_{i,n}}/k_0(T),\ i = 1, 2 \\ L_n = K_{1,n}.K_{2,n}/k_0(T),\ n \geq 0 \end{cases}$$

Then $K_1.K_2 = \cup_{n \geq 0} L_n$, which implies $K_1.K_2.\overline{k} = K$.

So, we are left to show that $K_1.K_2/k_0(T)$ is regular or, equivalently, that $L_n/k_0(T)$ is regular, $n \geq 0$. This, in turn, is equivalent to $[L_n.\overline{k} : \overline{k}(T)] = [L_n : k_0(T)]$. On the one hand,

$$\begin{aligned} [L_n.\overline{k} : \overline{k}(T)] &= [L_n.\overline{k} : K^P]|G_0| \\ &= [K^{Q_{1,n}}.K^{Q_{2,n}} : K^P]|G_0| \\ &= [K^{Q_{1,n}} : K^P][K^{Q_{2,n}} : K^P]|G_0| \\ &= [K_{1,n} : L_0][K_{2,n} : L_0]|G_0| \end{aligned}$$

and, on the other hand, $[L_n : k_0(T)] = [L_n : L_0]|G_0|$. But, $[K_{i,n} : L_0]|[L_n : L_0]$, $i = 1, 2$, which entails $[K_{1,n} : L_0][K_{2,n} : L_0]|[L_n : L_0]$ (as $(|Q_1/Q_{1,n}|, |Q_2/Q_{2,n}|) = 1$) and so $[K_{1,n} : L_0][K_{2,n} : L_0] = [L_n : L_0]$.

5.4 Applications

As a corollary of theorems 5.1 and 5.3, one obtains theorem 5.2.

Proof of theorem 2. We re-use the reduction argument from the beginning of section 5.2. With the notation there, assume $K/\overline{k}(T)$ is a Galois extension with field of moduli k and group G. Then, for any prime $p|\,|P|$, the subextension $K^{S'_p}/\overline{k}(T)$ is Galois with field of moduli k and group G/S'_p. Since G/S'_p is an extension of the finite group G_0 by the free pro-p group P_p of finite rank, theorem 5.3 implies that $K^{S'_p}/\overline{k}(T)$ is defined over a finite extension k_0/k, hence contradicting theorem 5.1 for G/S'_p. □

As a special case of theorem 5.2, we obtain the following generalization of theorem 6.1 [BF02]

Corollary 5.14 *Let* $\mathbf{C}$ *be a* r*-tuple of non trivial* p'*-conjugacy classes of* G *such that* $\mathrm{sni}(\mathbf{C}) \neq \emptyset$*. Then there is no projective system of* k*-rational points on the modular tower defined by the data* $(G, p, \mathbf{C})$ *for any number field* $k/\mathbb{Q}$*.*

In the following, let $1 \to P \to G \to G_0 \to 1$ be a short exact sequence of profinite groups with G_0 a finite group and P a pronilpotent projective group of finite rank with only finitely many rank 1 p-Sylow subgroups.

5.4.1 Galois realizations of G

Though it is not possible to realize regularly G over a number field, theorem 5.3 yields the following.

Corollary 5.15 *The group* G *can be regularly realized over an algebraic extension* $k/\mathbb{Q}$ *where only a finite number of primes ramify.*

Proof. Let $g_1, ..., g_r \in G$ be a generating system of G such that $g_1 \cdots g_r = 1$ and denote by C_i the conjugacy class of g_i, $i = 1, ..., r$. Set $\mathbf{C} = (C_1, ..., C_r)$ and let $\mathbf{C}_n = (C_{1,n}, ..., C_{r,n})$ be the canonical image of $\mathbf{C}$ in $G_{n,P} := G/\prod_{p\mid |P|}(S_p)_n$ (where, as usual, S_p denotes the p-Sylow of P and $(S_p)_n$ the nth term of its Frattini series, $p\mid |P|$), $n \geq 0$. The projective system of r-tuples $(\mathbf{C}_n)_{n\geq 0}$ defines a tower of Hurwitz spaces

$$\underline{\mathcal{H}} := (\mathcal{H}_{r,G_{n+1,P}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r,G_{n,P}}(\mathbf{C}_n))_{n\geq 0}$$

Consider then any $\mathbf{t} \in \mathcal{U}_r(\mathbb{Q})$ and a projective system of points $(\mathbf{p}_n)_{n\geq 0}$ on $\underline{\mathcal{H}}$ above $\mathbf{t}$. Each $\mathbf{p}_n$ corresponds to a G-cover f_n with invariants $G_{n,P}$, $\mathbf{C}_n$, $\mathbf{t}$ and field of moduli k_n, $n \geq 0$. Denote by $S_{\mathbf{t}}$ the finite set of primes where $\mathbf{t}$ has bad reduction and by $S(|G|)$ the set of all prime divisors of $|G|$. By Beckmann's theorem [Be89], the only primes which may ramify in $k := \cup_{n\geq 0} k_n$ are those from $S_{\mathbf{t}} \cup S(|G|)$ and since all the $(f_n)_{n\geq 0}$ have their field of moduli contained in k, theorem 5.3 implies they all are defined over a finite extension k_0/k. □

Corollary 5.16 *The group* G *is the Galois group of an algebraic extension* K/k *with* $k/\mathbb{Q}$ *an algebraic extension where only a finite number of primes ramify.*

Proof. By corollary 5.15, there exists a regular Galois extension $K/k(T)$ with group G, a finite number of branch points and such that $k/\mathbb{Q}$ is an algebraic extension where only a finite number of primes - $p_1, ..., p_n$ - ramify. In particular, k is contained in the maximal algebraic extension $\mathbb{Q}_{p_1,...,p_n}/\mathbb{Q}$ unramified outside $p_1, ..., p_r$. Let $q \notin \{p_1, ..., p_n\}$ a prime then $\mathbb{Q}_{p_1,...,p_n}(\sqrt{q})/\mathbb{Q}_{p_1,...,p_n}$ is a proper quadratic extension (indeed, q ramifies in $\mathbb{Q}(\sqrt{q})/\mathbb{Q}$!) and $\mathbb{Q}_{p_1,...,p_n}/\mathbb{Q}$ being Galois, deduce from Weissauer's theorem that $\tilde{k} := \mathbb{Q}_{p_1,...,p_n}(\sqrt{q})$ is Hilbertian. Conclude by [S89], §10.6 (the proposition and the theorem) observing that G verifies (iv) of the proposition and, so, the theorem can be applied. □

5.4.2 On the "weak disappearance" of rational points along Hurwitz towers

The spirit of Fried's conjecture is that under suitable assumptions rational points over number fields k disappear beyond a certain level (depending only on d) on towers of Hurwitz spaces (see §5.5.3 for a precise statement). Proposition 5.17 below is a weak form : if one only considers rational points lying above branch points divisor $\mathbf{t} \in \mathcal{U}_r(\overline{\mathbb{Q}})$ with good reduction at some prime q, then they do disappear beyond a certain level.

More precisely, let $(\mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r_n,G_n}(\mathbf{C}_n))_{n\geq 0}$ be the Hurwitz tower previously considered where $\mathbf{C}$ is any tuple of non trivial conjugacy classes of G and $\mathbf{C}_n$ the image of $\mathbf{C}$ in G_n. Define for each prime q the subset $X_r^0(q) \subset \mathcal{U}_r(\overline{\mathbb{Q}})$ of all the divisors $\mathbf{t} \in \mathcal{U}_r(\overline{\mathbb{Q}})$ having good reduction at q and, given a number field k, by $X_r(k, q)$ the $\mathrm{PGL}_2(k)$-orbit of $X_r^0(q)$. Then, let $\mathcal{H}_{n,q}(k) := \mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(k) \cap (\Psi_{r_n,G_n})^{-1}(X_r(k, q))$ be the subset of $\mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(k)$ corresponding to $\overline{\mathbb{Q}}$ G-covers with invariants G_n, $\mathbf{C}_n$, field of moduli k and a branch point divisor lying in $X_r(k, q)$.

Proposition 5.17 *For any prime q not dividing $|G|$ and any integer $d \geq 1$ there exists $n(q,d,\mathbf{C}) \geq 0$ such that*

$$(\star) \quad \bigcup_{[k:\mathbb{Q}]\leq d} \mathcal{H}_{n,q}(k) = \emptyset, \quad n \geq n(q,d,\mathbf{C})$$

Proof. From [W98], corollary 4.2.3 and the remark following it, for any prime q not dividing $|G|$ the tower of Hurwitz spaces $(\mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r_n,G_n}(\mathbf{C}_n))_{n\geq 0}$ has good reduction modulo q. For any $n \geq 0$, let $f_n : X_n \to \mathbb{P}^1_{\mathbb{Q}}$ be a G-cover with invariants G_n, $\mathbf{t}_n$, $\mathbf{C}_n$ and field of moduli a number field k_n such that $[k_n : \mathbb{Q}] = d$, that is a k_n-rational point $\mathbf{p}_n$ on $\mathcal{H}_{r_n,G_n}(\mathbf{C}_n)$. Assume furthermore that for some prime q not dividing $|G|$, $\mathbf{t}_n \in X_r(k_n,q)$ for all $n \geq 0$. Then, up to composing by elements of $\mathrm{PGL}_2(k_n)$, one may assume that $\mathbf{t}_n \in X_r^0(q)$ for all $n \geq 0$. As a result, for any place $\mathcal{Q}_n$ of k_n dividing q, f_n has good reduction modulo $\mathcal{Q}_n$ and reduces to a G-cover $\overline{f}_n$ with invariants G_n, $\overline{\mathbf{t}}_n$, $\mathbf{C}_n$ and field of moduli contained in $\mathbb{F}_{q^d}$, that is a $\mathbb{F}_{q^d}$-rational point $\overline{\mathbf{p}}_n$ on the reduced Hurwitz space $\overline{\mathcal{H}}_{r_n,G_n}(\mathbf{C}_n)$[6]. This produces a projective system of non-empty finite sets

$$(\overline{\mathcal{H}}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1})(\mathbb{F}_{q^d}) \to \overline{\mathcal{H}}_{r_n,G_n}(\mathbf{C}_n)(\mathbb{F}_{q^d}))_{n\geq 0}$$

the projective limit of which should be empty by the finite field version of theorem 5.2 : a contradiction. □

Remark 5.18 About q-adic realizations The same kind of arguments show that for any prime q not dividing $|G|$ and any finite extension $k/\mathbb{Q}_q$, there exists a regular realization of G over k if and only if G is generated by a finite number of elements of finite order the product of which is trivial and, in that case, any regular realization of G over k has a finite branch point divisor with bad reduction at q. Indeed, the only if condition follows from the fact lemma 5.7 holds for any field k of characteristic 0 such that $[k \cap \mathbb{Q}^{ab} : \mathbb{Q}]$ is finite. So any regular realization $K/k(T)$ of G has only inertia groups of finite order. But then, these are the ones of the finite extension $K^P/k(T)$ so there are only finitely many of them. The if condition can be proved using Pop's Half Riemann existence theorem [P94] as in [DDes04]. The last assertion is obtained by reducing modulo q as in the proof of proposition 5.17.

The necessary bad reduction at q of the branch point divisor of any regular realization of G over q-adic fields also suggests that the bad reduction at q of the branch point divisors of known regular realizations of finite groups over q-adic fields might not only be due to the method involved.

A way to tackle Fried's conjecture is to bound the $n(q,d,\mathbf{C})$ uniformly in q. We come back to this in §5.5.2, giving, when $\mathbf{C} = (C_1,...,C_r)$ is a r-tuple of non trivial conjugacy classes of elements of finite order, an effective bound - still depending on q - for $n(q,d,\mathbf{C})$.

5.5 Around Fried's conjecture

We now consider a short exact sequence of profinite groups $1 \to P \to G \to G_0 \to 1$ with G_0 a finite group and P a free pro-p group of finite rank ρ. In §5.5.3, we will deal with the special case of the universal p-Frattini cover $G :=_p \tilde{G}_0$ of a finite p-perfect group G_0.

5.5.1 The abelianization procedure

We formalize here an idea which is reminiscent of the strategy of lemmas 5.6, 5.7. It consists in defining a quotient tower $\underline{\widetilde{\mathcal{H}}}$ of our initial tower $\underline{\mathcal{H}} = (\mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1}) \to \mathcal{H}_{r_n,G_n}(\mathbf{C}_n))_{n\geq 0}$. This tower $\underline{\widetilde{\mathcal{H}}}$, we call the *abelianized tower* of $\underline{\mathcal{H}}$ is easier to handle and, since what is at stake is the disappearance of rational points on $\underline{\mathcal{H}}$ beyond a certain level, it is enough to consider $\underline{\widetilde{\mathcal{H}}}$.

To define $\tilde{\mathcal{H}}$, as in lemmas 5.6, 5.7, write $\overline{G} = G/[P,P]$, $\overline{G}_n = \overline{G}/(P^{ab})_n$, $n \geq 0$ and for any tuple

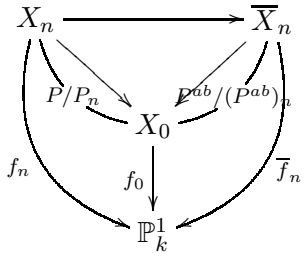
[6] Indeed, if $\mathcal{Q}$ is any place of $\overline{\mathbb{Q}}$ dividing $\mathcal{Q}_n$, identifying $\Gamma_{\mathbb{F}_q}$ with $D_{\mathcal{Q}}/I_{\mathcal{Q}}$ (where $D_{\mathcal{Q}}$ and $I_{\mathcal{Q}}$ respectively denote the decomposition and inertia groups of $\mathcal{Q}$ in $\overline{\mathbb{Q}}/\mathbb{Q}$), the reduction modulo $\mathcal{Q}$ yields a canonical Galois-equivariant isomorphism $c : (\pi^{\mathrm{alg}}_{\mathbb{Q},\mathbf{t}})^{(q')} \simeq (\pi^{\mathrm{alg}}_{\mathbb{F}_q,\mathbf{t}})^{(q')}$ and, if f_n corresponds to a group epimorphism $\Phi_{f_n} : (\pi^{\mathrm{alg}}_{\mathbb{Q},\mathbf{t}})^{(q')} \twoheadrightarrow^n_p \tilde{G}$ then $\overline{f}_n$ corresponds to $\Phi_{f_n} \circ c^{-1}$.

$\mathbf{C}$ of conjugacy classes of G, $\overline{\mathbf{C}}$ for the image of $\mathbf{C}$ in $G \twoheadrightarrow \overline{G}$ and $\overline{\mathbf{C}}_n$ for the image of $\overline{\mathbf{C}}$ in $\overline{G} \twoheadrightarrow \overline{G}_n$ (also assume the length r_n of $\mathbf{C}_n$ is finite), $n \geq 0$. From the canonical commutative diagrams of finite groups (*) one deduces the canonical commutative diagrams of Hurwitz spaces (**)

$$(*)\ \begin{array}{ccc} G_{n+1} & \twoheadrightarrow & \overline{G}_{n+1} \\ \downarrow & & \downarrow \\ G_n & \twoheadrightarrow & \overline{G}_n \end{array}\ ,n \geq 0 \qquad (**)\ \begin{array}{ccc} \mathcal{H}_{r_{n+1},G_{n+1}}(\mathbf{C}_{n+1}) & \twoheadrightarrow & \mathcal{H}_{r_{n+1},\overline{G}_{n+1}}(\overline{\mathbf{C}}_{n+1}) \\ \downarrow & & \downarrow \\ \mathcal{H}_{r_n,G_n}(\mathbf{C}_n) & \twoheadrightarrow & \mathcal{H}_{r_n,\overline{G}_n}(\overline{\mathbf{C}}_n) \end{array}\ ,n \geq 0$$

The right-hand side of diagram (**) is the abelianized tower $\underline{\widetilde{\mathcal{H}}}$ of $\underline{\mathcal{H}}$.

Given a number field k, any G-cover $f_n : X_n \to \mathbb{P}^1_k$ defined over k with invariants G_n, $\mathbf{C}_n$ induces a G-cover $\overline{f}_n : \overline{X}_n \to \mathbb{P}^1_k$ defined over k with invariants $\overline{G}_n$, $\overline{\mathbf{C}}_n$. Denote by $f_0 : X_0 \to \mathbb{P}^1_k$ the quotient of $\overline{f}_n$ modulo $P^{ab}/(P^{ab})_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^\rho$, which is also the quotient of f_n modulo P/P_n.



Reducing ourselves to the abelian cover $\overline{X}_n \to X_0$ will allow us to use the jacobian tool in the etale case.

From now on, assume furthermore $\mathbf{C} = (C_1, ..., C_r)$ *is a* r*-tuple of non trivial conjugacy classes of elements of finite order* and write o_i for the order of any element of $C_{0,i}$, $i = 1, ..., r$. Since P is torsion free, the covers $X_n \to X_0$ and $\overline{X}_n \to X_0$ are etale. Indeed, let C be a conjugacy class of elements of finite order and $g \in C$. Let α be the order of the elements of C_0 then $g^\alpha \in P$. But P is torsion free and g^α is of finite order so, conclude that $g^\alpha = 1$ that is, the elements of C and C_0 have the same order α that is, there is no ramification above X_0.

With $o(\mathbf{C}_0) = \max_{1 \leq i \leq t}\{o_i\}$, one can always find a field extension k_0/k of degree $[k_0 : k] \leq \frac{|G_0|}{o(\mathbf{C}_0)}$ such that $X_0(k_0) \neq \emptyset$. Thus, the abelian etale cover $\overline{X}_n \times_k k_0 \to X_0 \times_k k_0$ with group $P^{ab}/(P^{ab})_n \simeq (\mathbb{Z}/p^n\mathbb{Z})^\rho$ arises from a cartesian diagram

$$\begin{array}{ccc} \overline{X}_n \times_k k_0 & \longrightarrow & A_n \\ \downarrow & \square & \downarrow \\ X_0 \times_k k_0 & \longrightarrow & \mathrm{Jac}(X_0 \times_k k_0) \end{array}$$

where A_n is an abelian variety defined over k_0, isogenous to $\mathrm{Jac}(X_0 \times_k k_0)$ and carrying a k_0-torsion point of order p^n. Conclude

Abelianization procedure conclusion : *Given a number field* k *and an integer* $n \geq 0$*, any G-cover* $f_n : X_n \to \mathbb{P}^1_k$ *defined over* k *with invariants* G_n, $\mathbf{C}_n$ *gives rise to an abelian variety* A_n *defined over an extension* k_0 *of* k *of degree* $[k_0 : k] \leq \frac{|G_0|}{o(\mathbf{C}_0)}$*, isogenous to* $\mathrm{Jac}(X_0 \times_k k_0)$ and carrying a k_0-torsion point of order p^n (where X_0 denotes the quotient of X_n modulo P/P_n).

5.5.2 An effective bound for k-rational points in the non-obstruction locus

We retain the notation and hypotheses above. Denote by $n(q, d, \mathbf{C})^{noob}$ the smallest integer such that $(\star)$ from proposition 5.17 holds with $\mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(k)^{noob}$ replacing $\mathcal{H}_{r_n,G_n}(\mathbf{C}_n)(k)$. Our aim is

to find an explicit bound for $n(q,d,\mathbf{C})^{noob}$. Define $g_{\mathbf{C}_0} = 1 + |G|(\frac{1}{2}\sum_{i=1}^{r}\frac{o_i-1}{o_i} - 1)$ and $\mathcal{N}(g,n) = n + 2g(\sqrt{n}-1) + 2^g$.

Proposition 5.19 *We have* $n(q,d,\mathbf{C})^{noob} \leq \dfrac{\ln(\mathcal{N}(g_{\mathbf{C}_0}, q^{d|G_0|/o(\mathbf{C}_0)}))}{\ln(p)}$.

Proof. Let k be any number field such that $[k:\mathbb{Q}] \leq d$ and $f_n : X_n \to \mathbb{P}^1_k$ be a G-cover defined over k with invariants G_n, $\mathbf{C}_n$, $\mathbf{t}$. Let q be a prime not dividing $p|G_0|$ and such that $\mathbf{t} \in X_r(k,q)$; up to composing f_n by an element of $\mathrm{PGL}_2(k)$, we may assume $\mathbf{t} \in X^0_r(q)$. Let $\mathcal{Q}$ be any place of k_0 dividing q (where k_0 is, as above, a finite extension of k such that $X_0(k_0) \neq \emptyset$ and $[k_0:k] \leq \frac{|G_0|}{o(\mathbf{C}_0)}$). Then X_0 has good reduction at $\mathcal{Q}$ and, consequently, so does $\mathrm{Jac}(X_0 \times_k k_0)$. As a result, if F denotes the residue field of k_0 at $\mathcal{Q}$, $p^n | \ |\overline{\mathrm{Jac}(X_0 \times_k k_0)}(F)|$ so, in particular,

$$n \leq \frac{\ln(|\overline{\mathrm{Jac}(X_0 \times_k k_0)}|(F))}{\ln(p)}$$

We are left to compute $|\overline{\mathrm{Jac}(X_0 \times_k k_0)}(F)|$. For this observe that by the Riemann-Hurwitz formula, X_0 has genus $g_{\mathbf{C}_0}$ so $\overline{\mathrm{Jac}(X_0 \times_k k_0)}$ is a $g_{\mathbf{C}_0}$-dimensional abelian variety defined over F which, by Lang-Weil bounds [Mi86], theorem 9.1, yields

$$||\overline{\mathrm{Jac}(X_0 \times_k k_0)}(F)| - |F|| \leq 2^{g_{\mathbf{C}_0}}(\sqrt{|F|}-1) + 2g_{\mathbf{C}_0}$$

and conclude using $|F| \leq q^{d|G_0|/o(\mathbf{C}_0)}$. □

5.5.3 Modular towers and the strong torsion conjecture

We use here the notation introduced in §5.1.2.2 for modular towers. In this context, Fried's conjecture is the following statement[7].

Conjecture 5.20 *If G_0 is a p-perfect finite group then, for any integer $r \geq 3$, any r-tuple $\mathbf{C}_0$ of p'-conjugacy classes of G_0 and any integer $d \geq 1$ there exists $n(d, g_{\mathbf{C}_0}) \geq 0$ such that*

$$\bigcup_{[k:\mathbb{Q}]\leq d} \mathcal{H}_{r,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)(k) = \emptyset, \text{ for each } n \geq n(d, g_{\mathbf{C}_0})$$

As theorem 5.4 from the introduction asserts, we will show it is a consequence of the Strong Torsion Conjecture for abelian varieties [Si92], [Ka98].

Conjecture 5.21 (S.T.C.) *Given two integers g, $d \geq 1$, there exists an integer $n(d,g) \geq 1$ such that the set of all abelian varieties A (i) defined over a number field k of degree $[k:\mathbb{Q}] \leq d$, (ii) of dimension g and (iii) carrying a k-rational torsion point of order n is empty for $n \geq n(d,g)$.*

We decompose the proof of theorem 5.4 in two steps :

First step : Conjecture 5.21 combined with the abelianization procedure conclusion (and the arguments of the proof of proposition 5.19) implies that

$$\bigcup_{[k:\mathbb{Q}]\leq d} \mathcal{H}_{r,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)(k)^{noob} = \emptyset, \text{ for each } n \geq n(\frac{d|G_0|}{o(\mathbf{C}_0)}, g_{\mathbf{C}_0})$$

[7] Fried's conjecture is actually weaker than our conjecture 5.20 [FK97]. Namely, it states that for any number field k there should exist $n(k, G_0, \mathbf{C}_0) \geq 0$ such that $\mathcal{H}_{r,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)(k) = \emptyset$, for each $n \geq n(k, G_0, \mathbf{C}_0)$. However, Merel's theorem for modular curves makes it rather natural to generalize Fried's conjecture by conjecture 5.20 (as it is alluded to, for instance, in [F95a] theorem 1.1 and Appendix B.)

In order to remove the "noob" superscript, we will use a cohomological argument.

Second step : Denote by $s_{m,n} : {}_p\tilde{G}_m \twoheadrightarrow {}_p\tilde{G}_n$ the canonical epimorphism, $m \geq n$. From lemmas 5.10, 5.11 we have $P \cap Z({}_p\tilde{G}) = \{1\}$ so, in particular, for each $n \geq 0$ there exists $N_n \geq n$ such that the image of $P/P_{N_n} \cap Z({}_p^{N_n}\tilde{G})$ in $P/P_n \cap Z({}_p^n\tilde{G})$ via the canonical epimorphism $s_{N_n,n}$ is trivial (recall that $P \cap Z({}_p\tilde{G}) = \varprojlim P/P_n \cap Z({}_p^n\tilde{G})$). Setting $n_1 = n(\frac{d|G_0|}{o(\mathbf{C}_0)}, g_{\mathbf{C}_0})$ and $n_2 = N_{n_1}$, we are going to show that for any integer $d \geq |G|$

$$\bigcup_{[k:\mathbb{Q}]\leq d/|G|} \mathcal{H}_{r,{}_p^n\tilde{G}}(\mathbf{C}_n)(k) = \emptyset, \text{ for each } n \geq n_2$$

So, let k be a number field such that $[k : \mathbb{Q}] \leq d/|G|$ and suppose there exists a G-cover $f_{n_2} : X_{n_2} \to \mathbb{P}^1_{\mathbb{Q}}$ with invariants ${}_p^{n_2}\tilde{G}$, $\mathbf{C}_{n_2}$ and field of moduli k. Denote by f_{n_1} its quotient modulo P_{n_1}/P_{n_2}. If $[\omega_{n_2}] \in \mathrm{H}^2(k, Z({}_p^{n_2}\tilde{G}))$ is the cohomological obstruction for f_{n_2} to be defined over k then $[s_{n_2,n_1} \circ \omega_{n_2}] \in \mathrm{H}^2(k, Z({}_p^{n_1}\tilde{G}))$ is the cohomological obstruction for f_{n_1} to be defined over k. We aim at showing there exists a finite extension k_0/k with $[k_0 : k] \leq |G|$ (so, $[k_0 : \mathbb{Q}] \leq d$) such that $[s_{n_2,n_1} \circ \omega_{n_2}]$ becomes trivial in $\mathrm{H}^2(k_0, Z({}_p^{n_1}\tilde{G}))$. Consequently, f_{n_1} will be defined over k_0 hence contradicting the definition of n_1.

Consider the following canonical diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & s_{n_2,0}(Z({}_p^{n_2}\tilde{G})) & \longrightarrow & G_0 & \longrightarrow & G_0/s_{n_2,0}(Z({}_p^{n_2}\tilde{G})) & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle s_{n_2,0}} & & \uparrow{\scriptstyle s_{n_2,0}} & & \uparrow{\scriptstyle \overline{s}_{n_2,0}} & & \\
1 & \longrightarrow & Z({}_p^{n_2}\tilde{G}) & \longrightarrow & {}_p^{n_2}\tilde{G} & \longrightarrow & {}_p^{n_2}\tilde{G}/Z({}_p^{n_2}\tilde{G}) & \longrightarrow & 1 \\
 & & & & & & \uparrow{\scriptstyle \overline{\phi}_{n_2}} & & \\
 & & & & & & \Gamma_k & &
\end{array}$$

and set $k_0 := \overline{k}^{\ker(\overline{s}_{n_2,0} \circ \overline{\phi}_{n_2})}$. Then $[s_{n_2,0} \circ \omega_{n_2}] = 0$ in $\mathrm{H}^2(k_0, s_{n_2,0}(Z({}_p^{n_2}\tilde{G})))$ that is there exists $\tilde{h} : \Gamma_{k_0} \to s_{n_2,0}(Z({}_p^{n_2}\tilde{G}))$ such that $s_{n_2,0} \circ \omega_{n_2}(\sigma, \tau) = \tilde{h}(\sigma\tau)^{-1}\tilde{h}(\sigma)\tilde{h}(\tau)$, $\sigma, \tau \in \Gamma_{k_0}$. Since $s_{n_2,0} : Z({}_p^{n_2}\tilde{G}) \twoheadrightarrow s_{n_2,0}(Z({}_p^{n_2}\tilde{G}))$ is an epimorphism, one can define a map $\tilde{h}_{n_2} : \Gamma_{k_0} \to Z({}_p^{n_2}\tilde{G})$ such that $s_{n_2,0} \circ \tilde{h}_{n_2} = \tilde{h}$ and thus a coboundary

$$\begin{array}{rccc}
\tilde{\omega}_{n_2} : & \Gamma_{k_0}^2 & \to & Z({}_p^{n_2}\tilde{G}) \\
 & \sigma, \tau & \to & \tilde{h}_{n_2}(\sigma\tau)^{-1}\tilde{h}_{n_2}(\sigma)\tilde{h}_{n_2}(\tau)
\end{array}$$

Now, up to replacing ω_{n_2} by the equivalent cocycle $\omega_{n_2}\tilde{\omega}_{n_2}^{-1}$, one has $s_{n_2,0} \circ \omega_{n_2} = 0$ that is $\mathrm{Im}(\omega_{n_2}) < P/P_{n_2} \cap Z({}_p^{n_2}\tilde{G})$. But then, by definition of n_2, we have $s_{n_2,n_1} \circ \omega_{n_2} = 0$. □

Remark 5.22 (a) The variant of conjecture 5.21 for which it is only requested to bound the p-torsion (that is where the bound $n(d, g)$ is replaced by a bound $n(d, g, p)$ also depending on p and condition (iii) by condition (iii)' *carrying a k-rational torsion point of order p^n*) still implies conjecture 5.20, provided the bound $n(d, g_{\mathbf{C}})$ is replaced by a bound $n(d, g_{\mathbf{C}}, p)$ depending also on p.

(b) Provided that $P \cap Z(G) = \{1\}$, the second step of the proof of theorem 5.4 also yields an effective bound for $n(\mathbf{C}, q, d)$ itself. Namely, one can take $n(q, d, \mathbf{C}) := N_{n(q,d|G|,\mathbf{C})^{noob}}$, where N is defined as in the proof of theorem 5.4. For instance, if $G = \mathbb{Z}/2\mathbb{Z} \rtimes \mathbb{Z}_2$ then $n(q, d, \mathbf{C}) = n(q, d, \mathbf{C})^{noob} + 1$.

The discussion above provides a conjectural approach of conjecture 5.20. When considering the weaker form of conjecture 5.20 obtained by replacing the bound $n(\mathbf{C}, d)$ by a bound $n(\mathbf{C}, k)$ depending on the number field k, there is an alternative conjectural approach, based on reduced modular towers $(\mathcal{H}^{rd}_{r,{}_p^{n+1}\tilde{G}}(\mathbf{C}_{n+1}) \to \mathcal{H}^{rd}_{r,{}_p^n\tilde{G}}(\mathbf{C}_n))_{n\geq 0}$ (we refer to [FK97] or [DF99] for the existence and properties of reduced Hurwitz spaces ; in brief, $\mathcal{H}^{rd}_{r,G}(\mathbf{C})$ is the quotient space $\mathcal{H}_{r,G}(\mathbf{C})/\mathrm{PSL}_2(\mathbb{C})$ where the action

of $\mathrm{PSL}_2(\mathbb{C})$ on $\mathcal{H}_{r,G}(\mathbf{C})$ is obtained by extending the one of $\mathrm{PSL}_2(\mathbb{C})$ on $\mathcal{U}_r(\mathbb{C})$ and, in particular, it is a $r-3$-dimensional variety). This approach consists in proving that all the geometrically irreducible components of $\mathcal{H}^{rd}_{r,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)$ are of general type (of genus ≥ 2 when $r=4$) in order to obtain, relying on the Bombieri-Lang conjecture (Faltings' theorem when $r=4$), that if $\mathcal{H}^{rd}_{r,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)(k)\neq\emptyset$ for all $n\geq 0$ then $\varprojlim \mathcal{H}^{rd}_{r,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)(k)\neq\emptyset$. Up to taking a finite extension k_0/k, this entails that $\varprojlim \mathcal{H}_{r,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)(k_0)\neq\emptyset$, [DF99] §6.5, contradicting theorem 5.2. When $r=4$, M. Fried gives in [F04] an outline of the proof of the fact all the geometrically irreducible components of $\mathcal{H}^{rd}_{4,\frac{n}{p}\tilde{G}}(\mathbf{C}_n)$ have genus ≥ 2 for n large enough.

Chapitre 6

Standard Hurwitz curves

Sommaire

Given a finite group G and a r-tuple $\mathbf{C}$ of non trivial conjugacy classes of G, we call standard Hurwitz curve any 1-dimensional closed subvariety of $\mathcal{H}'_{r,G}(\mathbf{C})$ obtained by fixing the $r-1$ last branch points that is, given $\mathbf{t}' \in \mathcal{U}^{r-1}$, we consider the cartesian square :

$$\begin{array}{ccc} \mathcal{H}'_{r,G}(\mathbf{C})_{\mathbf{t}'} & \longrightarrow & \mathcal{H}'_{r,G}(\mathbf{C}) \\ \downarrow{\scriptstyle \Psi'_{r,G,\mathbf{t}'}} & \square & \downarrow{\scriptstyle \Psi'_{r,G}} \\ \mathcal{U}^r_{\mathbf{t}'} & \longrightarrow & \mathcal{U}^r \end{array}$$

Using the homotopy sequence of the fibration with connected fibers

$$\begin{array}{cccc} p_{2,r} & \mathcal{U}^r(\mathbb{C}) & \to & \mathcal{U}^{r-1}(\mathbb{C}) \\ & (t_1, ..., t_r) & \to & (t_2, ..., t_r) \end{array}$$

which gives rise to the short exact sequence of fundamental groups

$$1 \to \pi_1^{\mathrm{top}}(\mathcal{U}^r_{\mathbf{t}'_{2,r}}, \mathbf{t}'_{1,1}) \to \pi_1^{\mathrm{top}}(\mathcal{U}^r, \mathbf{t}') \to \pi_1^{\mathrm{top}}(\mathcal{U}^{r-1}, \mathbf{t}'_{r,2})$$

(where we write $\mathbf{t}'_{i,j} = (t_i, ..., t_j)$ for any $\mathbf{t}' = (t_1, ..., t_r) \in \mathcal{U}^r$, $1 \leq i \leq j \leq r$) one can show that $\pi_1^{\mathrm{top}}(\mathcal{U}^r_{\mathbf{t}'_{2,r}}, \mathbf{t}'_{1,1}) =< \{A_{1,j}\}_{2 \leq j \leq r} >=: \Pi_{1,r}$ where $A_{1,j} = Q_1 \cdots Q_{j-2} Q_{j-1}^{-2} Q_{j-2}^{-1} \cdots Q_1^{-1}$, $2 \leq j \leq r$ (in particular, one recovers the sphere relation $A_{1,2} \cdots A_{1,r} = 1$). We will allso write $a_{1,j} = A_{1,j}^{-1}$. Thus, the completed ramified cover $\overline{\Psi}'_{r,G,\mathbf{t}'} : \overline{\mathcal{H}}'_{r,G}(\mathbf{C})_{\mathbf{t}'} \to \mathbb{P}^1$ corresponds to the action of $\Pi_{1,r}$ on $\overline{\mathrm{sni}}(\mathbf{C})$ induced by the one of SH_r. This will allow us to use Hurwitz formula to compute the genus $g(\mathbf{C})$ of the standard Hurwitz curve $\overline{\mathcal{H}}'_{r,G}(\mathbf{C})_{\mathbf{t}'}$.

6.1 Genus of standard Hurwitz curves

[DF94] §4 provides a general genus formula for standard Hurwitz curves when $r = 4$, precisely for any $\Pi_{1,4}$-orbit $O \in \overline{\mathrm{sni}}(\mathbf{C})/\Pi_{1,4}$, the genus of the corresponding geometrically irreducible component

is given by :

$$2(|O| + g(\mathbf{C}) - 1) = \mathrm{Ind}(A_{1,2}) + \mathrm{Ind}(A_{1,3}) + \mathrm{Ind}(A_{1,4})$$

where $\mathrm{Ind}(A_{1,j}) = \sum_{\mathbf{g}\in O}(i_{1,j}(\mathbf{g}) - 1)/i_{1,j}(\mathbf{g})$, $j = 2, 3, 4$ and

$$\begin{aligned} i_{1,2}(\mathbf{g}) &= |< g_1g_2 > / < g_1g_2 > \cap Z(g_1, g_2)Z(g_3)| \\ i_{1,3}(\mathbf{g}) &= |< g_4g_2 > / < g_4g_2 > \cap Z(g_4, g_2)Z(g_3)| \\ i_{1,4}(\mathbf{g}) &= |< g_4g_1 > / < g_4g_1 > \cap Z(g_4, g_1)Z(g_3)| \end{aligned}$$

(where $Z(g_i, g_j) = Z(g_i) \cap Z(g_j)$ and $Z(g)$ is the centralizer of g in G). The purpose of this section is to generalize this formula for any $r \geq 4$.

6.1.1 Invariants associated with a standard Hurwitz curve

Given a finite group G and a r-tuple $\mathbf{C}$ of non trivial conjugacy classes of G, one can associate to $\mathbf{C}$ a family of numerical invariants $\{(g_O, l_O)\}_{O\in\overline{\mathrm{sni}}(\mathbf{C})/\Pi_{1,r}}$. Indeed, there is a one-to-one correspondence between the connected components of $\mathcal{H}'_{r,G}(\mathbf{C})$ and the orbits of $\overline{\mathrm{sni}}(\mathbf{C})/SH_r$. Given $O \in \overline{\mathrm{sni}}(\mathbf{C})/SH_r$ and $\mathbf{g} \in O$, the corresponding connected component $X(O)$ is the set of those G-covers f such that there exists $Q \in SH_r$ and a standard ordered topological bouquet $\underline{\gamma}$ for $\mathbb{P}^1(\mathbb{C})\setminus\mathbf{t}$ with $BCD_{Q.\underline{\gamma}}(f) \in O$. Now, let $\mathbf{t}'_{2,r} \in \mathcal{U}^{r-1}(\mathbb{C})$ and $(\Psi'_{r,G})_{\mathbf{t}'_{2,r}} : X(O)_{\mathbf{t}'_{2,r}} \to \mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}_{2,r}$ be the corresponding cover. Once again, there is a one-to-one correspondence between the connected components of $X(O)_{\mathbf{t}'_{2,r}}$ and the orbits of $O/\Pi_{1,r}$. Since $\Pi_{1,r}$ is normal in SH_r ([Bi74] theorem), it permutes transitively the orbits of $O/\Pi_{1,r}$ and, as a result they all have the same length, l_O. We define the genus of a given orbit $U \in O/\Pi_{1,r}$ by Riemann-Hurwitz's formula :

$$g_U = 1 - |U| + \frac{1}{2}\sum_{2\leq i\leq r}\sum_{1\leq j\leq r_i}(\mathrm{long(c_{i,j})} - 1)$$

where $c_{i,1} \circ \cdots \circ c_{i,r_i}$ is the decomposition of the permutation induced on U by $A_{1,i}$ into a product of disjoint cycles, $i = 2, ..., r$. Given $U_1 \neq U_2 \in O/\Pi_{1,r}$ and $Q \in SH_r$ such that $Q \cdot U_1 = U_2$ if $c_{i,1}\circ\cdots\circ c_{i,r_i}$ is the decomposition of $A_{1,i}$ on U_1 then $(Qc_{i,1}Q^{-1})\circ\cdots\circ(Qc_{i,r_i}Q^{-1})$ is the one of $A_{1,i}$ on U_2 so $g_{U_1} = g_{U_2}$. We denote the common genus of the orbits of $O/\Pi_{1,r}$ by g_O. The end of this section is devoted to giving a general formula for g_O.

6.1.2 A general formula to compute the genus

Let $U \in O/\Pi_{1,r}$. First, note that

$$\sum_{2\leq i\leq r}\sum_{1\leq j\leq r_i}(\mathrm{long(c_{i,j})} - 1) = \sum_{2\leq \mathrm{i}\leq \mathrm{r}}\sum_{1\leq \mathrm{j}\leq \mathrm{r_i}}(\mathrm{long(c_{i,j}^{-1})} - 1)$$

and that

$$\sum_{1\leq j\leq r_i}(\mathrm{long}(c_{i,j}^{-1}) - 1) = \sum_{1\leq j\leq r_i}\sum_{\mathbf{g}\in\mathrm{supp}(c_{i,j})}\frac{(|< a_{1,i} > .\mathbf{g}| - 1)}{|< a_{1,i} > .\mathbf{g}|} = \sum_{\mathbf{g}\in U}\frac{(|< a_{1,i} > .\mathbf{g}| - 1)}{|< a_{1,i} > .\mathbf{g}|}$$

The following technical lemma explains how to compute the $|< a_{1,i} > .\mathbf{g}|$, $i = 2, ..., r$.

Lemma 6.1 *For any* $\mathbf{g} = (g_1, ..., g_r) \in \overline{\mathrm{sni}}(\mathbf{C}, G)$ *and for any* $2 \leq i \leq r$

$$a_{1,i}^n.\mathbf{g} = (g_1^{(g_i^{\alpha_i}g_1)^n}, g_2, ..., g_{i-1}, g_i^{(g_1^{\alpha_i^{-1}}g_i)^n}, g_{i+1}, ..., g_r)$$

where $\alpha_i = g_1...g_{i-1}$.

Proof. For $n=1$: A straightforward computation shows that

$$a_{1,i}.\mathbf{g} = (g_1^{g_2\cdots g_{i-1}\alpha_i^{-1}g_1g_i^{\alpha_i}}, g_2, ..., g_{i-1}, g_i^{g_1^{\alpha_i^{-1}}}, g_{i+1}, ..., g_r)$$

which can also be written

$$\begin{aligned}(g_1^{g_2\cdots g_{i-1}\alpha_i^{-1}g_1g_i^{\alpha_i}}, g_2, ..., g_{i-1}, g_i^{g_1^{\alpha_i^{-1}}}, g_{i+1}, ..., g_r) &= (g_1^{g_1^{-1}\alpha_i\alpha_i^{-1}g_1g_i^{\alpha_i}}, g_2, ..., g_{i-1}, g_i^{g_1^{\alpha_i^{-1}}}, g_{i+1}, ..., g_r)\\ &= (g_1^{g_i^{\alpha_i}}, g_2, ..., g_{i-1}, g_i^{g_1^{\alpha_i^{-1}}}, g_{i+1}, ..., g_r)\\ &= (g_1^{g_i^{\alpha_i}g_1}, g_2, ..., g_{i-1}, g_i^{g_1^{\alpha_i^{-1}}g_i}, g_{i+1}, ..., g_r)\end{aligned}$$

For $n\geq 1$: suppose $a_{1,i}^n.\mathbf{g} = (g_1^{(g_i^{\alpha_i}g_1)^n}, g_2, ..., g_{i-1}, g_i^{(g_1^{\alpha_i^{-1}}g_i)^n}, g_{i+1}, ..., g_r) =: (g_{1,n}, ..., g_{r,n})$.
Since $\alpha_{i,n} = g_{1,n}...g_{i-1,n} = g_{1,n}g_1^{-1}\alpha_i$, we get

$$\begin{aligned}a_{1,i}^{n+1}.\mathbf{g} = a_{1,i}.(a_{1,i}^n.\mathbf{g}) &= (g_{1,n}^{g_{i,n}^{\alpha_{i,n}}g_{1,n}}, g_{2,n}, ..., g_{i-1,n}, g_{i,n}^{g_{1,n}^{\alpha_{i,n}^{-1}}g_{i,n}}, g_{i+1,n}, ..., g_{r,n})\\ &= (g_{1,n}^{g_{i,n}^{g_{1,n}g_1^{-1}\alpha_i}g_{1,n}}, g_2, ..., g_{i-1}, g_{i,n}^{g_{1,n}^{\alpha_i^{-1}g_1g_{1,n}^{-1}}g_{i,n}}, g_{i+1}, ..., g_r)\\ &=: (g_{1,n+1}, g_{2,n+1}, ..., g_{i-1,n+1}, g_{i,n+1}, g_{i+1,n+1}, ..., g_{r,n+1})\end{aligned}$$

Rewriting

$$\begin{cases} g_{1,n} = g_1^{(g_i^{\alpha_i}g_1)^n} = \alpha_i(g_ig_1^{\alpha_i^{-1}})^n\alpha_i^{-1}g_1\alpha_i(g_ig_1^{\alpha_i^{-1}})^{-n}\alpha_i^{-1} = \alpha_ig_i(g_1^{\alpha_i^{-1}}g_i)^{n-1}g_1^{\alpha_i^{-1}}(g_1^{\alpha_i^{-1}}g_i)^{-(n-1)}g_i^{-1}\alpha_i^{-1} \\ g_{i,n} = g_i^{(g_1^{\alpha_i^{-1}}g_i)^n} = \alpha_i^{-1}(g_1g_i^{\alpha_i})^n\alpha_ig_i\alpha_i^{-1}(g_1g_i^{\alpha_i})^{-n}\alpha_i = \alpha_i^{-1}g_1(g_i^{\alpha_i}g_1)^{n-1}g_i^{\alpha_i}(g_i^{\alpha_i}g_1)^{-(n-1)}g_1^{-1}\alpha_i \end{cases}$$

We get then

$$g_{1,n+1} = g_{1,n}^{g_{1,n}(g_{i,n}^{g_1^{-1}\alpha_i})} = g_{1,n}\left((g_i^{\alpha_i}g_1)^{n-1}g_i^{\alpha_i}(g_i^{\alpha_i}g_1)^{-(n-1)}\right)g_{1,n}\left((g_i^{\alpha_i}g_1)^{n-1}g_i^{-1\,\alpha_i}(g_i^{\alpha_i}g_1)^{-(n-1)}\right)g_{1,n}^{-1}$$

but

$$g_{1,n}(g_i^{\alpha_i}g_1)^{n-1}g_i^{\alpha_i}(g_i^{\alpha_i}g_1)^{-(n-1)} = (g_i^{\alpha_i}g_1)^ng_1(g_i^{\alpha_i}g_1)^{-n}(g_i^{\alpha_i}g_1)^{n-1}g_i^{\alpha_i(g_i^{\alpha_i}g_1)^{-(n-1)}} = g_i^{\alpha_i}g_1$$

which implies $g_{1,n+1} = (g_i^{\alpha_i}g_1)g_{1,n}(g_i^{\alpha_i}g_1)^{-1} = g_1^{(g_i^{\alpha_i}g_1)^{n+1}}$.

Likewise, for $g_{i,n+1}$ we get

$$g_{i,n+1} = (g_{i,n}^{g_1^{-1}\alpha_i})^{\alpha_i^{-1}g_1g_{1,n}} = \left((g_i^{\alpha_i})^{(g_i^{\alpha_i}g_1)^{n-1}}\right)^{\alpha_i^{-1}g_1g_{1,n}} = \alpha_i^{-1}g_1(g_i^{\alpha_i}g_1)^ng_i^{\alpha_i}(g_i^{\alpha_i}g_1)^{-n}g_1^{-1}\alpha_i$$

but, $\alpha_i^{-1}g_1(g_i^{\alpha_i}g_1)^n = (g_1^{\alpha_i^{-1}}g_i)^{n+1}\alpha_i^{-1}g_i^{-1\,\alpha_i}$, which implies $g_{i,n+1} = g_i^{(g_1^{\alpha_i^{-1}}g_i)^{n+1}}$ □

As a result, for any $\mathbf{g}\in U$, $a_{1,i}^n\cdot\mathbf{g} = \mathbf{g}$ if and only if

(*) there exists $\gamma\in\cap_{2\leq i\neq j\leq r}\mathrm{Cen}_G(g_j)$ such that $g_1^{(g_i^{\alpha_i}g_1)^n} = g_1^\gamma$ and $g_i^{(g_1^{\alpha_i^{-1}}g_i)^n} = g_i^\gamma$

But, assume $g_1^{(g_i^{\alpha_i}g_1)^n} = g_1^\gamma$ then $\begin{aligned} g_i^{(g_1^{\alpha_i^{-1}}g_i)^n} &= (g_1^{(g_i^{\alpha_i}g_1)^n}g_2\cdots g_{i-1})^{-1}(g_{i+1}\cdots g_r)^{-1}\\ &= (g_1^\gamma g_2\cdots g_{i-1})^{-1}(g_{i+1}\cdots g_r)^{-1}\\ &= g_i^\gamma\end{aligned}$

So (*) is equivalent to

(**) $(g_i^{\alpha_i}g_1)^n\in(\cap_{2\leq i\neq j\leq r}\mathrm{Cen}_G(g_j)\mathrm{Cen}_G(g_1))\cap<g_i^{\alpha_i}g_1>$

But the right-hand term of the formula above is a subgroup of $< g_i^{\alpha_i} g_1 >$. Indeed, $g_i^{\alpha_i} g_1 = (g_1 \cdots g_i)(g_2 \cdots g_{i-1})^{-1} = (g_{i+1} \cdots g_r^{-1})(g_2 \cdots g_{i-1})^{-1}$ so any element $u \in \cap_{2 \leq i \neq j \leq r} \mathrm{Cen}_G(g_j)$ commutes with $g_i^{\alpha_i} g_1$. Setting $Z_i(\mathbf{g}) = (\cap_{2 \leq i \neq j \leq r} \mathrm{Cen}_G(g_j))\mathrm{Cen}_G(g_1)$, $i = 2, ..., r$, we deduce

$$| < a_{1,i} > .\mathbf{g}| = \min\{\mathrm{n} \geq 1 | (\mathrm{g_i^{\alpha_i} g_1})^{\mathrm{n}} \in \mathrm{Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 >}\} = | < \mathrm{g_i^{\alpha_i} g_1} > / \mathrm{Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1} > |$$

That is,

Proposition 6.2 (general genus formula)

$$g_O = 1 + \frac{(r-3)l_O}{2} - \frac{1}{2} \sum_{2 \leq i \leq r} \sum_{\mathbf{g} \in U} \frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 > |}{| < g_i^{\alpha_i} g_1 > |}.$$

(Note that, if $\cap_{2 \leq i \neq j \leq r} \mathrm{Cen_G(g_j)} = \mathrm{Z(G)}$*, then* $Z_i(\mathbf{g})$ *is just* $\mathrm{Cen}_G(g_1)$*,* $i = 2, ..., r$*).*

Remark 6.3 Given a group epimorphism $s : G \twoheadrightarrow \overline{G}$, $\mathbf{C}$ a tuple of conjugacy classes of G, $\overline{\mathbf{C}} = s(\mathbf{C})$ one can observe that for any $\mathbf{g} \in \overline{\mathrm{sni}}(\mathbf{C})$ if $\frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 >|}{| < g_i^{\alpha_i} g_1 >|} = 1$ then $\frac{|Z_i(\overline{\mathbf{g}}) \cap < \overline{g}_i^{\alpha_i} \overline{g}_1 >|}{| < \overline{g}_i^{\alpha_i} \overline{g}_1 >|} = 1$ as well.

In the next section, we use this genus formula to give a lower bound for the genus and thus, illustrating problem **B**.3 [F95a].

6.1.3 Growth of the genus

We keep the notations of section 6.1.2. Define the function $m_i : O \to \mathbb{N}^\star$ by $m_i(\mathbf{g}) = \frac{| < g_i^{\alpha_i} g_1 > |}{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 > |}$ (so $m_i(\mathbf{g}) | \, | < g_i^{\alpha_i} g_1 > |$). Then one can rewrite

$$g_O = 1 + \frac{(r-3)l_O}{2} - \frac{1}{2} \sum_{m \in \mathbb{N}^\star} \frac{1}{m} \sum_{2 \leq i \leq r} |m_i^{-1}(m)|.$$

A first minoration of g_O is given by $g_O \geq 1 + \frac{(r-6)l_O - M_O}{4}$, where $M_O = \sum_{2 \leq i \leq r} |m_i^{-1}(1)|$. This emphasizes the intuitive idea that as soon as r is large enough and $\mathbf{C}$ "g-complete enough", standard Hurwitz curves are intricate arithmetic objects. More precisely observe that :

- If $M_O \leq (r-6)l_O - 2$ the $g_O \geq 2$.
- If $M_O \leq 7 + (r-10)l_O$ then $1 + \frac{g_O}{2} > l_O$ that is, the corresponding standard Hurwitz curves are general in the sense of [**?**], theorem F.1.2.2.

Let us precise the notion of being "g-complete enough" by giving a definition compatible with problem **B**.3 [F95a]. Given an r-tuple $\mathbf{C} \in \mathcal{C}_r(G)$ and an integer $t \geq 3$ we will say $\mathbf{C}$ is t-g-complete if for any $O \in \overline{\mathrm{sni}}(\mathbf{C})/SH_r$ we have $g_0 \geq 1 + f(t)l_0$ where $f : \mathbb{N}^\star \to \mathbb{R}$ is a function verifying $\lim_{n \to +\infty} f(n) = +\infty$. Here are two examples of t-g-complete tuples :

1. If $\mathbf{C} = (C_1, ..., C_r)$ such that $|C_1| \geq 2$ and there exists a partition $\{2, ..., r\} = I_1 \cup ... \cup I_t$ with $(C_i)_{i \in I_k}$ g-complete, $k = 1, ..., t$.

   Proof. Assume $t \geq 2$ then, when removing C_1 and C_i from $\mathbf{C}$, the resulting tuple is still g-complete, which entails that $Z_i(\mathbf{g}) = \mathrm{Cen}_G(g_1)$, $i = 2, ..., r$, $\mathbf{g} \in U$. Thus, $\frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 >|}{| < g_i^{\alpha_i} g_1 >|} = 1$ iff $g_i^{\alpha_i} \in \mathrm{Cen}_G(g_1$. But, if $g_i^{\alpha_i} \in \mathrm{Cen}_G(g_1$ for all $i \in I_k$ then, by the g-completeness assumption, $\mathrm{Cen}_G(g_1) = G$: a contradition since g_1 is not central. Thus there exists $\emptyset \neq J_k(\mathbf{g}) \subset I_k$ such that for any $i \in J_k(\mathbf{g})$, $\frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 >|}{| < g_i^{\alpha_i} g_1 >|} = 1$ iff $g_i^{\alpha_i} \in \mathrm{Cen}_G(g_1 \leq \frac{1}{2}$, $k = 1, ..., t$, $\mathbf{g} \in U$. As a result we get

$$\begin{array}{rcl} g_O & = & 1 + \frac{(r-3)l_O}{2} - \frac{1}{2} \sum_{\mathbf{g} \in U} \sum_{1 \leq k \leq t} \sum_{i \in I_k} \frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 >|}{| < g_i^{\alpha_i} g_1 >|} \\ & \geq & 1 + \frac{(r-3)l_O}{2} - \frac{1}{2} \sum_{\mathbf{g} \in U} \sum_{1 \leq k \leq t} (\frac{1}{2} + (|I_k| - 1)) \\ & \geq & 1 + \frac{(r-3)l_O}{2} - \frac{l_O}{2} \sum_{1 \leq k \leq t} (|I_k| - \frac{1}{2}) \\ & \geq & 1 + (\frac{t}{4} - 1)l_O) \end{array}$$

2. If $\mathbf{C} = (C_1, C_1^{-1}, ..., C_r)$ such that there exists a partition $\{3, ..., r\} = I_1 \cup ... \cup I_t$ with $(C_1, (C_i)_{i \in I_k})$ g-complete and there exists $i_k \in I_k$ such that $C_{i_k} \cap \mathrm{Cen}_G(g_1) = \emptyset$, $k = 1, ..., t$.

Proof. Assume $t \geq 2$ then, when removing C_1 and C_i from $\mathbf{C}$, the resulting tuple is still g-complete, which entails that $Z_i(\mathbf{g}) = \mathrm{Cen}_G(g_1)$, $i = 2, ..., r$, $\mathbf{g} \in U$. Thus, $\frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 >|}{|< g_i^{\alpha_i} g_1 >|} = 1$ iff $g_i^{\alpha_i} \in \mathrm{Cen}_G(g_1$. But, following from the hypothesis, there exists $i \in I_k$ such that $g_i^{\alpha_i} \notin \mathrm{Cen}_G(g_1$ and, consequently, $\frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 >|}{|< g_i^{\alpha_i} g_1 >|} \leq \frac{1}{2}$, for all $\mathbf{g} \in U$. As a result we get

$$\begin{array}{rcl} g_O & \geq & 1 + \frac{(r-3)l_O}{2} - \frac{1}{2} \sum_{\mathbf{g} \in U} (1 + \sum_{1 \leq k \leq t} \sum_{i \in I_k} \frac{|Z_i(\mathbf{g}) \cap < g_i^{\alpha_i} g_1 >|}{|< g_i^{\alpha_i} g_1 >|}) \\ & \geq & 1 + \frac{(r-3)l_O}{2} - \frac{1}{2}(l_O + \sum_{\mathbf{g} \in U} \sum_{1 \leq k \leq t} (\frac{1}{2} + (|I_k| - 1)) \\ & \geq & 1 + \frac{(r-3)l_O}{2} - \frac{l_O}{2}(1 + \sum_{1 \leq k \leq t} (|I_k| - \frac{1}{2}) \\ & \geq & 1 + (\frac{t}{4} - 1) l_O) \end{array}$$

Now, recall that problem **B**.2 [F95a] asks for a condition to ensure a standard HM-curve remains geometrically irreducible. Problem **B**.3 [F95a] asks furthermore for a condition to ensure the genus of standard HM-curves grows towards $+\infty$ along a Modular Tower. Chapter **??** deals with the former problem, as for the latter, let us come back to an example : take $G = M_{11}$ and $\mathbf{C} = ([8A], [11A]^r)$. According to the Atlas $(8A, 11A)$ is g-complete and $\mathrm{Cen}_{M_{11}}(8A) =< 8A >$, $\mathrm{Cen}_{M_{11}}(11A) =< 11A >$; in particular, we always have $11A \cap \mathrm{Cen}_{M_{11}}(8A) = \emptyset$. For r large enough, we know that $|O^{HM}(\mathbf{C})/\Pi_{1,2+2r}| = 1$ thus, by case 2 above $g_{O^{HM}(\mathbf{C})} \geq 1 + (\frac{r}{4} - 1)|O^{HM}(\mathbf{C})| \geq 2$ as soon as $r \geq 5$. If we consider for instance the Modular Tower associated with the data $(M_{11}, \mathbf{C}, 3)$ we know that $|O^{HM}(\mathbf{C}_n)/\Pi_{1,2+2r}| = 1$, $n \geq 0$ and since $\mathbf{C}_n$ also verifies case 2 above (recall being g-complete is a property which passes to Frattini extensions) we obtain, $g_{O^{HM}(\mathbf{C}_n)} \geq 1 + (\frac{r}{4} - 1)|O^{HM}(\mathbf{C}_n)|$. As a result, as soom as r is large enough (and ≥ 5) we get a tower

$$(\mathcal{H}'^{HM}_{2r+2, p^{n+1} \tilde{M}_{11}}(\mathbf{C}_{n+1})_{\mathbf{t}'} \to \mathcal{H}'^{HM}_{2r+2, p^n \tilde{M}_{11}}(\mathbf{C}_n)_{\mathbf{t}'})_{n \geq 0}$$

of geometrically irreducible HM-curves defined over $\mathbb{Q}(\mathbf{C}', \mathbf{t}')$ the genus of which grows towards $+\infty$ with n, for any $\mathbf{t}' \in \mathcal{U}^{2r+1}(\overline{\mathbb{Q}})$. In particular, by theorem 6.1 of **??** for any finite extension $k/\mathbb{Q}(\mathbf{C}', \mathbf{t}')$ there exists $n(k) \geq 0$ such that for any $n \geq n(k)$, $\mathcal{H}'^{HM}_{2r+2, p^n \tilde{M}_{11}}(\mathbf{C}_n)_{\mathbf{t}'}(k) = \emptyset$.

6.2 Hasse property for Hurwitz curves when $r = 4$

6.2.1 How to get rational points on a genus 0 curve ?

Recall first the classical classification statement about curves of genus 0 over a field k.

Proposition 6.4 *Let X/k be a smooth projective curve of genus 0 defined over a field k then (1) X/k is isomorphic (2) X/k is isomorphic*

Proof. By Riemann Roch theorem, the canonical divisor $K \in \mathrm{Div}(X/k)$ of X/k is of degree -2 so $-K$ is a very ample divisor of degree 2 and linear dimension 3 defining a k-embedding of X into $\mathbb{P}^2_k$ as a smooth curve of degree 2 that is, a conic. If furthermore X has a k-rational point $P \in \mathrm{Div}(X/k)$, by Riemann Roch theorem, there exists a non constant algebraic function $x \in k(X) \setminus k$ such that $(x) \geq -P$. But P is effective of degree 1 therefore $(x)_\infty = P$ and $[k(X) : k(x)] = \deg(x)_\infty = 1$. □

There is two distinct ways to show X/k possesses a k-rational point. The first one is a consequence of Riemann-Roch theorem :

Proposition 6.5 *Let X/k a smooth projective curve of genus 0 defined over k then X/k possesses a k-rational point if and only if it possesses an odd degree divisor.*

Proof. Since the canonical divisor $K \in \mathrm{Div}(X/k)$ is of degree -2, any divisor $D \in \mathrm{Div}(X/k)$ of odd degree deg(D) = 2n+1 defines a divisor $D - nK$ of degree 1. So, assume $D \in \mathrm{Div}(X/k)$ is of degree 1, by Riemann-Roch theorem there exists a non constant algebraic function $x \in k(X) \setminus k$ such that $D + (x) \geq 0$. So $P = D + (x)$ is an effective divisor of degree 1 that is, corresponds to a k-rational point on X/k. □

The second one is a special case of the Hasse principle for quadratic forms :

Proposition 6.6 *Let $k/\mathbb{Q}$ be a number field and X/k a smooth projective curve of genus 0 defined over k then the following assertions are equivalent :*

(i) X/k *is isomorphic over* k *to* $\mathbb{P}^1_k$.
(ii) X/k *possesses a* k_v*-rational point over all completions* k_v *of* k.
(iii) X/k *possesses a* k_v*-rational point over all but one completions* k_v *of* k.

Sketch of the proof. We obviously have $(i) \Rightarrow (ii) \Rightarrow (iii)$. $(ii) \Rightarrow (i)$ results from the local global property for Hilbert symbols and $(iii) \Rightarrow (ii)$ from the product formula $\prod_{v\in M_k}(a,b)_v = 1$. □

Classical genus 0 methods are based on proposition 6.5. The most classical one consists in exhibiting genus 0 standard Hurwitz curves defined over a number field k and using the branch cycle description of the covers $\Psi'_{r,G,\mathbf{t}'}$ to show one of the ramified place is of odd degree [Ma89], [Det00] *etc.* The following example shows however finding an odd degree ramified place is not always possible.

Example 6.7 *(Dicyclic group of order 16)* The dicyclic group of order $4n$ is given by the generators and relations

$$T_{4n} =< u, v | u^{2n} = 1, u^n = v^2, v^{-1}uv = u^{-1} >$$

Assume $n = 2^k$, $k \geq 2$ and denote the two conjugacy classes of non trivial involutions by $B_{1,k} = \{u^{2i}v\}_{0\leq i\leq 2^k-1}$, $B_{2,k} = \{u^{2i+1}v\}_{0\leq i\leq 2^k-1}$. Then the 4-tuple $\mathbf{C}_k = (B_{1,k}, B_{1,k}, B_{2,k}, B_{2,k})$ has the property that $\Pi_{1,4}$ acts transitively on $\overline{\mathrm{sni}}(\mathbf{C}_k)$ and straightforward computations gives : $|\overline{\mathrm{sni}}(\mathbf{C}_k)| = 2^{2k-1}$, $a_{1,2}$ has type $((1)^{2^k}, ((2^{k-r-1})^{2^{k-1}})_{0\leq r\leq k-2})$, $a_{1,3}$ and $a_{1,4}$ have type $((2^k)^{2^{k-1}})$. As a result $g(\mathbf{C}_k) = 2^{k-2}(2^k - k - 3) + 1$. In particular for $k = 2$, $|\overline{\mathrm{sni}}(\mathbf{C}_2)| = 8$, $a_{1,2}$ has type $((1)^4, (2)^2)$, $a_{1,3}$ and $a_{1,4}$ have type $((4)^2)$ and $g(\mathbf{C}_2) = 0$. Thus, choosing $\mathbf{t}' = (t_2, t_3, t_4) \in \mathcal{U}^3(\mathbb{Q})$ we obtain a genus 0 standard Hurwitz curve defined over $\mathbb{Q}$ but we cannot assert one of the ramified place is of odd degree.

However, proposition 6.6 can be applied to the curve of example 6.7. The next sections describe how, and provide a general method when $r = 4$ (and some technical properties are fulfilled) to use the Hasse principle instead of the odd degree divisor method to find rational points on Hurwitz curves.

6.2.2 The Hasse condition for Hurwitz curves when $r = 4$

6.2.2.1 Using directly patching methods

Theorem 6.8 (Nearly Hasse Condition) *Let G be a finite group and $\mathbf{C} = (C_1, C_1^{-1}, C_2, C_2^{-1})$ a symetric 4-tuple of non trivial conjugacy classes. Assume $\overline{\mathrm{hm}}(\mathbf{C}) \neq \emptyset$. Then there exists a finite cyclotomic extension $\mathbb{Q}'_{\mathbf{C}}/\mathbb{Q}$ such that for any place v of $\mathbb{Q}'_{\mathbf{C}}$, of residue characteristic prime to $|G|$, there exists a HM-G-cover f_v defined over $(\mathbb{Q}'_{\mathbf{C}})_v$ with invariants G, $\mathbf{C}$, $(t_v, 0, 1, 2)$.*

Remark 6.9 Denote by o_i the order of the elements in C_i, $i = 1, 2$, by m their less common multiple and for any integer $n \geq 1$ write $\zeta_n := \mathrm{e}^{\frac{2\pi i}{n}}$. Then the finite cyclotomic extension $\mathbb{Q}'_{\mathbf{C}}/\mathbb{Q}$ verifies $\mathbb{Q}'_{\mathbf{C}} \subset \mathbb{Q}(\zeta_m)$ and actually depends on the rationality properties of the tuple $\mathbf{C} = (C_1, C_1^{-1}, C_2, C_2^{-1})$: $\mathbb{Q}'_{\mathbf{C}} = \overline{\mathbb{Q}}^{\Delta'_{\mathbf{C}}}$ where $\Delta'_{\mathbf{C}} = \{\sigma \in \Gamma_{\mathbb{Q}} \mid C_i^{\chi(\sigma)} = C_i,\ i = 1, 2\}$.

Proof. We proceed in two steps.

The first step consists in showing theorem 6.8 is true when replacing $(t_v, 0, 1, 2)$ by $(x_{1,v}, y_{1,v}, x_{2,v}, y_{2,v}) \in \mathcal{U}^4(\mathbb{Q})$ or by $(x_{1,v}, y_{1,v}, x_{2,v}, y_{2,v}) \in \mathcal{U}^4(\overline{\mathbb{Q}})$ with $x_{i,v} = z_i$, $y_{i,v} = \overline{z}_i$ and $z_i \in \mathbb{Q}(\zeta_m)$, $i = 1, 2$.

By assumption $\overline{\mathrm{hm}}(\mathbf{C}) \neq \emptyset$ so let us fix a HM-representative $\mathbf{g} = (g_1, g_1^{-1}, g_2, g_2^{-1}) \in \overline{\mathrm{hm}}(\mathbf{C})$.
(1) Real G-covers : Given an r-tuple $\mathbf{C}$ of non trivial conjugacy classes and a real branch point divisor $\mathbf{t} \in \mathcal{U}_r(\mathbb{R})$ consisting of $r = r_1 + 2r_2$ branch points with

- r_1 real branch points $t_1, ..., t_{r_1}$.
- r_2 complex conjugated pairs $\{z_i, \overline{z}_i\} \subset \mathbb{P}^1(\mathbb{C} \setminus \mathbb{P}^1(\mathbb{R}))$; we will generally write $z_i = t_{r_1+i+1}$, $\overline{z}_i = t_{r_1+i+2}$, $i = 1, ..., r_2$.

then [DF94] there exists a topological bouquet $\underline{\gamma}$ for $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ based at $t_0 \in \mathbb{P}^1(\mathbb{R}) \setminus \mathbf{t}$ such that via the identification $\mathrm{Rev}^{\mathrm{G}}_{\mathbf{t}',\mathbf{C}} \simeq \overline{\mathrm{sni}}(\mathbf{C})$ induced by the monodromy $BCD_{\underline{\gamma}}$, the G-covers defined over $\mathbb{R}$ correspond to the equivalence classes of those $(g_1, ..., g_r)$ in $\mathrm{sni}(\mathbf{C})$ verifying, for some involution

$g_0 \in G$,
- $g_i^{g_0} = (g_i^{-1})^{g_1 \cdots g_{i-1}}$, $i = 1, ..., r_1$.
- $g_{r_1+2i-1}^{g_0} = (g_{r_1+2i}^{-1})^{g_1 \cdots g_{r_1}}$, $i = 1, ..., r_2$.

Thus, $\mathbf{g}$ defines - via $BCD_{\underline{\gamma}}$ - a G-cover defined over $\mathbb{R}$ with branch point tuple $\mathbf{t}' = (\overline{\zeta}_{o_1}, \zeta_{o_1}, 2\overline{\zeta}_{o_2}, 2\zeta_{o_2})$ if $o_1, o_2 >$.

(2) p-adic G-covers : Let k be a complete valued field of characteristic 0 and of residue characteristic p. Suppose given $\{x_1, y_1, x_2, y_2\} \in \mathcal{U}^4(k)$ and consider the conditions above :

(*) $|x_i - y_i| < |x_1 - x_2||p|^{\frac{1}{p-1}}$, $i = 1, 2$ (with the convention $|p|^{\frac{1}{p-1}} = 1$ if $p = 0$).
(**) x_i, y_i lie in the same coset, $i = 1, 2$ and x_1, x_2 lie in pairwise distinct cosets.

where $a, b \in k$ lie in the same coset means that either $|a|, |b| \leq 1$ and $|a - b| < 1$ or $|a|, |b| > 1$.

Take for instance $x_1^p := 1$, $y_1^p := p + 1$, $x_2^p := p^{-2}$, $y_2^p := p^{-2} + 1$. Then $|x_1^p| = |y_1^p| = 1 \geq 1$ and $|x_1^p - y_1^p| = |p| < 1$, $|x_1^p| = |y_1^p| = |p|^{-2} > 1$ so condition (**) is fulfilled. As for condition (*), one has $|x_1^p - x_2^p| = |p|^{-2}$ so $\max\{|x_1^p - y_1^p||x_2^p - y_2^p|, \} = |p| < |p|^{\frac{1}{p-1}}|x_1^p - x_2^p|$. Futhermore, any G-cover $f_i : X_i \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ with group $< g_i >$, inertia canonical invariant $(\{g_i\}, \{g_i^{-1}\})$ and branch points (x_i^p, y_i^p) is defined over $\mathbb{Q}(\zeta_{o_i}) \subset \mathbb{Q}(\zeta_m)$ and has a $\mathbb{Q}(\zeta_{o_i})$-rational unramified point the fiber above which is totally $\mathbb{Q}(\zeta_{o_i})$-rational, $i = 1, 2$. condition (**) allows us to glue together - viarigid geometry [L95] - the G-covers $f_1 \times_{\mathbb{Q}(\zeta_{o_1})} \mathbb{Q}(\zeta_m)_P$ and $f_2 \times_{\mathbb{Q}(\zeta_{o_2})} \mathbb{Q}(\zeta_m)_P$ to get a G-cover $f : X \to \mathbb{P}^1_{\mathbb{Q}(\zeta_m)_P}$ defined over $\mathbb{Q}(\zeta_m)_P$ with invariants G, $\mathbf{C}$, $(x_1^p, x_2^p, y_1^p, y_2^p)$. By proposition 1.4 and remark 1.6 of [DE03], condition (*) is enough to assert f is a HM-G-cover.

The second step relies on the following technical lemma

Lemma 6.10 *Let $\{x, z, \overline{z}\}, \{x', z', \overline{z}'\} \in \mathcal{U}_3(\mathbb{C})$ then the single homography $\phi \in \mathrm{PSL}_2(\mathbb{C})$ sending $(x, z, \overline{z})$ on to $(x', z', \overline{z}')$ is in $\mathrm{PSL}_2(\mathbb{Q}(x, x', \mathrm{Re}(zz'), \mathrm{Im}(zz')))$.*

In particular, this yields the final remark of theorem 6.8. □

In the statement of theorem 6.8, the places of residue characteristic dividing $|G|$ have to be excluded. This is a technical - but essential, if considering the Hasse property ! - hypothesis required to be sure the G-covers we build are HM-G-covers [DE03]. To my knowledge, there is no proof yet concerning the existence of HM-G-covers defined over complete field of residue characteristic dividing $|G|$ so one step is still missing to apply the Hasse principle to HM-components. However, if removing the HM-hypothesis, one can prove exactly as above but without the (**) condition :

Theorem 6.11 (Hasse Condition) *Let G be a finite group and $\mathbf{C} = (C_1, C_1^{-1}, C_2, C_2^{-1})$ a symetric 4-tuple of non trivial conjugacy classes. Assume $\overline{\mathrm{hm}}(\mathbf{C}) \neq \emptyset$. Then there exists a finite cyclotomic extension $\mathbb{Q}'_{\mathbf{C}}/\mathbb{Q}$ such that for any place v of $\mathbb{Q}'_{\mathbf{C}}$, there exists a G-cover f_v defined over $(\mathbb{Q}'_{\mathbf{C}})_v$ with invariants G, $\mathbf{C}$, $(t_v, 0, 1, 2)$.*

6.2.2.2 Using Pop's Half Riemann Existence Theorem

We retain the notations of the paragraph above. Given a prime p and a place P of $\mathbb{Q}'_{\mathbf{C}}$ dividing p, we consider the valuation v associated with P. Write $o_i = p^{u_i} m_i$ with $p \not| m_i$, $i = 1, 2$ and choose, for instance, $\mathbf{t}'^p = (x_1^p, y_1^p, x_2^p, y_2^p) \in \mathcal{U}^4(\mathbb{Q})$ as follows : $x_1^p = 0$, $x_2^p = 1$, $y_i^p = x_i + p^{u_i+2}$, $i = 1, 2$. One immediately checks that

$$v(x_i^p - y_i^p) - \frac{u_i + 1}{p - 1} v(p) = (u_i + 2 - \frac{u_i + 1}{p - 1}) v(p) \geq v(p) > 0 = v(x_1^p - x_2^p)$$

As a result, by proposition 3.27 (which is based on Pop's Half Riemann Existence Theorem [P94]), the number $|\overline{\mathrm{sni}}_{\mathbf{t}'}^{(\mathbb{Q}'_{\mathbf{C}})_v}(\mathbf{C})|$ of G-cover defined over $\mathbb{Q}'_{\mathbf{C}}$ with invariants G, $\mathbf{C}$, $\mathbf{t}$ verifies

$$|\overline{\mathrm{sni}}_{\mathbf{t}'}^{(\mathbb{Q}'_{\mathbf{C}})_v}(\mathbf{C})| \geq |\overline{\mathrm{hm}}(\mathbf{C})|$$

Now, using one more time lemma 6.10, we get

Proposition 6.12 *Let G be a non abelian finite group and $\mathbf{C} = (C_1, C_1^{-1}, C_2, C_2^{-1})$ a symmetric 4-tuple of non trivial conjugacy classes of G. Assume there is a $\Pi_{1,4}$-orbit $O \in \overline{\mathrm{sni}}(\mathbf{C})/\Pi_{1,4}$ such that $|\overline{\mathrm{sni}}(\mathbf{C})| - |O| > |\overline{\mathrm{hm}}(\mathbf{C})|$ then there exists a cyclotomic extension $\mathbb{Q}'_{\mathbf{C}}/\mathbb{Q}$ such that, denoting by $\mathcal{H}'_{4,G}(O)$ the geometrically irreducible component of $\mathcal{H}'_{4,G}(_mathbfC)$ corresponding to $SH_4.O$ one has :*

(i) $\mathcal{H}'_{4,G}(O)$ is defined over $\mathbb{Q}'_{\mathbf{C}}$ and, for any $\mathbf{t}' \in \mathcal{U}^3$, $\mathcal{H}'_{4,G}(O)_{\mathbf{t}'}$ remains geometrically irreducible.

(ii) For any place v of $\mathbb{Q}'_{\mathbf{C}}$, $\mathcal{H}'_{4,G}(O)_{\mathbf{t}'_{\mathbf{C}}}$ carries $(\mathbb{Q}'_{\mathbf{C}})_v$-points corresponding to G-covers defined over $(\mathbb{Q}'_{\mathbf{C}})_v$, where $\mathbf{t}'_{\mathbf{C}} = (0,1,2) \in \mathcal{U}^3(\mathbb{Q})$.

Proof. To prove (i), it is enough to prove that there is no other $\Pi_{1,4}$-orbit $O' \neq O \in \overline{\mathrm{sni}}(\mathbf{C})/\Pi_{1,4}$ such that $|O| = |O'|$ since this directly implies that $O = SH_4.O$. First, note that $|\overline{\mathrm{sni}}(\mathbf{C})| \geq 2|\overline{\mathrm{hm}}(\mathbf{C})|$. Indeed, the map

$$\begin{array}{rccc} a_{1,2}: & \overline{\mathrm{hm}}(\mathbf{C}) & \to & a_{1,2}.\overline{\mathrm{hm}}(\mathbf{C}) \\ & (g_1, g_1^{-1}, g_2, g_2^{-1}) & \to & (g_1^{g_2}, g_1^{-1}, g_2^{g_1}, g_2^{-1}) \end{array}$$

is a bijection and, since $G =< g_1, g_2 >$ is a non abelian group, one necessarily has $g_1 \neq g_1^{g_2}$ that is, $\overline{\mathrm{hm}}(\mathbf{C}) \cap a_{1,2}.\overline{\mathrm{hm}}(\mathbf{C}) = \emptyset$. So, if there exists $O' \neq O \in \overline{\mathrm{sni}}(\mathbf{C})/\Pi_{1,4}$ such that $|O| = |O'|$ then $|\overline{\mathrm{hm}}(\mathbf{C})| > |\overline{\mathrm{sni}}(\mathbf{C})| - |O| > \overline{\mathrm{hm}}(\mathbf{C}) \geq |O|$ and thus $|\overline{\mathrm{hm}}(\mathbf{C})| = 2|\overline{\mathrm{hm}}(\mathbf{C})| - |\overline{\mathrm{hm}}(\mathbf{C})| < |\overline{\mathrm{sni}}(\mathbf{C})| - |O| < |\overline{\mathrm{hm}}(\mathbf{C})|$: a contradiction. For (ii), the discussion above shows that for any place v of $\mathbb{Q}'_{\mathbf{C}}$ above a given prime p, $\mathcal{H}'_{4,G}(O) \cap (\Pi'_{4,G})^{-1}(\mathbf{t}'^p)$ carries $(\mathbb{Q}'_{\mathbf{C}})_v$-points corresponding to G-covers defined over $(\mathbb{Q}'_{\mathbf{C}})_v$; conclude using lemma 6.10. □

6.2.3 Description of the Hasse-genus 0 method for $r = 4$

Starting from a finite (non abelian) group G and a symetric 4-tuple $\mathbf{C} = (C_1, C_1^{-1}, C_2, C_2^{-1})$ of non trivial conjugacy classes of G, we can now give a general procedure to test the existence of $\mathbb{Q}'_{\mathbf{C}}$-points on $\mathcal{H}'_{4,G}(\mathbf{C})$. Indeed, suppose there exists a $\Pi_{1,4}$-orbit $O \in \overline{\mathrm{sni}}(\mathbf{C})/\Pi_{1,4}$ such that :

(G) $g_O = 0$.
(H) One of the three following condition is fulfilled :

(1) $O = \overline{\mathrm{sni}}(\mathbf{C})$.
(2) $|\overline{\mathrm{sni}}(\mathbf{C})| - |O| > |\overline{\mathrm{hm}}(\mathbf{C})|$
(3) G is a p-group and there is only one HM-orbit $O^{HM}(\mathbf{C}) \in \overline{\mathrm{sni}}(\mathbf{C})/SH_4$ and $O = O^{HM}(\mathbf{C})$.

Let $\mathbb{Q}'_{\mathbf{C}}$ be as in the preceeding paragraph and write $\mathbf{t}' := (0,1,2)$. Condition (G) implies that $\mathcal{H}'_{4,G}(O)_{\mathbf{t}'_{\mathbf{C}}}$ is a geometrically irreducible genus 0 curve defined over $\mathbb{Q}'_{\mathbf{C}}$, conditions (H) (1)-(2) that for any place v of $\mathbb{Q}'_{\mathbf{C}}$, $\mathcal{H}'_{4,G}(O)_{\mathbf{t}'_{\mathbf{C}}}$ carries $(\mathbb{Q}'_{\mathbf{C}})_v$-points corresponding to G-covers defined over $(\mathbb{Q}'_{\mathbf{C}})_v$ (*cf.* propositions 6.11 and 6.12) and condition (H) (3) that for any place v of $\mathbb{Q}'_{\mathbf{C}}$ not dividing p, $\mathcal{H}'_{4,G}(O)_{\mathbf{t}'_{\mathbf{C}}}$ carries $(\mathbb{Q}'_{\mathbf{C}})_v$-points corresponding to G-covers defined over $(\mathbb{Q}'_{\mathbf{C}})_v$ (*cf.* proposition 6.8). Now, apply proposition 6.6 (i) for (H) (1)-(2) and (ii) for (H) (3), observing that, for (H) (3), $\mathbb{Q}'_{\mathbf{C}}/\mathbb{Q}$ is a cyclotomic extension only containing p^nth roots of 1 so the only prime which ramifies in $\mathbb{Q}'_{\mathbf{C}}/\mathbb{Q}$ is p and it is totally ramified that is there is only one place v of $\mathbb{Q}'_{\mathbf{C}}$ dividing it. Finally, conclude that

Theorem 6.13 (Hasse-genus 0 method) *If (G) and (H) are fulfilled then there exists a G-cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ with invariants G, $\mathbf{C}$, $(t_f, \mathbf{t}')$ and field of moduli $\mathbb{Q}'_{\mathbf{C}}$. Furthermore, this G-cover is a HM-G-cover.*

Remark 6.14 We have presented our Hasse-genus 0 method for standard Hurwitz curves but it can be generalized to any kind of symmetrised Hurwitz curves (*cf.* [Ma89]) as well as for reduced Hurwitz curves (*cf.* [DF99], [BF02]) since, when $r = 4$, any k-point of the reduced Hurwitz space lifts to a k-point on the inner Hurwitz space, [DF99], proposition 6.8. Furthermore, the use of symmetrised Hurwitz curves or reduced Hurwitz curve is all the more interesting that they are often defined over smaller number fields than standard Hurwitz curves.

Bibliographie

[BF02] P. Bayley et M. Fried, *Hurwitz monodromy, spin separation and higher levels of Modular Towers*, Proceedings of the Von Neumann Symposium on Arithmetic Fundamental Groups and Noncommutative Algebra (MSRI 1999), Proceedings of Symposia in Pure Mathematics, AMS, ed. par M. Fried et Y. Ihara, 2002.

[Be89] S. Beckmann, *Ramified primes in the field of moduli of branched coverings of curves*, J. Algebra, **125**, p.236-255, 1989.

[Bi74] J.S.Birman, *Braids, links and mapping class groups*, Princeton University Press, 1974.

[C04a] A. Cadoret, *Thèse de doctorat*, to appear.

[C04b] A. Cadoret, *Counting real Galois covers of the projective line*, Pacific J. Math **219** No 1, p.101-129, 2005.

[C04c] A. Cadoret, *Harbater-Mumford subvarieties of moduli spaces of covers*, Preprint.

[C04d] A. Cadoret, *Rational points on Hurwitz towers*, Preprint.

[CoH85] K. Coombes et D.Harbater *Hurwitz families and arithmetic Galois groups*, Duke Math.J.,**52**, p.821-839,
1985.

[CoRo04] J.-M. Couveignes et N. Ros *Des obstructions globales à la descente des revêtements*, to appear, Acta Arithmetica.

[D92] P. Dèbes *Critère de descente pour le corps de définition des G-revêtements de* $\mathbb{P}^1$, C.R. Acad. Sci. Paris, t.315, série I, p. 863-868, 1992.

[D95] P. Dèbes *Covers of* $\mathbb{P}^1$ *over the p-adics*, in Recent Developments in the Inverse Galois Problem, Contemporary Math. **186**, p. 217-238, 1995.

[D04] P. Dèbes *Modular Towers, construction and diophantine questions*, Preprint, 2004.

[DDes04] P.Dèbes et B. Deschamps, *Corps ψ-libres et théorie inverse de Galois infinie*, J. fur die reine und angew. Math., **574**, p. 197-218, 2004.

[DDo97] P.Dèbes and J.-C. Douai, *Algebraic covers : field of moduli versus field of definition*, Annales Sci. E.N.S., **30**, p. 303-338, 1997.

[DDo98] P. Dèbes and J.-C. Douai, *Local-global principles for algebraic covers*, Israel Journal of Math. **103**, p.237-257, 1998.

[DDoMo04] P.Dèbes,J.-C.Douai, L. Moret-Bailly, *Descent varieties for algebraic covers*, J. fur die reine und angew. Math. **574**, p. 51-78, 2004.

[DE03] P. Dèbes and M. Emsalem, *Harbater-Mumford Components and Towers of Moduli Spaces*, preprint, 2003.

[DF94] P. Dèbes and M. Fried, *Nonrigid Constructions in Galois Theory*, Pacific J. Math. **163** No.1, p.81-122, 1994.

[DF99] P. Dèbes and M. Fried, *Integral spacialization of families of rational functions*, Pacific J. Math. **190** No.1, p.45-85, 1999.

[DH98] P. Dèbes and D. Harbater, *Fields of definition of p-adic covers*, J. fur die reine und angew. Math, **498**, p.223-236, 1998.

[Des95] B. Deschamps, *Existence de points p-adiques pour tout p sur un espace de Hurwitz*, Proceedings AMS-NSF Summer Conference, **186**, Cont. Math. series, Recent Developments in the Inverse Galois Problem, p.111-171, 1995.

[Det00] M. Dettweiler, *Plane curve complements and curves on Hurwitz spaces*, Preprint, 2000.

[Di58] L.E. Dickson, *Linear groups with an exposition of the Galois theory*, Dover, 1958.

[E01] M. Emsalem, *Espaces de Hurwitz*, in *Arithmétique des revêtements algébriques*, Séminaires et Congrès **5**, p. 63-99, 2001.

[F95a] M. Fried, *Introduction to Modular Towers :Generalizing the relation between dihedral groups and modular curves*, Proceedings AMS-NSF Summer Conference, **186**, Cont. Math. series, Recent Developments in the Inverse Galois Problem, p.111-171, 1995.

[F95b] M. Fried, *Topics in Galois theory*, expanded version of review of Serre's book with same title, Proceedings AMS-NSF Summer Conference, **186**, Cont. Math. series, Recent Developments in the Inverse Galois Problem, p.111-171, 1995.

[F04] M. Fried, *Higher rank modular towers*, preprint, 2004.

[FK97] M.Fried and Y.Kopeliovich, *Applying modular towers to the inverse Galois problem*, in *Geometric Galois Action*, London Math. Soc. Lecture Note Series **243**, L.Schneps and P.Lochak ed., Cambridge University Press, p. 151-175, 1997.

[FV91] M. Fried and H. Volklein, *The Inverse Galois Problem and Rational Points on Moduli Spaces*, Math. Ann. **290**, p. 771-800, 1991.

[GPR97] B.W.Green,F.Pop,P.Roquette, *On Rumely's Local-Global principle*, Jber.d.Dt.Math.-Verein **97**, p. 43-74, 1997.

[Gr61] A.Grothendieck, *Revêtements Etales et Groupe Fondamental- S.G.A. 1* Lecture Notes in Math. **224**, 1961.

[H87] D.Harbater, *Galois coverings of the arithmetic line*, Lecture Notes in Math. **1240**, p. 165-195, 1987.

[H03] D.Harbater, *Patching and Galois theory*, MSRI Publications series **41**, Cambridge University Press, p. 313-424, 2003.

[Ha77] R.Hartshorne, *Algebraic Geometry*, G.T.M. **52**, Springer-Verlag, 1977.

[HeR85] W. Herfort et L.Ribes, *Torsion elements and centralizers in free products of profinite groups*, J. fur die reine und angew. Math., **358**, p. 155-161, 1985.

[Ka98] S. Kamienny *On torsion in abelian varieties*, Communication in Algebra **26**, p. 1675-1678, 1998.

[L02] S. Lang *Algebra revised third edition*, GTM **211**, Springer-Verlag, 2002.

[L95] Q.Liu, *Tout groupe fini est groupe de Galois sur* $\mathbb{Q}_p(T)$, Contemporary Mathematics. **186**, p. 261-265, 1995.

[MMa99] G.Malle and H.B.Matzat *Inverse Galois Theory*, S.M.M., Springer-Verlag, 1999.

[Ma89] H.B. Matzat *Rationality criteria for Galois extensions*, in Ihara et al., Galois groups over $\mathbb{Q}$, Proc. Workshop Berkeley 1987, Publ. Math. Sci. Res. Inst. **16**, p. 361-383, Springer Verlag, 1989.

[Mi86] J.S. Milne , *Abelian varieties*, in *Arithmetic Geometry*, G. Cornell and J.H. Silverman ed., Springer-Verlag, 1986.

[Mo89] L.Moret-Bailly, *Groupes de Picard et problèmes de Skolem II*, Annales Sci. E.N.S., **22**, p.181-194, 1989.

[P94] F.Pop, *Half Riemann's existence theorem*, Algebra and Number Theory (G.Frey and J.Ritters, eds.), De Gruyter Proceedings in Mathematics, p. 1-26, 1994.

[P96] F.Pop, *Embedding problems over large fields*, Annals of math. **144**, p. 1-35, 1996. Cambridge Studies in Advanced Mathematics, **53**, Cambridge University Press, 1999.

[Ri04] E.Riboulet-Deyris , Thèse de doctorat, 2004.

[RZ00] L.Ribes and P.Zalesskii *Profinite Groups*, E.M.G. **40**, Springer-Verlag, 2000.

[R82] D. J.S.Robinson, *A Course in the Theory of Groups*, Springer-Verlag, GTM 80, 1982.

[RoW04] M.Romagny and S.Wewers *Hurwitz spaces*, Preprint, 2004.

[S89] J.-P.Serre, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, Friedr. Wieweg & Sohn, 1989.

[S92] J.-P.Serre *Topics in Galois theory*, Notes written by Henri Darmon, Jones and Barlett Publishers, Boston, 1992.

[S98] J.-P. Serre, *Représentation linéaire des groupes finis* (fifth edition), Hermann, 1998.

[Si92] A. Silverberg, *Points of finite order on Abelian varieties*, in *p-adic Methods in Number Theory and Algebraic Geometry*, Adolphson, Sperber, Tretkoff eds ; Contmporary Math. **133**, A.M.S., p. 175-193, 1992.

[Su86] M. Suzuki, *Group Theory I, II*, G.M.W. **247**, **248**, Springer-Verlag, 1986.

[V99] H.Volklein, *Groups as Galois groups - an introduction*, Cambridge Studies in Advanced Mathematics, **53**, Cambridge University Press, 1999.

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

[W98] S.Wewers, *Construction of Hurwitz Spaces*, Thesis, Preprint **21** of the IEM, Essen, 1998.

[W02] S. Wewers, *Field of moduli and field of definition of Galois covers*, Proceedings of Symposia in Pure Mathematics volume **70**, p. 221-245, 2002.

[Wi84] H. Wielandt, *Finite Permutation Groups*, Academic Press, 1984.

Résumé

Cette thèse aborde le problème de Galois inverse régulier via l'arithmétique des espaces de Hurwitz. La première partie - en français - comporte deux chapitres, l'un de préliminaires et l'autre de présentation détaillée des résultats. La seconde partie - en anglais - rassemble trois articles et un dernier chapitre original. Le chapitre 3 donne une méthode utilisant les caractères pour calculer le nombre de (G-)revêtements avec invariants fixés de corps des modules/ de définition réel. Cela permet en particulier d'exhiber de nombreuses familles infinies de groupes admettant des G-revêtements non définis sur leur corps des modules et de donner des réalisations régulières non rigides des groupes prodihédraux sur le corps des nombres algébriques totalement réels avec diviseur de ramification rationnel. On prouve au chapitre 4 un resultat de structure "à la Conway et Parker" pour les espaces de Hurwitz et les tours modulaires mais avec, en outre, une interprétation modulaire en terme de diviseur de ramification. Combiné aux techniques de recollement à la Harbater, aux variétés de descente et au principe local-global ce resultat permet de montrer, par exemple, que tout groupe fini G contenant deux classes de conjugaison A, B telles que $G =< A >=< B >$ et $G =< a, b >$ pour tout $a \in A$, $b \in B$ peut être réalisé régulièrement - ainsi que tous ses revêtements de Frattini - sur l'extension algébrique totalement p-adique (pour les places p ne divise pas $|G|$) d'un corps cyclotomique $k \subset \mathbb{Q}(e^{\frac{2\pi i}{|G|}})$ avec tous ses points de branchement $\mathbb{Q}$-rationnels sauf éventuellement un. Au chapitre 5, on montre qu'un groupe profini extension d'un groupe fini par un groupe pronilpotent projectif de rang fini ne peut être le groupe de Galois d'une extension réguliè re de corps des modules un corps de nombres. On montre aussi que la strong torsion conjecture pour les variétés abéliennes implique une conjecture de Fried pour les tours modulaires. Le chapitre 6, enfin, contient deux résultats sur les courbes de Hurwitz : une formule générique permettant de calculer leur genre et une méthode de genre 0 pour $r = 4$ utilisant le principe de Hasse.

Abstract

This thesis deals with the regular inverse Galois problem via the arithmetic of Hurwitz spaces. The first part - in french - is divided into a preliminary chapter and a survey chapter. The second part - in english - consists in three papers and a fourth original chapter. Chapter 3 gives a method based on character theory to compute the number of (G-)covers with given invariants and a real field of moduli/of definition. This method applies to the field of moduli/field of definition problem and to the non rigid regular realization of the prodihedral groups over the field of all the totally real algebraic numbers with a rational branch point divisor. Chapter 4 states a "Conway and Parker's" structure result for Hurwitz spaces and modular towers but with, furthermore, a modular interpretation in terms of branch points. This result, combined with Harbater's patching methods, descent varieties and local-global principle shows that any finite group G containing two conjugacy classes A, B such that $G =< A >=< B >$ and $G =< a, b >$ for all $a \in A$, $b \in B$ can be regularly realized - as well as all its Frattini covers - over the algebraic totally p-adic extension (for places p not dividing $|G|$) of a cyclotomic field $k \subset \mathbb{Q}(e^{\frac{2\pi i}{|G|}})$ with all its branch points except may be one $\mathbb{Q}$-rational. Chapter 5 shows that a profinite group which is an extension of a finite group by a pronilpotent projective group of finite rank can't be the Galois group of a regular extension with field of moduli a number field. It also shows the strong torsion conjecture for abelian varieties implies one of Fried's conjectures for modular towers. Eventually, chapter 6 is about standard Hurwitz curves ; it gives a general formula to compute their genus and describe a genus 0 method for $r = 4$ based on the Hasse principle.