Université de Lille

Laboratoire Paul Painlevé

THÈSE

présentée pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LILLE

École Doctorale MADIS-631

par

Béranger SEGUIN

Géométrie et arithmétique des composantes des espaces de Hurwitz

---

Sous la direction de Prof. Pierre DÈBES et de Prof. Ariane MÉZARD

Soutenue le 06/07/2023 devant le jury composé de :

Jean-Marc COUVEIGNES	Professeur, Université de Bordeaux	Rapporteur
Pierre DÈBES	Professeur, Université de Lille	Directeur
Mladen DIMITROV	Professeur, Université de Lille	Président du jury
Ariane MÉZARD	Professeur, École Normale Supérieure, Paris	Directrice
Tamás SZAMUELY	Professor, Università degli studi di Pisa	Examinateur
Craig WESTERLAND	Associate Professor, University of Minnesota	Rapporteur

Univ. Lille, CNRS, UMR 8524 - Laboratoire Paul Painlevé, F-59000 Lille, France.

D.M.A., École Normale Supérieure, 45 rue d'Ulm, 75005 Paris, France

GÉOMÉTRIE ET ARITHMÉTIQUE DES COMPOSANTES DES ESPACES DE HURWITZ

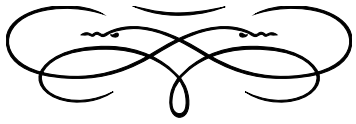
Résumé en français

Les espaces de Hurwitz sont des espaces de modules qui classifient les revêtements ramifiés de la droite projective sur lesquels un groupe G, fixé, agit. Leurs propriétés géométriques et arithmétiques sont liées à des questions de théorie des nombres, et notamment au problème de Galois inverse. Dans cette thèse, on étudie les composantes connexes de ces espaces. Dans un premier temps, on démontre des résultats concernant l'évolution du nombre de composantes connexes des espaces de Hurwitz à mesure que le nombre de points de branchement des revêtements qu'ils classifient augmente. Dans un second temps, on démontre des résultats de stabilité, sous l'opération de recollement des composantes connexes des espaces de Hurwitz, de leur corps de définition. Ces résultats relient les propriétés topologiques et arithmétiques des revêtements. Trois chapitres d'exposition, dénués d'énoncés originaux, présentent les différents objets étudiés. Dans un appendice, on résume la thèse à l'attention du grand public.

Summary in English

Hurwitz spaces are moduli spaces that classify ramified covers of the projective line on which a fixed group G acts. Their geometric and arithmetic properties are related to number theoretical questions, particularly the inverse Galois problem. In this thesis, we study the connected components of these spaces. Firstly, we prove results concerning the asymptotical behaviour of the count of connected components of Hurwitz spaces as the number of branch points of the covers they classify grows. Secondly, we establish stability results for fields of definitions of connected components of Hurwitz spaces under the gluing operation. These results relate topological and arithmetical properties of covers. Three expository chapters, devoid of original statements, present the various objects. In an appendix, we summarize the thesis for the general public.

Remerciements



À Michel Deiss.

Il est traditionnel de commencer un manuscrit de thèse par des remerciements. Je dois confesser que l'exercice m'angoisse sévère – pas que je manque de personnes chères à qui crier merci, ou de gratitude à l'égard de celleux qui m'ont aidé, mais ma tendance « complétiste » me fait craindre si fort d'oublier des gens *absolument essentiels* (« mais si ! c'est lui qui m'a donné un stylo le jour où... ») que mes tentatives se transforment instantanément en liste, et perdent par là la chaleur qui donne en principe son intérêt à ce rituel. Chaleur qui, d'ailleurs, ne me vient pas toute seule sous les doigts – une sorte de pudeur, de timidité, me rend compliqué d'être aussi affectueux avec chacun·e que ce que mon cœur et mon instinct premier me commandent (ne sommes-nous pas sous l'œil sérieux de mes collègues ?). Aussi, je le dis tout de suite puisque sinon ça me hantera éternellement : par pitié, ami·e, ne t'indigne pas de ne pas te trouver nommé·e ici, ou de ne te deviner que sous la forme d'une initiale indistincte perdue au fin fond d'une liste – je te jure qu'il me sera cent fois plus agréable de te remercier en personne qu'ici, par un mot, par une poignée de mains, ou par un câlin (selon notre degré d'amitié). C'est dit. D'ailleurs, je ne donne pas d'explication au naturel variable avec lequel je nomme chacun·e : certain·e·s sont nommé·e·s en entier, d'autres n'ont qu'un prénom ou qu'une initiale ; aucune raison personnelle à ça, juste une sorte d'instinct rythmique (quasiment dicté par l'euphonie) selon le contexte et la nature du paragraphe. Vous voilà prévenu·e·s. Mes remerciements vont donc, sans ordre particulier :

À Ariane Mézard et Pierre Dèbes pour leur aide ininterrompue tout au long de ces trois années, pour leur générosité et leur bienveillance de chaque instant, pour leurs relectures nombreuses et toujours attentives de mon travail ainsi que pour leurs encouragements. Trois ans à vos côtés m'ont tant appris, tant fait grandir, tant façonné, que j'avoue avoir un frisson de panique à l'idée de quitter votre aile affable et d'essayer de voler des miennes. Merci du fond du cœur.

À Jean-Marc Couveignes et Craig Westerland pour avoir accepté d'être rapporteurs de cette thèse. À Olivier Benoist, Paul Cahen, François Charles, Gaëtan Chenevier, Nicolas Guès, Qing Liu, Dorian Ni, Maxime Ramzi, Silvain Rideau–Kikuchi, Raphaël Ruimy et Arnaud Vanhaecke qui ont chacun apporté de l'aide mathématique à un point ou un autre de ce manuscrit – parfois sans le savoir. À Andrea Bianchi, Jordan Ellenberg, Danny Neftin et Craig Westerland pour leur curiosité à l'égard de ce travail, et pour leurs questions intéressantes. À Tamás Szamuely pour son accueil chaleureux à Budapest (il y a longtemps déjà) durant lequel j'ai été exposé, puis ai pris goût, à la théorie des nombres ; merci à lui, ainsi qu'à Mladen Dimitrov, d'avoir accepté de faire partie du jury.

À mes collègues doctorant·e·s au DMA dont la conversation quotidienne – mathématique ou non – rend mes jours plus gais, en particulier Samuël, Coline, Arnaud, Vadim, Stefan, Nataniel et Paul. Aux mathématicien·ne·s d'ailleurs avec qui j'ai plaisir à discuter, notamment

Petra Flurin, Cécile Gachet, Robin Khanfir, André Leroy et Antoine Soulas. Au peuple joyeux de l'institut Fourier, qui m'a fait voir Grenoble sous son meilleur jour – jusqu'à ses hauteurs baignées de soleil et de chants.

Au lycée Fabert, sa MPSI2 et sa MP*, aux cours d'Anne Lux et de Jean-Denis Eiden ; à l'amitié précieuse et durable de Claire, Stan, Ilias, Guillaume et Marc-André. Au lycée Poncelet et son AbiBac, à Danielle Monnet et Jean-Yves Pennerath ; à Emeric, Marie et Fabian. Au collège Lucien Pougué, à Michel Deiss et Jean-Marc Ettenhuber ; à Maxence, Albin et Arnaud.

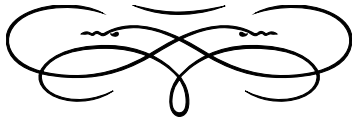
À ma mère, mon frère et ma sœur, ainsi qu'à mes grands-parents, pour tout ce qui nous unit et pour tout ce que je vous dois – mais notamment, ici, pour avoir offert à l'enfant puis à l'adolescent que j'étais un cadre propice (sur le plan de l'affection, des conditions matérielles, et de la stimulation intellectuelle) à mon épanouissement mathématique.

À mes ami·e·s Luc, Pablo, Lucie, Paul-Nicolas, Thibault, Lila, Thomas, Adélaïde et Théophile, pour votre hospitalité infinie, pour votre conversation toujours bienveillante et riche, et pour les soirées ~~JdR~~ crêpes de la plus grande qualité. À mes colocataires d'un temps durant cette thèse : M.D., A.F., L.G.–G., R.K., R.R. (à Villejuif), A.A., E.B., L.G., C.P., I.S., E.S., L.S., P.T., A.T. (à Cabourg), A.B., B.D., H. J.–I. (à Ivry), D.-I. R., A.T., F.T., N. (à Athis-Mons), C.F., S.M., N.P. (à Vitry) – à vous toustes, félicitations pour m'avoir supporté.

Aux Guès What, dont le jazz s'est trouvé au sein de mon emploi du temps en lutte constante contre les espaces de Hurwitz : merci à Emma, Valentin, Ulysse, Nicolas et François pour les moments de musique, les concerts, les révélations métaphysiques et les discussions nerdyshitpostesques. À l'Ernestophone, à Rise Up 3, et aux personnes bienveillantes et hautes en couleurs que j'y ai rencontrées – citons L.G., E.L.G., L.L., L.N., S.N.H., M.P. et G.S.–P. Aux ami·e·s musicien·ne·s en général – notamment Alexis, Yohan et Philibert. À la musique de Weather Report et de Casiopea. Aux chansons d'Anne Sylvestre, de Georges Brassens et de Michel Legrand. À Stravinsky.

Au séminaire souterrain Ktorphée et à son penchant pour Scriabine. À LibGen et Sci-Hub, à Aaron Schwartz, à Alexandra Elbakyan et à la science ouverte. Au crêpier de chez Nicos. À Garance que j'aime tout plein. À la vie, au soleil, à l'amour, et aux mathématiques dans ce qu'elles ont de joyeux et de festif.

Table des matières



Chapitre 1

Introduction (français)

(An English version of this introduction may be found on page 27.)

Organisation du chapitre

Cette thèse est consacrée à l'étude des composantes connexes des *espaces de Hurwitz*, espaces de modules de revêtements qui sont en lien avec des questions de théorie des nombres – notamment, le problème de Galois inverse. Nous nous intéressons à leurs composantes sous deux angles distincts :

— Dans un premier temps, nous nous intéressons au comportement *combinatoire* des composantes connexes des espaces de Hurwitz : que peut-on dire du comportement limite du nombre de ces composantes lorsque le nombre de points de branchement des revêtements augmente ?

  Cette question est au cœur des chapitres 5 à 7. Elle reprend des problématiques soulevées par les travaux d'Ellenberg, Tran, Venkatesh et Westerland, qui ont mis en évidence les liens entre l'homologie des espaces de Hurwitz et la distribution des corps de fonctions sur les corps finis [EVW16 ; EVW12 ; ETW17].

— Dans un second temps, nous considérons les propriétés *arithmétiques* des composantes des espaces de Hurwitz, et notamment leurs corps de définition.

  La construction de composantes ayant un petit corps de définition est une étape nécessaire à la résolution du problème de Galois inverse régulier – c'est donc une forme faible de ce problème. Cette question occupe le chapitre 8.

Dans les deux situations, tant pour compter les composantes que pour étudier leurs corps de définition, une même opération géométrique occupe une place centrale dans notre travail : il s'agit du *recollement* des composantes. L'importance combinatoire de cette opération est déjà manifeste dans [EVW16], et son rôle arithmétique dans [Cau12] ; nous faisons des efforts pour unifier les points de vue de ces auteurs afin de tirer tout le potentiel de leurs méthodes.

L'introduction est organisée de la façon suivante : dans la section 1.1, nous présentons les objets et questions dont nous nous préoccupons, en détaillant les motivations derrière leur étude. Nous présentons nos principaux résultats dans la section 1.2. Dans la section 1.3, nous précisons le contenu de chacun des chapitres. Enfin, nous fixons quelques notations communes à l'ensemble du texte dans la section 1.4.

1.1. Thèmes abordés

Les objets centraux de cette thèse sont les **espaces de Hurwitz**. Un groupe fini G et un entier n étant fixés, les espaces de Hurwitz sont des espaces de modules qui classifient les G-revêtements ramifiés en n points – le plus souvent, nous considérons des revêtements de la droite projective $\mathbb{P}^1$. Il existe diverses sortes d'espace de Hurwitz, selon qu'on ordonne ou non les points de branchement, qu'on munisse ou non les revêtements d'un point marqué, qu'on exige ou non que les revêtements soient connexes, etc.

La géométrie de ces espaces de modules traduit le fait qu'on puisse déformer un revêtement de manière continue à mesure que ses n points de branchement se déplacent en restant distincts. Les espaces de Hurwitz sont eux-mêmes des revêtements finis, non ramifiés et non nécessairement connexes, des espaces de configurations de n points de la droite. Pour cette raison, les propriétés géométriques de ces espaces proviennent en grande partie de faits combinatoires concernant les groupes de tresses et leur action sur les listes d'éléments de G.

On peut aborder les espaces de Hurwitz d'un point de vue purement géométrique – ce sont alors des espaces topologiques ou analytiques –, mais également d'un point de vue algébrique – ce sont alors des schémas ou des champs.

1.1.1. Motivations pour l'étude géométrique et arithmétique des espaces de Hurwitz

Le versant algébrique des espaces de Hurwitz donne un sens à la recherche de **points rationnels**, et notamment de K-points lorsque K est un corps de nombres.

À des complications près (ces espaces de modules n'étant en général pas fins), les K-points des espaces de Hurwitz correspondent aux G-revêtements ramifiés de $\mathbb{P}^1_K$, c'est-à-dire – en supposant de plus ces revêtements irréductibles – à des extensions galoisiennes de $K(t)$ dont le groupe de Galois est G.

Le théorème d'irréductibilité de Hilbert établit qu'une telle extension peut être spécialisée en une extension de K dont le groupe de Galois est G. Pour cette raison, les espaces de Hurwitz sont un outil de choix pour l'étude du **problème de Galois inverse**, qui est la question de savoir si tout groupe fini est groupe de Galois d'une extension du corps des nombres rationnels. Si, par exemple, G est un groupe fini de centre trivial, il suffit pour le réaliser comme groupe de Galois d'une extension de $\mathbb{Q}$

de trouver un $\mathbb{Q}$-point d'un espace de Hurwitz de G-revêtements ramifiés connexes de la droite projective.

Par ailleurs, la question du dénombrement des $\mathbb{F}_q$-points des espaces de Hurwitz, lorsque q est premier avec $|G|$, est liée à la distribution des extensions de $\mathbb{F}_q(T)$ ayant un groupe de Galois donné, et donc à la **conjecture de Malle** sur les corps de fonctions sur les corps finis.

Cette piste a été explorée dans les articles [EVW16 ; EVW12 ; ETW17]. Ces articles mettent en évidence une stratégie pour le problème du dénombrement des extensions de corps qui repose sur les mêmes principes que la démonstration des conjectures de Weil : l'étude géométrique des espaces de Hurwitz, et notamment de leur **homologie**, est au cœur de cette approche.

1.1.2. Opérations de recollement et composantes des espaces de Hurwitz

Considérons deux G-revêtements ramifiés marqués de la droite complexe (projective ou affine) dont les groupes de monodromie respectifs sont des sous-groupes H et H' de G. On suppose que les lieux de ramifications de ces deux revêtements sont disjoints, et qu'ils comportent respectivement n et n' points de branchement. Il est possible de **recoller** ces revêtements afin d'obtenir un G-revêtement marqué, ramifié en $n + n'$ points, dont le groupe de monodromie est le sous-groupe de G engendré par H et H'.

Cette opération peut être décrite en termes combinatoires : une bijection relie les G-revêtements marqués, ramifiés en n points fixés, et les n-uplets $(g_1, \dots, g_n)$ d'éléments de G (avec la condition additionnelle que le produit $g_1 g_2 \cdots g_n$ vaille 1 dans le cas des revêtements de la droite projective). Pour recoller deux G-revêtements marqués, il suffit alors de concaténer les listes d'éléments de G correspondantes.

Les espaces de Hurwitz ne sont en général pas connexes, et leur non-connexité est une difficulté géométrique majeure. Étudier la géométrie d'une composante connexe prise indépendamment revient essentiellement à comprendre l'homologie des groupes de tresses ; il reste alors à comprendre comment combiner ces informations. Pour cela, il est nécessaire d'avoir une description fine des composantes connexes.

L'opération de recollement des G-revêtements marqués induit une opération au niveau des composantes des espaces de Hurwitz. Cet outil éclaire la question de la description de l'ensemble des composantes en munissant cet ensemble d'une structure algébrique. Plus précisément, on définit un *monoïde* et un *anneau* des composantes. Ces objets ont été introduits dans [EVW16], et ils sont centraux dans notre travail.

1.1.3. Dénombrement des composantes

On se pose la question du **nombre de composantes** des espaces de Hurwitz, et plus précisément du comportement asymptotique de ce nombre à mesure que le nombre de points de branchements augmente. Un outil important est la description combinatoire des revêtements : on compte les orbites, sous l'action du groupe des tresses, de n-uplets d'éléments de G. On utilise des invariants pour déterminer si deux n-uplets d'éléments de G (c'est-à-dire deux G-revêtements ramifiés en n points) sont dans la même orbite pour l'action du groupe des tresses (c'est-à-dire si les revêtements sont dans la même composante connexe).

La croissance du nombre de composantes est liée à des questions arithmétiques : le nombre de composantes connexes est le 0-ième nombre de Betti des espaces de Hurwitz, et il ressort de [EVW16 ; Tie16] que la dimension de l'homologie supérieure est contrôlée par ce nombre. En appliquant la formule de la trace de Grothendieck-Lefschetz et les majorations des valeurs propres du Frobenius par Deligne, on peut utiliser les nombres de Betti pour estimer le nombre de $\mathbb{F}_q$-points des espaces de Hurwitz. Cela permet de **compter les extensions** de $\mathbb{F}_q(T)$ ayant G pour groupe de Galois. Cette stratégie permet à Ellenberg, Tran et Westerland de démontrer la borne supérieure de la conjecture de Malle sur $\mathbb{F}_q(T)$.

En généralisant l'anneau des composantes de [EVW16] aux G-revêtements de la droite projective, on obtient un anneau gradué commutatif de type fini, dont la fonction de Hilbert compte les composantes des espaces de Hurwitz en fonction du nombre de points de branchement. La croissance de la fonction de Hilbert d'un anneau gradué correspond à des propriétés géométriques de son spectre, telles que la dimension et le degré : cela motive notre étude plus systématique de la géométrie des spectres des anneaux de composantes des espaces de Hurwitz (Chapitre 5).

Dans la situation historique des $\mathfrak{S}_d$-revêtements de la droite projective dont les éléments locaux de monodromie sont des transpositions, on donne une formule exacte pour le compte des composantes des espaces de Hurwitz (Théorème 6.1.2), et on décrit le spectre de l'anneau des composantes (Théorème 6.1.3).

1.1.4. **Corps de définition des composantes**

La question de déterminer quelles sont les composantes connexes des espaces de Hurwitz qui sont définies sur $\mathbb{Q}$ – et en particulier d'en isoler certaines qui sont susceptibles de contenir des points rationnels – est abordée dans [FV91 ; DE06 ; Cau12 ; EVW12]. Nous nous concentrons sur le problème de la **stabilité du corps de définition des composantes des espaces de Hurwitz sous l'opération de recollement** (la question 8.1.1). Cette problématique figure déjà dans [DE06 ; Cau12] mais nous choisissons de lui donner une place centrale.

Notre démarche s'inscrit dans la recherche d'opérations de recollement sur des corps non algébriquement clos. Par exemple, sur un corps valué complet, l'opération de *patching* introduite par Harbater [Har03] entraîne une réponse positive au problème de Galois inverse régulier – il suffit de recoller des revêtements dont le groupe est cyclique. Dans notre cas, nous nous plaçons sur des corps de nombres, mais on affaiblit le problème en remplaçant les revêtements par des composantes d'espaces de Hurwitz – c'est-à-dire des familles géométriquement irréductibles de revêtements. L'opération de recollement, d'origine géométrique, est très « transcendante » : on ne s'attend pas a priori à ce qu'elle ait de bonnes propriétés arithmétiques. Nous démontrons le théorème 8.1.2, qui apporte une réponse positive à la question dans des situations multiples. La démonstration de ce résultat utilise des outils divers : un théorème de [Cau12] et des calculs de tresses ; le *lifting invariant* introduit dans [EVW12] ; la théorie du patching de Harbater [Har03].

1.2. Contributions

Les contributions de cette thèse sont concentrées dans les chapitres 4 à 6 (pour les résultats combinatoires/géométriques) et dans le chapitre 8 (pour les résultats arithmétiques). Les chapitres 2, 3 et 7 sont des chapitres d'exposition.

Dans ce qui suit, on récapitule les résultats principaux de chaque chapitre en donnant des descriptions rapides. On écrit volontiers des énoncés concis, plus faibles que ceux du manuscrit.

Chapitre 4 Counting Components of Hurwitz Spaces

Issu de [Seg22]

Résultat principal : Théorème 4.3.1

On fixe un groupe G et un ensemble D de classes de conjugaison de G. On fixe également une fonction $\xi : D \to \{1, 2, \dots\}$ qui attribue à chaque classe $\gamma \in D$ une « multiplicité ». Dans ce qui suit, X désigne soit la droite affine complexe $\mathbb{A}^1(\mathbb{C})$, soit la droite projective complexe $\mathbb{P}^1(\mathbb{C})$. Dans les deux cas, un point base t_0 est fixé.

On considère un sous-groupe H de G qui a une intersection non vide avec chaque classe de conjugaison $\gamma \in D$ et qui est engendré par les intersections $\gamma \cap H$ pour $\gamma \in D$ (Définition 3.2.20).

On désigne par $\pi_0\mathrm{CHur}^*(H, D_H, n\xi_H)$ l'ensemble des composantes connexes de l'espace de Hurwitz (Définition 3.2.15) des G-revêtements marqués ramifiés de (X, t_0) (Définitions 2.2.13 et 2.3.15) satisfaisant les propriétés suivantes :

— leur groupe de monodromie (Définition 2.2.18) est le groupe H ;
— leurs classes de monodromie (Définition 2.3.25), vues comme classes de conjugaison de G, appartiennent toutes à l'ensemble D ;
— une classe $\gamma \in D$ est la classe de monodromie en exactement $n\xi(\gamma)$ points de branchement.

Description du théorème 4.3.1. On obtient des estimations, lorsque l'entier n tend vers l'infini, du nombre de composantes suivant :

$$\mathrm{HF}_H(n) = |\pi_0\mathrm{CHur}^*(H, D_H, n\xi_H)|.$$

Dans tous les cas, la mesure principale de la croissance de ce nombre est le *nombre de délitement* $\Omega(D_H)$ (Définition 4.2.3) : il s'agit de la différence entre le nombre de classes de conjugaison de H qui sont incluses dans une classe de conjugaison de G appartenant à l'ensemble D, et le cardinal de l'ensemble D. Ce nombre mesure donc à quel point les classes de conjugaison de G appartenant à D tendent à se séparer en plusieurs classes de conjugaison lorsqu'on les intersecte avec le sous-groupe H.

Voici les estimations qu'on obtient, qui différent selon les situations :

— Lorsque X est la droite affine complexe $\mathbb{A}^1(\mathbb{C})$, on obtient un équivalent explicite dans tous les cas :

Forme concise du théorème 4.3.1 (i)

La fonction HF_H est équivalente à un monôme de degré $\Omega(D_H)$:

$$\mathrm{HF}_H(n) \underset{n\to\infty}{\sim} \alpha n^{\Omega(D_H)}.$$

On calcule le coefficient dominant α, dont l'expression fait intervenir le second groupe d'homologie de H.

— Lorsque X est la droite projective complexe $\mathbb{P}^1(\mathbb{C})$, l'énoncé le plus général est peu contraignant :

Théorème 4.3.1 (iv)

La fonction HF_H est un $O\left(n^{\Omega(D_H)}\right)$, mais n'est pas un $o\left(n^{\Omega(D_H)}\right)$.

En revanche, dans des situations particulières, on a davantage d'informations :

Forme concise des théorèmes 4.3.1 (ii) et 4.3.1 (iii)

On calcule un « coefficient dominant moyen » de HF_H dans les deux situations suivantes :

- le nombre de délitement $\Omega(D_H)$ est nul, c'est-à-dire que l'intersection des classes de conjugaison considérées (les éléments de D) avec le sous-groupe H sont des classes de conjugaison de H (voir la définition 4.2.2) ;
- l'ensemble D ne contient qu'une seule classe de conjugaison c de G, et $\xi(c) = 1$.

L'homologie du groupe H intervient dans l'expression du coefficient dominant.

Ces estimations généralisent certains des résultats de [EVW16] : les auteurs démontrent un phénomène de *stabilité homologique* lorsque $X = \mathbb{A}^1(\mathbb{C})$, $\Omega(D_H) = 0$, $D = \{c\}$ et $\xi(c) = 1$. Une manifestation de la propriété de stabilité est le fait que la fonction HF_H soit bornée dans ce cas.

Chapitre 5 The Geometry of Rings of Components of Hurwitz Spaces

Issu de [Seg22]

Résultats principaux : Théorèmes 5.1.4 et 5.5.13

Soit G un groupe fini, D un ensemble de classes de conjugaison de G, et ξ une application $D \to \{1, 2, \ldots\}$.

On note $\pi_0\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi)$ l'ensemble des composantes connexes de l'espace de Hurwitz des G-revêtements marqués ramifiés de $(\mathbb{P}^1(\mathbb{C}), \infty)$ satisfaisant les propriétés suivantes :

— leurs classes de monodromie (Définition 2.3.25), vues comme classes de conjugaison de G, appartiennent toutes à l'ensemble D.

— une classe de conjugaison $\gamma \in D$ est la classe de monodromie en exactement $n\xi(\gamma)$ points de branchement.

L'opération de recollement (Définition 2.4.18) induit une structure de monoïde gradué (Définition 3.4.10) commutatif (Proposition 3.4.6) de type fini (Corollaire 3.4.18) sur l'ensemble :

$$\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi) = \bigsqcup_{n \geq 0} \pi_0\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi).$$

Soit k un corps algébriquement clos et de caractéristique première à l'ordre du groupe G. L'*anneau des composantes* R (Définition 3.4.12) est l'algèbre du monoïde $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ sur le corps k :

$$R = k[\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)].$$

C'est une k-algèbre commutative de type fini. On considère l'ensemble $\mathrm{Spec}(R)(k)$ des k-points de son spectre, qu'on munit de la topologie de Zariski. L'objectif du chapitre 5 est de décrire cet ensemble, vu comme plongé dans un espace affine $\mathbb{A}^N(k)$.

Un premier résultat, la proposition 5.1.3, montre que $\mathrm{Spec}(R)(k)$ se décompose en une union disjointe de sous-ensembles $\gamma_\xi(H)$ (Définition 5.1.2), où H parcourt les sous-groupes de G :

$$\mathrm{Spec}(R)(k) = \bigsqcup_{H \in \mathrm{Sub}_{G,D}} \gamma_\xi(H).$$

Il suffit donc, pour décrire $\mathrm{Spec}(R)(k)$, de décrire chacun des ensembles $\gamma_\xi(H)$. C'est ce qu'accomplit partiellement le théorème 5.1.4.

Description du théorème 5.1.4. Le théorème 5.1.4 donne la dimension de Krull de l'ensemble $\gamma_\xi(H)$:

Théorème 5.1.4

La dimension de Krull de $\gamma_\xi(H)$ est égale à $\Omega(D_H) + 1$, où $\Omega(D_H)$ est le nombre de délitement (Définition 4.2.3).

Ce résultat repose sur les estimations obtenues dans le chapitre 4.

Dans la sous-section 5.4.5, on approfondit cette description géométrique. On suppose que R est engendré par ses éléments homogènes non triviaux de degré minimal et qu'on est dans une des deux situations couvertes par les théorèmes 4.3.1 (ii) et 4.3.1 (iii). On détermine alors le degré (comme sous-variété d'un espace projectif) de $\gamma_\xi(H)$. Par exemple, lorsque $\Omega(D_H) = 0$, l'ensemble $\gamma_\xi(H)$ est une union de droites se croisant à l'origine, privées de l'origine. On relie le nombre de ces droites au second groupe d'homologie de H.

Description du théorème 5.5.13. Le théorème 5.5.13 décrit l'ensemble $\mathrm{Spec}(R)(k)$ complètement dans des situations particulières. Plutôt que d'introduire de nombreuses notations, on fait ici des hypothèses plus restrictives. Le fait que les hypothèses faites ci-dessous entraînent celles du théorème 5.5.13 découle de la proposition 5.5.9

On se place dans la situation où l'ensemble D ne contient qu'une seule classe de conjugaison c et que $\xi(c) = 1$. On fait l'hypothèse que l'anneau des composantes R est engendré par ses éléments homogènes non triviaux de degré minimal, dont on désigne le nombre par N. On suppose de plus que, pour tout sous-groupe H de G tel que $H = \langle c \cap H \rangle$, il existe des sous-groupes $H_1, \ldots, H_k$ satisfaisant les propriétés suivantes :

— les sous-groupes $H_1, \ldots, H_k$ engendrent H:

$$H = \langle H_1, \ldots, H_k \rangle \ ;$$

— pour tous $i \neq j$, les éléments du sous-groupe H_i commutent avec les éléments du sous-groupe H_j ;

— si A et B sont deux parties disjointes de $\{1,\dots,k\}$, alors les sous-groupes $\langle (H_a)_{a\in A}\rangle$ et $\langle (H_b)_{b\in B}\rangle$ ont une intersection triviale ;

— on a :
$$c \cap H = \bigsqcup_{i=1}^{k} (c \cap H_i) \ ;$$

— pour tout $i \in \{1,\dots,k\}$, l'ensemble $c \cap H_i$ est une classe de conjugaison de H_i, c'est-à-dire que $\Omega(D_{H_i}) = 0$;

— l'ensemble $\pi_0 \mathrm{CHur}^{*}_{\mathbb{P}^1(\mathbb{C})}(H, D_H, n\xi_H)$ (voir ci-dessus dans la description du théorème 4.3.1) contient au plus une composante, pour tout n.

Pour chaque sous-groupe H de G tel que $c \cap H$ soit une classe de conjugaison de H, on définit un point particulier e_H de l'espace affine $\mathbb{A}^N(k)$, c'est-à-dire un vecteur $e_H \in k^N$ (voir la définition 5.5.11 pour la définition du point e_H). On décrit finalement $\mathrm{Spec}(R)(k)$ comme sous-ensemble de k^N :

Un cas particulier du théorème 5.5.13

Soit H un sous-groupe de G tel que $H = \langle c \cap H\rangle$ et des sous-groupes $H_1,\dots,H_k$ comme ci-dessus. On a :
$$\gamma_\xi(H) = \left\{ \sum_{i=1}^{k} \lambda_i e_{H_i} \;\middle|\; \lambda_1,\dots,\lambda_k \in k^\times \right\},$$
c'est-à-dire que $\gamma_\xi(H)$ est le sous-espace vectoriel de k^N engendré par $e_{H_1},\dots,e_{H_k}$, privé des sous-espaces vectoriels engendrés par $k-1$ quelconques de ces points.

En appliquant la proposition 5.1.3, on déduit de ce résultat une description complète de $\mathrm{Spec}(R)(k) = \bigsqcup_H \gamma_\xi(H)$.

Chapitre 6 A New Look at the Case of Symmetric Groups

Issu de [Seg22]

Résultats principaux : Théorèmes 6.1.1 à 6.1.3

Soit un entier $d \geq 3$, et soit c la classe de conjugaison des transpositions dans le groupe symétrique $\mathfrak{S}_d$. On s'intéresse aux mêmes objets que dans les chapitres 4 et 5, à savoir les anneaux des composantes des espaces de Hurwitz, leurs fonctions de Hilbert (c'est-à-dire la croissance du nombre de composantes), et leurs spectres. L'objectif est de décrire ces objets dans le cas spécifique où $X = \mathbb{P}^1(\mathbb{C})$, $G = \mathfrak{S}_d$, $D = \{c\}$ et $\xi(c) = 1$. Il s'agit d'une situation classique, considérée par Hurwitz lui-même – c'est d'ailleurs dans ce cadre que les espaces de Hurwitz ont d'abord été définis, voir [Hur91].

Pour énoncer les résultats de ce chapitre, on fixe un corps k, de caractéristique nulle ou strictement supérieure à d.

Description du théorème 6.1.1. On donne d'abord une présentation explicite du monoïde et de l'anneau des composantes, par générateurs et relations :

Théorème 6.1.1

Le monoïde gradué des composantes $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ est engendré par des éléments X_{ij} pour tous $1 \leq i < j \leq d$, de degré 2 et sujets aux relations suivantes – qui engendrent toutes les relations entre éléments de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$:

— Les relations de commutation :

$$X_{ij}X_{kl} = X_{kl}X_{ij} \quad \text{pour tous } \begin{cases} 1 \leq i < j \leq d \\ 1 \leq k < l \leq d \end{cases}.$$

— Les relations de tresses :

$$X_{ij}X_{jk} = X_{ik}X_{jk} = X_{ij}X_{ik} \quad \text{lorsque } 1 \leq i < j < k \leq d.$$

Cela constitue une présentation par générateurs et relations de ce monoïde. L'anneau des composantes :

$$R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) = k[\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)]$$

admet la présentation suivante, comme k-algèbre commutative graduée :

$$R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) \simeq \frac{k[(X_{ij})_{1\leq i<j\leq d}]}{(X_{ij}X_{jk} - X_{ik}X_{jk},\ X_{ij}X_{jk} - X_{ij}X_{ik})_{1\leq i<j<k\leq d}},$$

où les générateurs X_{ij} sont de degré 2.

Ce résultat est obtenu en caractérisant exactement les orbites, sous l'action du groupe des tresses, des uplets de transpositions dont le produit vaut 1 (Théorème 6.2.6).

Description du théorème 6.1.2. On détermine la fonction de Hilbert $\mathrm{HF}(n)$ de l'anneau des composantes. Cette fonction compte les composantes connexes de l'espace de Hurwitz des $\mathfrak{S}_d$-revêtements marqués de $\mathbb{P}^1(\mathbb{C})$, non nécessairement connexes, ayant n points de branchement en lesquels les éléments locaux de monodromie sont des transpositions.

Si n est impair, $\mathrm{HF}(n)$ est nul. On s'intéresse aux valeurs que prend HF en les entiers pairs, qui sont décrites par le théorème suivant :

Théorème 6.1.2

On pose $d' = \lfloor d/2 \rfloor$. Il existe un polynôme dont le coefficient dominant est :

$$\frac{d!}{2^{d'}(d')!(d'-1)!} n^{d'-1} \text{ si } d \text{ est pair,}$$
$$\left(1+\frac{d'}{3}\right) \frac{d!}{2^{d'}(d')!(d'-1)!} n^{d'-1} \text{ si } d \text{ est impair,}$$

tel que $\mathrm{HF}(2n)$ coïncide avec ce polynôme lorsque $n \geq d-1$.
On a une formule exacte pour $\mathrm{HF}(2n)$:

$$\sum_{s=1}^{d-1} \sum_{w=1}^{d-s} \sum_{j=0}^{w} (-1)^{w-j} \binom{n-s+w-1}{w-1} \binom{d}{d-s-w,\, w-j,\, s+j} S(s+j,\, j)$$

où $S(n, k)$ désigne les nombres de Stirling de seconde espèce.

Description du théorème 6.1.3. Dans l'esprit du chapitre 5, on décrit l'ensemble des k-points du spectre de l'anneau des composantes $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$, vu comme partie de $\mathbb{A}^{\frac{d(d-1)}{2}}(k) = k^{\frac{d(d-1)}{2}}$. On est dans le cas d'application du théorème 5.5.13, et on obtient une description similaire. On utilise pour indicer les coordonnées dans l'espace vectoriel $k^{\frac{d(d-1)}{2}}$ les couples (i, j) avec $1 \leq i < j \leq d$. On note $e_{i,j}$ le vecteur de base associé à la coordonnée (i, j), et on définit pour chaque partie A de $\{1, \ldots, d\}$ le vecteur e_A, somme des vecteurs de base $e_{i,j}$ sur les couples (i, j) où $i < j$ et $i, j \in A$.

On décrit alors l'ensemble des k-points du spectre de l'anneau des composantes :

Théorème 6.1.3

L'ensemble $\mathrm{Spec}\left(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)\right)(k)$ est l'union, prise sur toutes les familles maximales $\{A_1, \ldots, A_l\}$ de parties disjointes de $\{1, \ldots, d\}$, des sous-espaces vectoriels de $k^{\frac{d(d-1)}{2}}$ engendrés par les vecteurs $e_{A_1}, \ldots, e_{A_l}$.

Chapitre 8 Fields of Definition of Components of Hurwitz Spaces

Issu de [Seg23]

Résultat principal : Théorème 8.1.2

Dans ce chapitre, on étudie les corps de définition des composantes géométriquement connexes des espaces de Hurwitz. Plus précisément, on décrit des situations où le recollement de deux composantes, toutes deux définies sur un même corps de nombres K, est lui aussi défini sur K. Ce travail est un approfondissement des liens élucidés dans [Cau12], qui généralisent eux-mêmes des résultats de [DE06].

La recherche de composantes ayant un petit corps de définition est liée au versant régulier du problème de Galois inverse. En effet, toute extension galoisienne régulière de $\mathbb{Q}(t)$ ayant G pour groupe de Galois définit un point

rationnel de l'espace de Hurwitz correspondant ; la composante connexe de ce point est alors définie sur $\mathbb{Q}$. Ainsi, la recherche de composantes définies sur $\mathbb{Q}$ est une étape essentielle, qui nous aide à savoir où il est raisonnable de chercher des points rationnels.

Description du théorème 8.1.2. Soit K un corps de nombres. On considère deux composantes connexes x et y de l'espace de Hurwitz des G-revêtements marqués de la droite projective. On désigne par H_1 et H_2 les groupes de monodromie respectifs des G-revêtements marqués appartenant aux composantes x et y, et on note H le sous-groupe de G engendré par H_1 et H_2.

On suppose que les composantes x et y sont définies sur K. On pose alors la question 8.1.1 : la composante xy, obtenue par recollement des composantes x et y, est-elle définie sur K ?

Le théorème 8.1.2 donne une réponse partielle à cette question :

Théorème 8.1.2

(i) Si tout élément de H est produit d'un élément de H_1 et d'un élément de H_2, alors la composante xy est définie sur K.

(ii) Il existe un entier M ne dépendant que du groupe G tel que si toute classe de conjugaison de H qui est classe de monodromie des G-revêtements dans la composante xy est classe de monodromie en au moins M points de branchement, alors la composante xy est définie sur K. En particulier, $(xy)^M$ est définie sur K.

(iii) Il existe des éléments $\gamma, \gamma' \in H$ tels que $\left\langle H_1^{\gamma}, H_2^{\gamma'} \right\rangle = H$ et tels que la composante $x^{\gamma} y^{\gamma'}$, obtenue en faisant agir γ et γ' sur les composantes x et y puis en les recollant, soit définie sur K.

Chacun des trois énoncés qui constituent le théorème 8.1.2 est démontré avec des méthodes propres. Le théorème 8.1.2 entraîne l'existence, sur les corps de nombres, d'une variante affaiblie de l'opération de recollement : on ne recolle pas les G-revêtements eux-mêmes, mais leurs composantes.

Une application du théorème 8.1.2 (iii) est donnée dans l'exemple 8.4.6. L'unique groupe simple sporadique dont on ne sache pas encore s'il est groupe de Galois sur $\mathbb{Q}$ est le groupe de Mathieu M_{23} : la question de sa réalisation a été largement étudiée [Hä22]. Nous construisons des composantes définies sur $\mathbb{Q}$ de M_{23}-revêtements connexes n'ayant que quatre points de branchement (à comparer avec les quinze points de branchement utilisés par [Cau16]).

On montre aussi, dans la proposition 8.2.8, que si l'on connaît l'action du groupe de Galois absolu de K sur les composantes des espaces de Hurwitz jusqu'à un certain nombre de points de branchement (le majorant $|G|\exp(G)$ convient), alors on peut déterminer l'action de Galois sur une composante arbitraire.

1.3. Organisation du texte

On détaille à présent l'organisation du texte, chapitre par chapitre.

Les chapitres 2 et 3 sont des chapitres d'exposition en français.

Dans le chapitre 2, on présente des faits classiques sur les (G-)revêtements topologiques ramifiés (Sections 2.2 et 2.3) et leur description combinatoire (Section 2.4) Les énoncés de ce chapitre sont classiques : beaucoup pourront se contenter de la lecture de l'introduction (Section 2.1) ou du résumé en anglais (Section 2.5).

Dans le chapitre 3, on donne une définition des espaces de Hurwitz (Sections 3.2 et 3.3), puis des monoïdes et anneaux des composantes (Section 3.4) dont on mentionne diverses propriétés. Ce chapitre se conclut par un résumé en anglais (Section 3.5).

Les chapitres 4 à 6 sont issus de la prépublication [Seg22]. Ce découpage est motivé par la volonté de donner une plus grande autonomie aux thèmes abordés dans ces chapitres.

Dans le chapitre 4, on démontre le théorème 4.3.1, qui estime le nombre de composantes d'espaces de Hurwitz de G-revêtements dont la monodromie est contrainte et dont le nombre de points de branchement tend vers l'infini.

Dans le chapitre 5, on étudie la géométrie du spectre de l'anneau des composantes, en reliant cet objet aux questions combinatoires du chapitre qui précède. On énonce et démontre les théorèmes 5.1.4 et 5.5.13 présentés ci-dessus.

Le chapitre 6 s'intéresse aux objets des chapitres 4 et 5 dans le cas des $\mathfrak{S}_d$-revêtements de $\mathbb{P}^1(\mathbb{C})$ dont les éléments locaux de monodromie sont des transpositions. On donne une présentation du monoïde et de l'anneau des composantes (Théorème 6.1.1), un critère calculable d'égalité entre éléments du monoïde des composantes (Théorème 6.2.6 (v)), et une description du spectre de l'anneau des composantes (Théorème 6.1.3).

Le chapitre 7 est un troisième chapitre d'exposition, constitué de faits connus. On y présente rapidement la théorie des G-revêtements génériquement étales de la droite projective, l'équivalence entre revêtements de la droite et corps de fonctions (Sous-section 7.1.3), le théorème d'irréductibilité de Hilbert (Sous-section 7.1.3), le théorème d'existence de Riemann (Sous-section 7.1.4), et les espaces de modules de Hurwitz des G-revêtements ramifiés (marqués ou non) de $\mathbb{P}^1$ vus comme schémas (Section 7.2). On détaille les liens qui unissent ces schémas aux espaces de Hurwitz topologiques et le rôle de ces espaces dans l'étude de questions arithmétiques – notamment pour le problème de Galois inverse. Un résumé en anglais conclut le chapitre (Section 7.3).

Le chapitre 8, qui reprend les résultats de la prépublication [Seg23], consiste en la preuve du théorème 8.1.2. Les trois énoncés qui constituent le théorème sont démontrés dans trois sections correspondantes (Sections 8.2 à 8.4). Chacune de ces sections correspond à une approche particulière du problème, avec ses propres outils : l'action des tresses dans la section 8.2, le *lifting invariant* (voir la sous-section 3.4.7) dans la section 8.3, et la théorie du *patching* de Harbater dans la section 8.4.

À la suite du texte, dans l'appendice A, se trouvent un lexique bilingue des termes introduits dans le texte (Appendice A.1) et un index des notations (Appendice A.2).

Le document se conclut par l'appendice B, qui est une tentative de vulgarisation du contenu de cette thèse à l'attention du public non-mathématicien.

On signale par une petite clé 🔑 dans la marge les résultats clés.

1.4. Conventions et notations

Dans cette section, nous introduisons des termes et des notations qui sont utilisées tout au long de la thèse.

1.4.1. Notations générales

— Le cardinal d'un ensemble X est noté $|X|$.

— Si C est un objet dans une catégorie quelconque, son *groupe d'automorphismes* $\mathrm{Aut}(C)$ est l'ensemble des isomorphismes entre C et lui-même. Étant donné un morphisme $C \to D$, le groupe d'automorphismes $\mathrm{Aut}_D(C)$ est le sous-groupe de $\mathrm{Aut}(C)$ formé des automorphismes σ qui font commuter le diagramme :

$$\begin{array}{ccc} C & \xrightarrow{\sigma} & C \\ & \searrow \quad \swarrow & \\ & D & \end{array} .$$

— Le n-ième groupe symétrique $\mathfrak{S}_n$ est vu comme le groupe des permutations de l'ensemble $\{1, \dots, n\}$. Si A est une partie non-vide de $\{1, \dots, n\}$, on désigne par $\mathfrak{S}_A$ le sous-groupe de $\mathfrak{S}_n$ des permutations qui fixent les éléments qui ne sont pas dans A. Si $A_1, \dots, A_r$ sont des parties disjointes de $\{1, \dots, n\}$, alors $\mathfrak{S}_{A_1} \times \cdots \times \mathfrak{S}_{A_r}$ est le sous-groupe de $\mathfrak{S}_n$ engendré par $\mathfrak{S}_{A_1}$, …, $\mathfrak{S}_{A_r}$.

— Si γ_1 et γ_2 sont des chemins (ou des lacets, ou des classes d'homotopie de chemins/lacets) dans un espace topologique X, on note $\gamma_1 * \gamma_2$ leur concaténation dans l'ordre « d'abord γ_1, puis γ_2 » lorsque ces chemins sont concaténables. Nous n'écrivons pas toujours le symbole $*$, notamment pour les classes d'homotopie de lacets.

— Si $\underline{t} = (t_1, \dots, t_n)$ est une liste de n points d'un espace topologique (ou d'une variété algébrique) X, on note $X \setminus \underline{t}$ le sous-espace de X obtenu en le privant des points $t_1, \dots, t_n$. On utilise cette même notation si $\underline{t}$ est une partie finie de X, ou bien s'il s'agit d'une liste non-ordonnée de n points de X (c'est-à-dire une orbite de n-uplets d'éléments de X sous l'action du groupe symétrique $\mathfrak{S}_n$).

— On fixe une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$. Un corps de nombres est muni d'un plongement dans $\overline{\mathbb{Q}}$. Si K est un corps de nombres, on note Γ_K son groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$. Le caractère cyclotomique de K est le morphisme de groupes $\chi : \Gamma_K \to \widehat{\mathbb{Z}}^\times$ déterminé par l'action de Γ_K sur les racines de l'unité : si $\zeta \in \overline{\mathbb{Q}}$ est une racine n-ième de l'unité et $\sigma \in \Gamma_K$, alors $\sigma(\zeta) = \zeta^{\chi(\sigma) \mod n}$.

On utilise, pour certaines estimations asymptotiques, une variante de la notation « grand O » :

Définition 1.4.1. Si f est une fonction $\mathbb{N} \to \mathbb{N}$ et $\zeta \in \{0, 1, \ldots\}$, la notation :

$$f(n) = O^\sharp\left(n^\zeta\right)$$

signifie que $f(n) = O(n^\zeta)$ et $f(n) \neq o(n^\zeta)$. Autrement dit :

$$0 < \limsup_{n\to\infty} \left(n^{-\zeta} f(n)\right) < \infty.$$

L'exposant ζ de la définition 1.4.1, quand il existe, est défini de manière unique :

$$\zeta = \limsup_{n\to\infty} \frac{\log f(n)}{\log n}.$$

1.4.2. Groupes

Dans ce travail, G désigne toujours un groupe fini. On utilise en principe les symboles $H, H', H_1, H_2, \ldots$ pour désigner des sous-groupes de G. Les symboles $D, D_H, \ldots$ sont utilisés pour désigner des ensembles de parties de G ou H disjointes, non vides, et invariantes par conjugaison (possiblement des classes de conjugaison). Les éléments de l'ensemble D, ainsi que les classes de conjugaison de G ou de ses sous-groupes, sont désignées par les lettres grecques $\gamma, \gamma', \ldots$. On réserve l'utilisation des notations $D^*, D_H^*, \ldots$ pour le cas où tous les éléments sont des classes de conjugaison. Le caractère c désigne souvent une partie de G invariante par conjugaison (possiblement, une classe de conjugaison) ; dans la plupart des cas, c est l'union des ensembles $\gamma \in D$ et D^* est l'ensemble des classes de conjugaison de G contenues dans c. La lettre ξ fait référence à une application $D \to \{1, 2, \ldots\}$ fixée, qu'on voit comme une multiplicité.

Soit G un groupe fini.

— Si X est une partie de G, on note $\langle X \rangle$ le plus petit sous-groupe de G contenant X.

— Si X et Y sont des parties (ou des sous-groupes) de G, alors XY est l'ensemble formé des produits xy où $x \in X$ et $y \in Y$.

— Si $g, h \in G$, on utilise la notation suivante pour la conjugaison dans G :

$$g^h = hgh^{-1}.$$

Le groupe des automorphismes intérieurs de G est noté $\mathrm{Inn}(G)$.

— Une partie *invariante par conjugaison* de G est une union de classes de conjugaison de G.

— Si g est un élément de G, son ordre est noté $\mathrm{ord}(g)$. De même, si γ est une classe de conjugaison de G, l'ordre d'un quelconque de ses éléments est noté $\mathrm{ord}(\gamma)$. L'exposant du groupe G est noté $\exp(G)$.

— Si $n \in \widehat{\mathbb{Z}}$ est un entier profini et $g \in G$, alors g^n est l'élément g^k où $k = n \mod |G|$. Si γ est une classe de conjugaison de G et n est un entier profini (ou un entier), alors γ^n est la classe de conjugaison (bien définie) des puissances n-ièmes des éléments de γ.

— Soit K un corps de nombres. On définit la notion de *partie K-rationnelle* de G :

Définition 1.4.2. Une partie c de G est *K-rationnelle* si pour tout $g \in c$ et $\sigma \in \Gamma_K$ on a $g^{\chi(\sigma)} \in c$.

Si $K = \mathbb{Q}$, on a $\mathrm{Im}(\chi) = \widehat{\mathbb{Z}}^\times$. Ainsi, les parties $\mathbb{Q}$-rationnelles sont les parties closes par puissance n-ième pour tous les entiers n premiers avec $|G|$. Si K contient toutes les racines $|G|$-ièmes de l'unité, alors l'image de χ est triviale modulo $|G|$ et toute partie de G est K-rationnelle. Les parties suivantes sont toujours K-rationnelles : G, $G \setminus \{1\}$, et toute partie de G ne contenant que des involutions.

— On désigne par G^{ab} l'abélianisé du groupe G.

1.4.3. **Uplets**

On désigne les uplets (c'est-à-dire les listes ordonnées) par des lettres soulignées.

Si $\underline{g} = (g_1, g_2, \ldots, g_n)$ est un n-uplet d'éléments du groupe G, alors :

Définition: *Taille d'un uplet*

Définition 1.4.3. La *taille* du n-uplet $\underline{g} \in G^n$, notée $\left|\underline{g}\right|$, est l'entier n.

Définition: *Produit d'un uplet*

Définition 1.4.4. Le *produit* du n-uplet $\underline{g}$, noté $\pi\underline{g}$, est l'élément $g_1 g_2 \cdots g_n$ de G.

Définition: *Groupe d'un uplet*

Définition 1.4.5. Le *groupe* du n-uplet $\underline{g}$, noté $\left\langle \underline{g} \right\rangle$, est le sous-groupe de G engendré par $g_1, g_2, \ldots, g_n$.

Suivant [EVW12], on définit le *multidiscriminant*. Pour cela, soit H un sous-groupe de G et c une partie de H invariante par conjugaison telle que tous les éléments g_i appartiennent à c. Nous notons D^* l'ensemble des classes de conjugaison de H contenues dans c. Une classe de conjugaison $\gamma \in D^*$ *apparaît dans* $\underline{g}$ si au moins l'un des éléments $g_1, \ldots, g_n$ appartient à γ.

Définition: (H,c)*-multidiscriminant d'un uplet*

Définition 1.4.6. Le (H,c)*-multidiscriminant* du n-uplet $\underline{g}$ est l'application $\mu_{H,c}(\underline{g}) : D^* \to \{0, 1, \ldots\}$ qui associe à une classe de conjugaison $\gamma \in D^*$ le nombre d'éléments de $\underline{g}$ qui se trouvent dans γ :

$$\mu_{H,c}(\underline{g})(\gamma) = \left|\{i \in \{1, \ldots, n\} \mid g_i \in \gamma\}\right|.$$

Quand (H,c) n'est pas spécifié, le *multidiscriminant* du uplet $\underline{g}$ est son (H,c)-multidiscriminant, où H est le groupe $\left\langle \underline{g} \right\rangle$ et c est la plus petite partie de H invariante par conjugaison qui contienne $g_1, \ldots, g_n$.

Si $\underline{g}_1, \ldots, \underline{g}_s$ sont des uplets d'éléments de G, de tailles respectives $r_i = \left|\underline{g}_i\right|$, alors :

Définition: *Concaténation de uplets*

Définition 1.4.7. La *concaténation* $\underline{g}_1 \underline{g}_2 \cdots \underline{g}_s$ des uplets $\underline{g}_1, \ldots, \underline{g}_s$ est le $(\sum r_i)$-uplet suivant d'éléments de G:

$$\left(g_{1,1}, \ldots, g_{1,r_1}, g_{2,1}, \ldots, g_{2,r_2}, \ldots, g_{s,1}, \ldots, g_{s,r_s}\right).$$

Le *groupe* $\left\langle \underline{g}_1, \ldots, \underline{g}_s \right\rangle$ engendré par les uplets $\underline{g}_1, \ldots, \underline{g}_s$ est le sous-groupe de G engendré par les sous-groupes $\left\langle \underline{g}_1 \right\rangle, \ldots, \left\langle \underline{g}_s \right\rangle$.

1.4.4. **Terminologie pour les schémas**

Nous précisons ici la terminologie et les notations que nous utilisons pour désigner certaines propriétés des schémas, de leurs sous-schémas ou de leurs points. Ces termes sont utilisés tout au long des chapitres 7 et 8, mais peuvent être ignorés pour la lecture des autres chapitres.

Soit L un corps. Notre définition des L-schémas requiert la séparation :

Définition: *L-schéma*

Définition 1.4.8. Un *L-schéma* est un schéma muni d'un morphisme séparé dans $\mathrm{Spec}(L)$. Un *morphisme* entre deux L-schémas X et Y est un morphisme de schémas $X \to Y$ qui fait commuter le diagramme suivant :

$$\begin{array}{ccc} X & \longrightarrow & Y \\ & \searrow \quad \swarrow & \\ & \mathrm{Spec}(L) & \end{array} .$$

Soit $L' \mid L$ une extension de corps et X un L-schéma de type fini. On note l'extension des scalaires par un indice :

Définition: *Extension des scalaires*

Définition 1.4.9. L'*extension des scalaires de X à L'* est le L'-schéma suivant :

$$X_{L'} \overset{\text{def}}{=} X \underset{\mathrm{Spec}(L)}{\times} \mathrm{Spec}(L').$$

C'est-à-dire qu'on a le carré cartésien suivant :

$$\begin{array}{ccc} X_{L'} & \longrightarrow & \mathrm{Spec}(L') \\ \downarrow & \lrcorner & \downarrow \\ X & \longrightarrow & \mathrm{Spec}(L) \end{array}$$

Nos définitions et notations pour les points sont les suivantes :

Définition: *L'-point* *Point géométrique*

Définition 1.4.10. Un *L'-point de X* est un morphisme de L-schémas de $\mathrm{Spec}(L')$ dans X, ou de manière équivalente un morphisme de L'-schémas de $\mathrm{Spec}(L')$ dans $X_{L'}$. L'ensemble des L'-points de X est noté $X(L')$. Les $\overline{L}$-points de X sont aussi appelés *points géométriques*.

Définition: *Point L-rationnel* *L-modèle*

Définition 1.4.11. Un L'-point $x \in X(L')$ est *L-rationnel* s'il existe un L-point $x' \in X(L)$ tel que le diagramme de L-schémas suivant commute :

$$\begin{array}{ccccc} \mathrm{Spec}(L') & \longrightarrow & \mathrm{Spec}(L) & \xrightarrow{x'} & X \\ & \searrow & & \nearrow_{x} & \end{array}$$

Le point x' est alors appelé un *L-modèle* du point x.

On introduit les notions analogues pour les sous-schémas de $X_{L'}$:

Définition: *Sous-schéma défini sur L* *Corps de définition*

Définition 1.4.12. Un L'-sous-schéma Y de $X_{L'}$ est *défini sur L* s'il existe un L-sous-schéma Y' de X tel que $Y = (Y')_{L'}$ (en tant que sous-schémas de $X_{L'}$). Dans ce cas, le corps L est un *corps de définition* de Y, et le L-sous-schéma Y' est un *L-modèle* de Y.

On suppose à présent l'extension $L' \mid L$ galoisienne. Un automorphisme $\sigma \in \mathrm{Gal}(L' \mid L)$ induit un automorphisme du L-schéma $\mathrm{Spec}(L')$, qu'on note $\mathrm{Spec}(\sigma)$. Le groupe $\mathrm{Gal}(L' \mid L)$ agit sur un L'-point $x \in X(L')$ par la formule $\sigma.x = x \circ \mathrm{Spec}(\sigma)$, et sur un L'-sous-schéma $Y \subseteq X_{L'}$ comme produit fibré le long du morphisme $\mathrm{id}_X \underset{\mathrm{Spec}(L)}{\times} \mathrm{Spec}(\sigma)$:

$$\begin{array}{ccc} \mathrm{Spec}(L') & & \\ {\scriptstyle \mathrm{Spec}(\sigma)}\downarrow & \searrow^{\sigma.x} & \\ \mathrm{Spec}(L') & \xrightarrow[x]{} & X \end{array} \qquad \begin{array}{ccc} \sigma.Y & \longrightarrow & X_{L'} \\ \downarrow & \lrcorner & \downarrow{\scriptstyle \mathrm{id}_X \underset{\mathrm{Spec}(L)}{\times} \mathrm{Spec}(\sigma)} \\ Y & \longrightarrow & X_{L'} \end{array}.$$

Proposition 1.4.13. *On a les équivalences suivantes :*

Proposition: *Un énoncé de descente galoisienne*

— *Un L'-point de X est L-rationnel si et seulement s'il est invariant sous l'action de* $\mathrm{Gal}(L' \mid L)$.

— *Un L'-sous-schéma Y de $X_{L'}$ est défini sur L si et seulement s'il est globalement préservé par l'action de* $\mathrm{Gal}(L' \mid L)$*, c'est-à-dire que pour tout $\sigma \in \mathrm{Gal}(L' \mid L)$ il existe un L'-automorphisme σ' de Y qui fasse commuter le diagramme suivant :*

$$\begin{array}{ccc} Y & \xhookrightarrow{\subseteq} & X_{L'} \\ {\scriptstyle \sigma'}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_X \underset{\mathrm{Spec}(L)}{\times} \mathrm{Spec}(\sigma)} \\ Y & \xhookrightarrow{\subseteq} & X_{L'} \end{array}.$$

— *Si L' est algébriquement clos et que Y est un L'-sous-schéma réduit de $X_{L'}$, alors Y est défini sur L si et seulement si le sous-ensemble $Y(L')$ de $X(L')$ est globalement préservé par l'action de* $\mathrm{Gal}(L' \mid L)$ *sur les L'-points de X.*

Chapitre 1

Introduction (English)

(Une version en français de cette introduction se trouve page 9.)

Outline of the chapter

This thesis is devoted to the study of the connected components of *Hurwitz spaces*, moduli spaces of covers which are related to number-theoretical questions – notably the inverse Galois problem. We study the connected components of these spaces from two distinct perspectives:

— First, we investigate the *combinatorial* behavior of the connected components of Hurwitz spaces: what can be said about the asymptotical count of these components as the number of branch points of the covers increases?

  This question lies at the heart of Chapters 5 to 7. It revisits issues raised by the works of Ellenberg, Tran, Venkatesh, and Westerland, who highlighted connections between the homology of Hurwitz spaces and the statistical distribution of function fields over finite fields [EVW16; EVW12; ETW17].

— Secondly, we consider the *arithmetic* properties of the components of Hurwitz spaces, in particular their fields of definition.

  Constructing components with small fields of definition is a necessary step towards solving the regular inverse Galois problem – it is a weak form of this problem. We address this question in Chapter 8.

In both situations, for counting components as well as for studying their fields of definition, a single geometric operation plays a central role in our work: the *gluing* of components. The combinatorial importance of this operation is already apparent in [EVW16], and [Cau12] emphasizes its arithmetical relevance, but we make efforts to unify the paradigms of these authors in order to exploit the full potential of their methods.

Our introduction is organized as follows: in Section 1.1, we present in greater detail the objects and questions that we investigate, emphasizing the motivations behind their study. We detail our main results in Section 1.2. In Section 1.3, we specify the content of each chapter. Finally, we introduce some notation common to the whole text in Section 1.4.

1.1. Topics covered

The main objects of this thesis are **Hurwitz spaces**. Given a finite group G and an integer n, Hurwitz spaces are moduli spaces which classify G-covers branched at n points – we mostly consider covers of the projective line $\mathbb{P}^1$. There are various types of Hurwitz spaces, depending on whether the branch points are ordered or not, whether the covers are marked or not, whether the covers are required to be connected or not, etc.

The geometry of these moduli spaces reflects the fact that a cover can be continuously deformed as its n branch points move while remaining distinct. Hurwitz spaces are themselves covers, finite and unramified but not necessarily connected, of configuration spaces of n points on the projective line. For this reason, the geometric properties of these spaces largely come from combinatorial facts about braid groups and their action on lists of elements of G.

One can approach Hurwitz spaces from a purely geometric perspective – as topological or analytic spaces –, or from an algebraic perspective – as schemes or stacks.

1.1.1. Motivations for the geometric and arithmetic study of Hurwitz spaces

The algebraic aspect of Hurwitz spaces provides a framework for the study of **rational points**, particularly of K-points when K is a number field.

Up to some complications (these moduli spaces are generally not fine), K-points of Hurwitz spaces correspond to branched G-covers of $\mathbb{P}^1_K$, i.e. (assuming moreover that these covers are irreducible) to Galois extensions of $K(t)$ whose Galois groups are isomorphic to G.

Hilbert's irreducibility theorem establishes that such an extension can be specialized into an extension of K whose Galois group is G. Thus, Hurwitz spaces are a tool of choice for **inverse Galois theory**, whose main question is whether every finite group can be realized as the Galois group of an extension of the field of rational numbers. For example, if G is a finite centerless group, one can realize it as a Galois group over $\mathbb{Q}$ by finding a $\mathbb{Q}$-point of a Hurwitz space of connected branched G-covers of the projective line.

In a different direction, the count of $\mathbb{F}_q$-points of Hurwitz spaces, where q is coprime to $|G|$, is related to the distribution of extensions of $\mathbb{F}_q(T)$ with a given Galois group, and thus to the **Malle conjecture** on function fields over finite fields.

This approach has been explored in the articles [EVW16; EVW12; ETW17], which highlight a strategy for this counting problem which is based on the same principles as the proof of the Weil conjectures: the geometric study of Hurwitz spaces, and in particular of their **homology**, is at the heart of this idea.

1.1.2. The gluing operation and components of Hurwitz spaces

Consider two marked G-covers of the complex line (projective or affine) whose respective monodromy groups are subgroups H and H' of G. We assume that the branch locus of these two covers are disjoint, and consist of n and n' points respectively. It is then possible to **glue** these covers into a single marked G-cover, branched at $n + n'$ points, whose monodromy group is the subgroup of G generated by H and H'.

This operation can be described in combinatorial terms: a bijection relates marked G-covers, branched at n specified points and n-tuples $(g_1, \dots, g_n)$ of elements of G (with the additional condition that the product $g_1 g_2 \cdots g_n$ is equal to 1 in the case of the projective line). To glue two marked G-covers together, one concatenates the corresponding lists of elements of G.

Hurwitz spaces are generally not connected, and their non-connectedness is a major geometric difficulty. Studying the geometry of a component taken independently essentially amounts to understanding the homology of braid groups. The problem then remains of combining this information. For this, it is necessary to have a good understanding of the connected components.

The gluing operation, defined above in terms of marked G-covers, induces an operation at the level of connected components of Hurwitz spaces. This tool sheds light on the structure of the set of components by providing it with an algebraic structure. More precisely, we define a *monoid* and a *ring* of components. These objects were introduced in [EVW16], and they are central to our work.

1.1.3. Counting components

We explore the question of the **number of components** of Hurwitz spaces, and more specifically how this number behaves asymptotically as the number of branch points grows. An important tool is the combinatorial description of covers: we are counting the orbits, under the braid group action, of n-tuples of elements of G. We use invariants to determine whether two n-tuples of elements of G (that is, two marked G-covers branched at n points) are in the same orbit for the braid group action (that is, the covers are in the same connected component).

The growth of the number of connected components is related to arithmetic questions: the number of components is the 0-th Betti number of the Hurwitz spaces, and a key point of [EVW16; Tie16] is that the dimension of higher homology is controlled by this number. Using the Grothendieck-Lefschetz trace formula and Deligne's bounds on Frobenius eigenvalues, one can estimate the number of $\mathbb{F}_q$-points of Hurwitz spaces using the Betti numbers. This leads to an estimate of the **count of extensions** of $\mathbb{F}_q(T)$ with Galois group G. This strategy allows Ellenberg, Tran, and Westerland to prove the upper bound of Malle's conjecture over $\mathbb{F}_q(T)$.

Generalizing the ring of components from [EVW16] to G-covers of the projective line, we define a commutative graded ring of finite type, whose Hilbert function counts components of Hurwitz spaces as a function of the number of branch points.

The growth of the Hilbert function of a graded ring is related to **geometric properties** of its spectrum, such as dimensions and degrees. This motivates our further study of the geometry of spectrums of rings of components of the Hurwitz spaces (Chapter 5).

In the classical situation of $\mathfrak{S}_d$-covers of the projective line whose local monodromy elements are transpositions, we give an exact formula for the count of components of Hurwitz spaces (Theorem 6.1.2), and we describe the spectrum of the ring of components (Theorem 6.1.3).

1.1.4. Fields of definition of components of Hurwitz spaces

The question of determining which connected components of the Hurwitz spaces are defined over $\mathbb{Q}$ – and in particular, isolating those that are likely to contain rational points– is studied in [FV91; DE06; Cau12; EVW12]. We focus on the problem of **stability of fields of definition of components for the gluing operation** (Question 8.1.1). This question has already been addressed in [DE06; Cau12], but we give it a central place.

Our approach is related to the search for gluing operations on non-algebraically closed fields. For example, in the case of complete valued fields, a *patching* operation defined by Harbater [Har03] implies a positive answer to the regular inverse Galois problem: one can glue covers whose group is cyclic. In our case, we work over number fields, but we weaken the problem by replacing covers with components of Hurwitz spaces – i.e. geometrically irreducible families of covers. The gluing operation, which has a geometric origin, is very "transcendental": we do not expect it to have good arithmetic properties. We prove Theorem 8.1.2, which provides a positive answer to the question in various situations. The proof of this result uses diverse tools: a theorem from [Cau12] and braid calculations; the lifting invariant introduced in [EVW12]; and Harbater's patching theory [Har03].

1.2. Contributions

The contributions of this thesis are concentrated in Chapters 4 to 6 (for combinatorial/geometric results) and in Chapter 8 (for arithmetic results). Chapters 2, 3 and 7 serve as expository chapters.

In what follows, we summarize the main results of each chapter. Some statements are given in a concise form, which may be weaker than those in the manuscript.

Chapter 4 Counting Components of Hurwitz Spaces

Taken from [Seg22]

Main result: Theorem 4.3.1

Let G be a fixed group and let D be a set of conjugacy classes of G. We fix a function $\xi : D \to \mathbb{Z}$ that assigns to each class $\gamma \in D$ a "multiplicity". In what follows, the topological space X is either the complex affine line $\mathbb{A}^1(\mathbb{C})$ or the complex projective line $\mathbb{P}^1(\mathbb{C})$. In either case, a basepoint t_0 is fixed.

We consider a subgroup H of G that has a non-empty intersection with each conjugacy class $\gamma \in D$, and that is generated by the intersections $\gamma \cap H$ for $\gamma \in D$ (see Definition 3.2.20).

We denote by $\pi_0\mathrm{CHur}^*(H, D_H, n\xi_H)$ the set of connected components of the Hurwitz space (Definition 3.2.15) of marked branched G-covers of (X, t_0) (Definitions 2.2.13 and 2.3.15) which satisfy the following properties:

— their monodromy group (Definition 2.2.18) is the group H;
— their monodromy classes (Definition 2.3.25), seen as conjugacy classes of G, all belong to the set D;
— a class $\gamma \in D$ is the monodromy class at exactly $n\xi(\gamma)$ branch points.

Description of Theorem 4.3.1. We estimate the following number of components as the integer n tends to infinity:

$$\mathrm{HF}_H(n) = |\pi_0 \mathrm{CHur}^*(H, D_H, n\xi_H)|\,.$$

In all cases, the main measure of the growth of this number components is the *splitting number* $\Omega(D_H)$ (Definition 4.2.3): it is the difference between the number of conjugacy classes of H that are contained in a conjugacy class of G belonging to the set D, and the cardinality of the set D. This integer measures how much the conjugacy classes of G belonging to D tend to split into multiple conjugacy classes when intersected with the subgroup H.

We obtain the following estimates:

— When X is the affine complex line $\mathbb{A}^1(\mathbb{C})$, an explicit equivalent is obtained in all cases:

Concise statement of Theorem 4.3.1 (i)

The function HF_H is asymptotically equivalent to a monomial of degree $\Omega(D_H)$:

$$\mathrm{HF}_H(n) \underset{n\to\infty}{\sim} \alpha n^{\Omega(D_H)}.$$

We compute the leading coefficient α, which involves the second homology group of H.

— When X is the complex projective line $\mathbb{P}^1(\mathbb{C})$, the most general statement is less constraining:

Theorem 4.3.1 (iv)

The function HF_H is $O\left(n^{\Omega(D_H)}\right)$, but not $o\left(n^{\Omega(D_H)}\right)$.

However, in particular situations, better results are obtained:

Concise statement of Theorems 4.3.1 (ii) and 4.3.1 (iii)

An "average dominant coefficient" of HF_H is computed, assuming we are in one of the two following situations:

- the splitting number $\Omega(D_H)$ is zero, i.e. the intersection of the conjugacy classes considered (the elements of D) with the subgroup H are conjugacy classes of H (cf. Definition 4.2.2);
- the set D consists of a single conjugacy class c of G, and $\xi(c) = 1$.

The homology of the group H is involved in the expression of the leading coefficient.

These estimates generalize results from [EVW16]: the authors prove that there is a form of *homological stability* when $X = \mathbb{A}^1(\mathbb{C})$, $\Omega(D_H) = 0$, $D = \{c\}$ and $\xi(c) = 1$. An instance of this stability phenomenon is the fact that the function HF_H is bounded in this case.

Chapter 5 The Geometry of Rings of Components of Hurwitz Spaces

Taken from [Seg22]

Main results: Theorems 5.1.4 and 5.5.13

Let G be a finite group, D be a set of conjugacy classes of G, and $\xi : D \to \{1, 2, \ldots\}$ be a map.

Let $\pi_0\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi)$ be the set of connected components of the Hurwitz space of marked G-covers of $(\mathbb{P}^1(\mathbb{C}), \infty)$ that satisfy the following properties:

— their monodromy classes (Definition 2.3.25), seen as conjugacy classes of G, belong to the set D;

— a class $\gamma \in D$ is the monodromy class at exactly $n\xi(\gamma)$ branch points.

The gluing operation (Definition 2.4.18) induces a structure of commutative graded monoid of finite type (Definition 3.4.10, Proposition 3.4.6, et Corollary 3.4.18) on the following set:

$$\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi) = \bigsqcup_{n \geq 0} \pi_0\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi).$$

Let k be an algebraically closed field of characteristic coprime to the order of G. The *ring of components* R (Definition 3.4.12) is the algebra of the monoid $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ over the field k:

$$R = k[\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)].$$

It is a commutative k-algebra of finite type. We consider the set $\mathrm{Spec}(R)(k)$ of k-points of its spectrum, equipped with the Zariski topology. The goal of Chapter 5 is to describe this set, seen as embedded in a certain affine space $\mathbb{A}^N(k)$.

A first result, Proposition 5.1.3, states that $\mathrm{Spec}(R)(k)$ decomposes as a union of disjoint subsets $\gamma_\xi(H)$ (Definition 5.1.2) where H ranges over subgroups of G:

$$\mathrm{Spec}(R)(k) = \bigsqcup_{H \in \mathrm{Sub}_{G,D}} \gamma_\xi(H).$$

Thus, to describe $\mathrm{Spec}(R)(k)$, it suffices to describe each of the subsets $\gamma_\xi(H)$. Such a description is partially achieved by Theorem 5.1.4.

Description of Theorem 5.1.4. Theorem 5.1.4 computes the Krull dimension of the set $\gamma_\xi(H)$:

> **Theorem 5.1.4**
>
> The Krull dimension of $\gamma_\xi(H)$ is equal to $\Omega(D_H) + 1$, where $\Omega(D_H)$ is the splitting number (cf. Definition 4.2.3).

The proof of this result relies on the estimates from Chapter 4.

In Subsection 5.4.5, we go a little further. We assume that R is generated by its non-trivial homogeneous elements of minimal degree, and that we are in one of the two situations covered by Theorems 4.3.1 (ii) and 4.3.1 (iii). We determine the degree of $\gamma_\xi(H)$ as a subvariety of projective space. For instance, if $\Omega(D_H) = 0$, then $\gamma_\xi(H)$ is a union of lines intersecting at the origin, with the origin removed. We relate the number of these lines to the second homology group of H.

Description of Theorem 5.5.13. Theorem 5.5.13 describes the set $\mathrm{Spec}(R)(k)$ completely in specific situations. Rather than introducing numerous notations, we make stronger assumptions here. The fact that the hypotheses below imply those of Theorem 5.5.13 is a consequence of Proposition 5.5.9.

We consider the situation where D contains a single conjugacy class c and $\xi(c) = 1$. Furthermore, we assume that the ring of components R is generated by its nontrivial homogeneous elements of minimal degree, and we denote the number of these elements by N. We also assume that for any subgroup H of G such that $H = \langle c \cap H \rangle$, there exist subgroups $H_1, \dots, H_k$ satisfying the following properties:

— the subgroups $H_1, \dots, H_k$ generate H:

$$H = \langle H_1, \dots, H_k \rangle ;$$

— for all $i \neq j$, elements of H_i commute with elements of H_j;

— for any two disjoint subsets A and B of $1, \dots, k$, the subgroups $\langle (H_a)_{a \in A} \rangle$ and $\langle (H_b)_{b \in B} \rangle$ have trivial intersection;

— we have:

$$c \cap H = \bigsqcup_{i=1}^{k} (c \cap H_i);$$

— for all $i \in 1, \dots, k$, the set $c \cap H_i$ is a conjugacy class of H_i, i.e. $\Omega(D_{H_i}) = 0$;

— the set $\pi_0 \mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(H, D_H, n\xi_H)$ (cf. above in the description of Theorem 4.3.1) contains at most one component, for each n.

For each subgroup H of G such that $c \cap H$ is a conjugacy class of H, we define a specific point e_H in the affine space $\mathbb{A}^N(k)$, that is, a vector $e_H \in k^N$ (cf. Definition 5.5.11 for the definition of e_H). We finally describe $\mathrm{Spec}(R)(k)$ as a subset of k^N:

A special case of Theorem 5.5.13

Let H be a subgroup of G such that $H = \langle c \cap H \rangle$, and subgroups $H_1, \dots, H_k$ like above. Then:

$$\gamma_\xi(H) = \left\{ \sum_{i=1}^{k} \lambda_i e_{H_i} \;\middle|\; \lambda_1, \dots, \lambda_k \in k^\times \right\},$$

i.e. $\gamma_\xi(H)$ is the vector subspace of k^N generated by $e_{H_1}, \dots, e_{H_k}$, minus the vector subspaces generated by any $k-1$ of these points.

Combined with Proposition 5.1.3, this theorem gives a full description of $\mathrm{Spec}(R)(k) = \bigsqcup_H \gamma_\xi(H)$.

Chapter 6 A New Look at the Case of Symmetric Groups

Taken from [Seg22]

Main results: Theorems 6.1.1 to 6.1.3

Let $d \geq 3$ be an integer, and let c be the conjugacy class of transpositions in the symmetric group $\mathfrak{S}_d$. We consider the same objects as in Chapters 4 and 5, namely the rings of components of Hurwitz spaces, their Hilbert functions (i.e. the count of connected components of Hurwitz spaces as a function of the number of branch points), and their spectrums. Our goal is to describe these objects in the specific case where $X = \mathbb{P}^1(\mathbb{C})$, $G = \mathfrak{S}_d$, $D = \{c\}$, and $\xi(c) = 1$. This is a classical situation, studied by Hurwitz himself – indeed, it is in this context that Hurwitz spaces were first defined (cf. [Hur91]).

To state the results of this chapter, we fix a field k of characteristic zero or greater than d.

Description of Theorem 6.1.1. First, we give an explicit presentation of the monoid and ring of components, by generators and relations:

Theorem 6.1.1

The graded monoid of components $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ is generated by elements X_{ij} for all $1 \leq i < j \leq d$, of degree 2 and subject to the following relations which generate all relations among elements of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$:

— Commutation relations:

$$X_{ij}X_{kl} = X_{kl}X_{ij} \quad \text{for all } \begin{cases} 1 \leq i < j \leq d \\ 1 \leq k < l \leq d \end{cases}.$$

— Braid relations :

$$X_{ij}X_{jk} = X_{ik}X_{jk} = X_{ij}X_{ik} \quad \text{if } 1 \leq i < j < k \leq d.$$

This is a presentation by generators and relations of the monoid of components. The ring of components:

$$R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) = k[\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)]$$

has the following presentation as a graded commutative k-algebra:

$$R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) \simeq \frac{k[(X_{ij})_{1\leq i<j\leq d}]}{(X_{ij}X_{jk} - X_{ik}X_{jk},\ X_{ij}X_{jk} - X_{ij}X_{ik})_{1\leq i<j<k\leq d}}.$$

where the generators X_{ij} have degree 2.

This result follows from an exact characterization of orbits under the braid group action of tuples of transpositions whose product is 1 (Theorem 6.2.6).

Description of Theorem 6.1.2. We determine the Hilbert function $\mathrm{HF}(n)$ of the ring of components. This function counts the connected components of the Hurwitz space of $\mathfrak{S}_d$-marked covers of $\mathbb{P}^1(\mathbb{C})$, not necessarily connected,

branched at n points at which the local monodromy elements are transpositions.

If n is odd, then $\mathrm{HF}(n) = 0$. We focus on the values taken by HF at even integers; these values are described by the following theorem:

Theorem 6.1.2

Let $d' = \lfloor d/2 \rfloor$. There exists a polynomial with leading coefficient:

$$\frac{d!}{2^{d'}(d')!(d'-1)!} n^{d'-1} \text{ if } d \text{ is even,}$$
$$\left(1 + \frac{d'}{3}\right) \frac{d!}{2^{d'}(d')!(d'-1)!} n^{d'-1} \text{ if } d \text{ is odd,}$$

such that $\mathrm{HF}(2n)$ coincides with this polynomial for $n \geq d-1$.
We have an exact formula for $\mathrm{HF}(2n)$:

$$\sum_{s=1}^{d-1} \sum_{w=1}^{d-s} \sum_{j=0}^{w} (-1)^{w-j} \binom{n-s+w-1}{w-1} \binom{d}{d-s-w,\, w-j,\, s+j} S(s+j,\, j)$$

where $S(n,,k)$ denotes the Stirling numbers of the second kind.

Description du Theorem 6.1.3. In the spirit of Chapter 5, we describe the set of k-points of the spectrum of the ring of components $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$, seen as a subset of $\mathbb{A}^{\frac{d(d-1)}{2}}(k) = k^{\frac{d(d-1)}{2}}$. We are in a situation covered by Theorem 5.5.13, and we obtain a similar description. We use couples (i,j) with $1 \leq i < j \leq d$ to index the coordinates in the vector space $k^{\frac{d(d-1)}{2}}$. We denote by $e_{i,j}$ the basis vector associated with the coordinate (i,j), and we define for every subset $A \subseteq \{1,\dots,d\}$ the vector e_A, sum of the basis vectors $e_{i,j}$ taken over pairs (i,j) where $i<j$ and $i,j \in A$.

We then describe the set of k-points of the spectrum of the ring of components as follows:

Theorem 6.1.3

The set $\mathrm{Spec}\left(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)\right)(k)$ is the union of the vector subspaces of $k^{\frac{d(d-1)}{2}}$ spanned by the vectors $e_{A_1},\dots,e_{A_l}$, taken over all maximal families $\{A_1,\dots,A_l\}$ of disjoint subsets of $\{1,\dots,d\}$.

Chapter 8 Fields of Definition of Components of Hurwitz Spaces

Taken from [Seg23]

Main result: Theorem 8.1.2

In this chapter, we study fields of definition of connected components of Hurwitz spaces. Specifically, we describe situations where the gluing of two components, both defined over a given number field K, is also defined over K. This work builds on and extends the connections highlighted in [Cau12], which generalize the results of [DE06].

The search for components with a small field of definition is related to the regular inverse Galois problem. Indeed, a regular Galois extension of $\mathbb{Q}(t)$ whose Galois group is G corresponds to a rational point of the corresponding Hurwitz space; the connected component of this point is then defined over $\mathbb{Q}$. Therefore, finding components defined over $\mathbb{Q}$ is an essential step, which helps us know where rational points can reasonably be expected to be found.

Description of Theorem 8.1.2. Consider a number field K and two connected components x and y of the Hurwitz space of marked G-covers of the projective line. Let H_1 and H_2 be the respective monodromy groups of the marked G-covers belonging to the components x and y, and let H be the subgroup of G generated by H_1 and H_2.

Assume that the components x and y are defined over K. Our main focus is Question 8.1.1: is the component xy, obtained by gluing x and y, defined over K?

Theorem 8.1.2 provides a partial answer to this question:

Theorem 8.1.2

(i) If every element of H can be written is a product of an element of H_1 and an element of H_2, then the glued component xy is defined over K.

(ii) There exists an integer M, depending only on the group G, such that if every conjugacy class of H that is a monodromy class of the G-covers in the component xy is a monodromy class at at least M branch points, then the component xy is defined over K. In particular, $(xy)^M$ is defined over K.

(iii) There exist elements $\gamma, \gamma' \in H$ such that $\left\langle H_1^{\gamma}, H_2^{\gamma'} \right\rangle = H$ and such that the component $x^{\gamma}y^{\gamma'}$, obtained by letting γ, γ' act on the components x, y and by gluing the resulting components, is defined over K.

Each of the three statements that make up Theorem 8.1.2 is proven using specific methods. Theorem 8.1.2 can be seen as a weakened version, over number fields, of the gluing operation: we do not glue marked G-covers themselves, but their components.

An application of Theorem 8.1.2 (iii) is given in Example 8.4.6. The only sporadic simple group not yet known to be a Galois group over $\mathbb{Q}$ is the Mathieu group M_{23}: the question of its realization has been extensively studied [Hä22]. We construct components defined over $\mathbb{Q}$ of connected M_{23}-covers having only four branch points (to be compared with the fifteen branch points used by [Cau16]).

We also prove Proposition 8.2.8, which states that the action of the absolute Galois group of K on components of Hurwitz spaces is entirely determined by the action on components up to a certain number of branch points (one can take $|G|\exp(G)$).

1.3. Outline of this thesis

We now describe the organization of the text, chapter by chapter.

Chapters 2 and 3 are expository chapters in French.

In Chapter 2, we present classical facts about branched topological (G-)covers (Sections 2.2 and 2.3) and their combinatorial description (Section 2.4). The statements of this chapter are classical: for many, the introduction (Section 2.1) or the summary in English (Section 2.5) will provide enough information.

In Chapter 3, we define Hurwitz spaces (Sections 3.2 and 3.3) as well as monoids and rings of components defined in [EVW16] (Section 3.4). We mention various properties of these objects. The chapter ends with a summary in English (Section 3.5).

Chapters 4 to 6 are taken from the preprint [Seg22]. This paper has been split into three chapters to give more autonomy to the topics developed in each chapter.

In Chapter 4, we prove Theorem 4.3.1. This theorem gives asymptotic estimates of the number of components of Hurwitz spaces of G-covers whose monodromy is constrained and whose number of branch points tends to infinity.

In Chapter 5, we study the geometry of the spectrum of the ring of components, which we relate to the combinatorial questions of the previous chapter. In particular, we state and prove Theorems 5.1.4 and 5.5.13.

Chapter 6 concerns the explicit description of objects from Chapters 4 and 5 in the situation of $\mathfrak{S}_d$-covers of the complex projective line whose local monodromy elements are transpositions. We give a presentation of the monoid and of the ring of components (Theorem 6.1.1), a computable criterion of equality between elements of the monoid of components (Theorem 6.2.6 (v)), and a description of the set of geometric points of the spectrum of the ring of components (Theorem 6.1.3).

Chapter 7 is another exposition chapter, whose content is known. We quickly present algebraic G-covers of the projective line, the equivalence between covers of the line and function fields (Subsection 7.1.3), Hilbert's irreducibility theorem (Subsection 7.1.3), Riemann's existence theorem (Subsection 7.1.4), and Hurwitz spaces of branched G-covers (marked or not) of $\mathbb{P}^1$, seen as schemes (Section 7.2). We detail the links between these schemes and topological Hurwitz spaces, and we insist on the role of these spaces in the study of arithmetical question – notably for inverse Galois theory. A summary in English concludes the chapter (Section 7.3).

Chapter 8, whose content is taken from the preprint [Seg23], is centered around the proof of Theorem 8.1.2. The three statements which constitute the theorem are proved in three corresponding sections (Sections 8.2 to 8.4). Each section corresponds to a particular approach to the problem with its own tools: the braid action in Section 8.2, the lifting invariant (presented in Subsection 3.4.7) in Section 8.3, and Harbater's patching theory in Section 8.4.

In Appendix A, which comes after the text, the reader will find a bilingual glossary (Appendix A.1) and an index of notations (Appendix A.2).

Finally, the document ends with Appendix B, which is an attempt (in French) to give an idea of the contents of this thesis to non-mathematicians.

Key results are indicated by a small key 🔑 in the margin.

1.4. Conventions and notations

In this section, we define and introduce various terms and symbols which are used in the whole thesis.

1.4.1. General

— We denote the cardinality of a set X by $|X|$.

— If C is an object in any category, its *automorphism group* $\mathrm{Aut}(C)$ is the set of isomorphisms between C and itself. Given a morphism $C \to D$, the group $\mathrm{Aut}_D(C)$ is the subgroup of $\mathrm{Aut}(C)$ consisting of automorphisms σ which make the following diagram commute:

$$\begin{array}{ccc} C & \xrightarrow{\quad\sigma\quad} & C \\ & \searrow \quad \swarrow & \\ & D & \end{array}$$

— The n-th symmetric group $\mathfrak{S}_n$ is understood as the set of permutations of the set $\{1, \ldots, n\}$. If A is a non-empty subset of $\{1, \ldots, n\}$, we denote by $\mathfrak{S}_A$ the subgroup of $\mathfrak{S}_n$ consisting of permutations that stabilize every element not in A. If $A_1, \ldots, A_r$ are pairwise disjoint subsets of $\{1, \ldots, n\}$, then $\mathfrak{S}_{A_1} \times \cdots \times \mathfrak{S}_{A_r}$ is the subgroup of $\mathfrak{S}_n$ generated by $\mathfrak{S}_{A_1}, \ldots, \mathfrak{S}_{A_r}$.

— If γ_1, γ_2 are paths (or loops, or homotopy classes thereof) in a topological space X, then we denote by $\gamma_1 * \gamma_2$ their concatenation in the order "first γ_1, then γ_2" when they are composable. We do not always include the character $*$, especially when dealing with homotopy classes of loops.

— If $\underline{t} = (t_1, \ldots, t_n)$ is a list of n points of a topological space (or algebraic variety) X, then we denote by $X \setminus \underline{t}$ the subspace of X obtained by removing the points $t_1, \ldots, t_n$. The same applies if $\underline{t}$ is a finite subset of X, or if it is an unordered list – i.e., the orbit of an n-tuple under the action of the symmetric group $\mathfrak{S}_n$.

— We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Number fields are equipped with an embedding in $\overline{\mathbb{Q}}$. If K is a number field, we denote by Γ_K the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$. The cyclotomic character of K is the group morphism $\chi : \Gamma_K \to \widehat{\mathbb{Z}}^\times$ determined by the Galois action on roots of unity: if $\zeta \in \overline{\mathbb{Q}}$ is an n-th root of unity and $\sigma \in \Gamma_K$, then $\sigma(\zeta) = \zeta^{\chi(\sigma) \mod n}$.

We use a variant of the big O notation to state asymptotic results, to indicate that our bounds are sharp (hence the use of the $\sharp$ symbol):

Definition: *Sharp big O notation*

Definition 1.4.1. If f is a function $\mathbb{N} \to \mathbb{N}$ and $\zeta \in \{0, 1, \ldots\}$, the notation:

$$f(n) = O^\sharp\left(n^\zeta\right)$$

means that $f(n) = O(n^\zeta)$ and $f(n) \neq o(n^\zeta)$, i.e.:

$$0 < \limsup_{n \to \infty} \left(n^{-\zeta} f(n)\right) < \infty.$$

The exponent ζ from Definition 1.4.1, if it exists, is uniquely defined:

$$\zeta = \limsup_{n \to \infty} \frac{\log f(n)}{\log n}.$$

1.4.2. **Groups**

In this work, G always denotes a finite group. The characters $H, H', H_1, H_2, \ldots$ usually denote subgroups of the group G. The symbols $D, D_H, \ldots$ are used to denote sets of disjoint non-empty conjugation-invariant subsets of G or H (possibly conjugacy classes). Elements of the set D, as well as conjugacy classes, are denoted by the greek letters $\gamma, \gamma', \ldots$. The symbols $D^*, D_H^*, \ldots$ are reserved for the particular case where all elements are conjugacy classes. The character c often denotes a conjugation-invariant subset of G (possibly a conjugacy class); in general, c is the union of the sets $\gamma \in D$ and D^* is the set of all conjugacy classes G contained in c. The symbol ξ refers to a fixed map $D \to \{1, 2, \ldots\}$, seen as a multiplicity map.

Let G be a finite group.

— If X is a subset of G, then $\langle X \rangle$ is the smallest subgroup of G containing X.

— If X and Y are two subsets (or subgroups) of G, then XY is the set of products xy where $x \in X$ and $y \in Y$.

— If $g, h \in G$, we use the following notation for conjugation:

$$g^h = hgh^{-1}.$$

The group of inner automorphisms of G is denoted by $\mathrm{Inn}(G)$.

— A *conjugation-invariant subset* of G is a union of conjugacy classes of G.

— If g is an element of G, its order is denoted by $\mathrm{ord}(g)$. Similarly, if γ is a conjugacy class of G, the order of any of its elements is denoted by $\mathrm{ord}(\gamma)$. The exponent of the group G is denoted by $\exp(G)$.

— If $n \in \widehat{\mathbb{Z}}$ is a profinite integer and $g \in G$, then g^n is the element g^k where $k = n \mod |G|$. If γ is a conjugacy class of G and n is a profinite integer (or an integer), then γ^n is the well-defined conjugacy class of the n-th powers of elements of γ.

— Let K be a number field. We define K-rational subsets of G in the following way:

Definition 1.4.2. A subset c of G is *K-rational* if for every $g \in c$ and $\sigma \in \Gamma_K$ we have $g^{\chi(\sigma)} \in c$.

If $K = \mathbb{Q}$, we have $\mathrm{Im}(\chi) = \widehat{\mathbb{Z}}^\times$. Therefore, $\mathbb{Q}$-rational subsets are subsets closed under n-th powers for all n coprime with $|G|$. In contrast, if K contains all $|G|$-th roots of unity, then the image of χ is trivial modulo $|G|$ and every subset of G is K-rational. Examples of sets which are always K-rational include G, $G \setminus \{1\}$, as well as any subset of G consisting of involutions.

— We denote by G^{ab} the abelianization of the group G.

1.4.3. **Tuples**

We denote tuples (i.e. ordered lists) with underlined letters.
If $\underline{g} = (g_1, g_2, \ldots, g_n)$ is an n-tuple of elements of a group G, then:

Definition 1.4.3. The *size* of the n-tuple $\underline{g}$, denoted by $\left|\underline{g}\right|$, is the number n of items in $\underline{g}$.

Definition: *Size of a tuple*

Definition 1.4.4. The *product* of the n-tuple $\underline{g}$, denoted by $\pi\underline{g}$, is the element $g_1 g_2 \cdots g_n$ of G.

Definition: *Product of a tuple*

Definition 1.4.5. The *group* of the n-tuple $\underline{g}$, denoted by $\left\langle \underline{g} \right\rangle$, is the subgroup of G generated by $g_1, g_2, \ldots, g_n$.

Definition: *Group of a tuple*

Following [EVW12], we now define the *multidiscriminant*. For this, let H be a subgroup of G and c be a conjugation-invariant subset of H such that all the elements g_i belong to c. We denote by D^* the set of all conjugacy classes of H which are contained in c. A conjugacy class $\gamma \in D^*$ *appears in* $\underline{g}$ (or *occurs*) if there is some i for which $g_i \in \gamma$.

Definition 1.4.6. The (H,c)-*multidiscriminant* of $\underline{g}$ is the map $\mu_{H,c}(\underline{g}) : D^* \to \{0, 1, \ldots\}$ which maps a class $\gamma \in D^*$ to the number of items of $\underline{g}$ which are in γ, i.e.:

Definition: (H,c)-*multidiscriminant of a tuple*

$$\mu_{H,c}(\underline{g})(\gamma) = \left|\{i \in \{1, \ldots, n\} \mid g_i \in \gamma\}\right|.$$

When (H,c) is not specified, the *multidiscriminant* of $\underline{g}$ is the (H,c)-multidiscriminant where $H = \left\langle \underline{g} \right\rangle$ and c is the smallest conjugation-invariant subset of H which contains $g_1, \ldots, g_n$.

If $\underline{g}_1, \ldots, \underline{g}_s$ are tuples of elements of G, of respective sizes $r_i = \left|\underline{g}_i\right|$, then:

Definition 1.4.7. The *concatenation* $\underline{g}_1 \underline{g}_2 \cdots \underline{g}_s$ of the tuples $\underline{g}_1, \ldots, \underline{g}_s$ is the following $(\sum r_i)$-tuple of elements of G:

Definition: *Concatenation of tuples*

$$\left(g_{1,1}, \ldots, g_{1,r_1}, g_{2,1}, \ldots, g_{2,r_2}, \ldots, g_{s,1}, \ldots, g_{s,r_s}\right).$$

The *group* $\left\langle \underline{g}_1, \ldots, \underline{g}_s \right\rangle$ generated by the tuples $\underline{g}_1, \ldots, \underline{g}_s$ is the subgroup of G generated by the subgroups $\left\langle \underline{g}_1 \right\rangle, \ldots, \left\langle \underline{g}_s \right\rangle$.

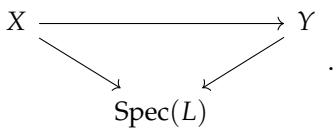
1.4.4. Terminology for schemes

We detail here the terminology and notation which we use to refer to some properties of schemes, of their subschemes or of their points. These terms are used extensively in Chapters 7 and 8, but they can be ignored for other chapters.

Let L be a field. Our definition of L-schemes includes separatedness:

Definition 1.4.8. *L-schemes* are schemes equipped with a separated morphism into $\mathrm{Spec}(L)$. A *morphism* between two L-schemes X and Y is a morphism of schemes $X \to Y$ which makes the following diagram commute:

Definition: *L-scheme*



Let $L' \mid L$ be a field extension and X be an L-scheme of finite type. We denote extension of scalars by a subscript:

Definition: *Extension of scalars*

Definition 1.4.9. The *extension of scalars of X to L'* is the following L'-scheme:

$$X_{L'} \overset{\text{def}}{=} X \underset{\mathrm{Spec}(L)}{\times} \mathrm{Spec}(L').$$

It fits in the following Cartesian square:

$$\begin{array}{ccc} X_{L'} & \longrightarrow & \mathrm{Spec}(L') \\ \downarrow & \lrcorner & \downarrow \\ X & \longrightarrow & \mathrm{Spec}(L) \end{array}$$

Our definitions and notation for points are the following:

Definition: *L'-point* *Geometric point*

Definition 1.4.10. An *L'-point* of X is a morphism of L-schemes from $\mathrm{Spec}(L')$ to X, or equivalently a morphism of L'-schemes from $\mathrm{Spec}(L')$ to $X_{L'}$. The set of L'-points of X is denoted by $X(L')$. The $\overline{L}$-points of X are also called *geometric points*.

Definition: *L-rational point* *L-model*

Definition 1.4.11. An L'-point $x \in X(L')$ is *L-rational* if there exists an L-point $x' \in X(L)$ such that the following diagram of L-schemes commutes:

$$\begin{array}{ccccc} \mathrm{Spec}(L') & \longrightarrow & \mathrm{Spec}(L) & \xrightarrow{x'} & X \\ & \searrow & & \nearrow_{x} & \end{array}$$

The point x' is called an *L-model* of the point x.

We introduce the analogous notion for subschemes of $X_{L'}$:

Definition: *Subscheme defined over L* *Field of definition*

Definition 1.4.12. An L'-subscheme Y of $X_{L'}$ is *defined over L* if there exists an L-subscheme Y' of X such that $Y = (Y')_{L'}$ (as subschemes of $X_{L'}$). In this case, the field L is a *field of definition* of Y, and the L-subscheme Y' is an *L-model* of Y.

Assume now $L' \mid L$ is Galois. An automorphism $\sigma \in \mathrm{Gal}(L' \mid L)$ induces an L-automorphism of $\mathrm{Spec}(L')$ which we denote by $\mathrm{Spec}(\sigma)$. The group $\mathrm{Gal}(L' \mid L)$ acts on an L'-point $x \in X(L')$ by the formula $\sigma.x = x \circ \mathrm{Spec}(\sigma)$ and on an L'-subscheme $Y \subseteq X_{L'}$ by pullback along $\mathrm{id}_X \underset{\mathrm{Spec}(L)}{\times} \mathrm{Spec}(\sigma)$:

$$\begin{array}{ccc} \mathrm{Spec}(L') & & \\ {\scriptstyle \mathrm{Spec}(\sigma)}\downarrow & \searrow^{\sigma.x} & \\ \mathrm{Spec}(L') & \xrightarrow[x]{} & X \end{array} \qquad \begin{array}{ccc} \sigma.Y & \longrightarrow & X_{L'} \\ \downarrow & \lrcorner & \downarrow{\scriptstyle \mathrm{id}_X \underset{\mathrm{Spec}(L)}{\times} \mathrm{Spec}(\sigma)} \\ Y & \longrightarrow & X_{L'} \end{array}.$$

We state the following classical "descent" results:

Proposition: *A result of Galois descent*

Proposition 1.4.13. *The following equivalences hold:*

— *An L'-point of X is L-rational if and only if it is invariant under the action of* $\mathrm{Gal}(L' \mid L)$.

— *An L'-subscheme Y of $X_{L'}$ is defined over L if and only if it is globally preserved by the action of* $\mathrm{Gal}(L' \mid L)$*, i.e. for every $\sigma \in \mathrm{Gal}(L' \mid L)$ there is an L'-automorphism σ' of Y such that the following diagram commutes:*

$$\begin{array}{ccc} Y & \overset{\subseteq}{\hookrightarrow} & X_{L'} \\ {\scriptstyle \sigma'}\downarrow & & \downarrow{\scriptstyle \mathrm{id}_X \underset{\mathrm{Spec}(L)}{\times} \mathrm{Spec}(\sigma)} \\ Y & \overset{\subseteq}{\hookrightarrow} & X_{L'} \end{array}.$$

— *If L' is algebraically closed and Y is a reduced L'-subscheme of $X_{L'}$, then Y is defined over L if and only if the subset $Y(L')$ of $X(L')$ is globally preserved by the action of* $\mathrm{Gal}(L' \mid L)$.

Chapitre 2

Théorie topologique des G-revêtements

(A summary of this chapter in English may be found in Section 2.5)

Résumé du chapitre

Dans ce chapitre, nous rappelons les définitions et faits principaux concernant les G-revêtements, qu'on aborde ici de façon purement topologique. Nous en profitons pour lever les possibles ambiguïtés terminologiques : par exemple, ici, un G-revêtement n'est pas nécessairement connexe.

On insiste sur la description combinatoire des G-revêtements et sur la possibilité de les recoller.

Organisation du chapitre

L'eau que tu bois,
A connu la mer.
— E. Guillevic,
Du domaine, 1977.

Pour tout le chapitre, on fixe un groupe fini G.

2.1. Introduction

Dans ce chapitre d'exposition, on présente des généralités sur les revêtements topologiques et les G-revêtements (Section 2.2), sur les revêtements ramifiés (Section 2.3), et sur la description combinatoire des G-revêtements de la droite (Section 2.4), notamment sur la possibilité de recoller ces revêtements (Sous-section 2.4.2). À l'attention des lecteur·rice·s ayant connaissance de la théorie des revêtements, on résume brièvement le contenu de ce chapitre en insistant sur les choix terminologiques les moins usuels :

— Nous considérons principalement des G-revêtements ramifiés de la droite affine complexe $\mathbb{A}^1(\mathbb{C})$ (c'est-à-dire, topologiquement, du plan $\mathbb{R}^2$) et de la droite projective complexe (la sphère de Riemann $\mathbb{S}^1$).

— On appelle *G-revêtement* d'un espace topologique X, ramifié en une configuration $\underline{t} = \{t_1, \dots, t_n\}$ (Définition 2.3.8) un revêtement p de $X \setminus \underline{t}$ muni d'une action du groupe G (c'est-à-dire un morphisme de G dans le groupe $\mathrm{Aut}(p)$ des automorphismes du revêtement) qui est libre et transitive sur chaque fibre (Définitions 2.2.10 et 2.3.15).

  On n'exige pas des points de $\underline{t}$ qu'ils soient effectivement des points de ramification (voir la définition 2.3.27 et la proposition 2.3.26), et on ne demande pas aux G-revêtements d'être connexes. En particulier, un G-revêtement n'a pas nécessairement G pour groupe d'automorphismes (voir la proposition 2.2.25).

  Un G-revêtement de l'espace topologique pointé (X, t_0) est *marqué* lorsqu'il est non-ramifié en t_0 et muni d'un point marqué dans la fibre au-dessus de t_0 (Définition 2.2.13).

— Étant donné un G-revêtement marqué de l'espace (X, t_0), ramifié en une configuration $\underline{t}$, on peut considérer son *morphisme de monodromie* φ (Définition 2.2.17), qui est un morphisme de groupes :

$$\varphi : \pi_1(X \setminus \underline{t}, t_0) \to G.$$

Ce morphisme est surjectif si et seulement si le revêtement considéré est connexe. En général, son image est un sous-groupe de G qu'on appelle le *groupe de monodromie* du G-revêtement marqué (Définition 2.2.18). Le morphisme de monodromie caractérise uniquement le G-revêtement marqué à isomorphisme de G-revêtements marqués près (Théorème 2.2.26).

— Dans le cas où X est la droite affine $\mathbb{A}^1(\mathbb{C})$, le groupe fondamental $\pi_1(X \setminus \underline{t}, t_0)$ est engendré librement par des générateurs particuliers, qui forment un *bouquet topologique* associé à la configuration $\underline{t}$ (Définition 2.3.19 et Proposition 2.4.12). Un bouquet topologique étant fixé, les classes d'isomorphisme de G-revêtements marqués de la droite affine $\mathbb{A}^1(\mathbb{C})$ ramifiés en une configuration $\underline{t} = \{t_1, \dots, t_n\}$ donnée sont en bijection avec les n-uplets $\underline{g} = (g_1, \dots, g_n)$ d'éléments de G (Théorème 2.4.14). On dit que le uplet $\underline{g}$ est la *description des cycles de branchement* du G-revêtement marqué (pour le bouquet choisi), les éléments $g_1, \dots, g_n$ sont les *éléments locaux de monodromie* et les classes de conjugaison de ces éléments sont les *classes de monodromie* (qui ne dépendent pas du choix du bouquet) (Définitions 2.3.25 et 2.3.28).

Dans le cas où X est la droite projective complexe $\mathbb{P}^1(\mathbb{C})$, un bouquet topologique $(\gamma_1, \dots, \gamma_n)$ engendre également le groupe fondamental $\pi_1(X \setminus \underline{t}, t_0)$, et les générateurs satisfont la relation $\gamma_1 \cdots \gamma_n = 1$. Dans la description combinatoire précédente, il faut ne considérer que les uplets $\underline{g} = (g_1, \dots, g_n)$ dont le produit $\pi\underline{g} = g_1 \cdots g_n$ vaut 1. L'ensemble de ces n-uplets est en bijection avec l'ensemble des classes d'isomorphisme de G-revêtements marqués de $\mathbb{P}^1(\mathbb{C})$ ramifiés en une configuration donnée de n points de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_0\}$.

Pour les G-revêtements non-marqués, les uplets doivent être considérés modulo l'action de conjugaison de G (de tous les éléments du uplet simultanément) – action qui correspond à un changement de point marqué (Proposition 2.2.20, Corollaire 2.2.21, Théorème 2.2.28, et Remarque 2.4.15).

— Étant donnés deux G-revêtements marqués de $\mathbb{P}^1(\mathbb{C})$, ramifiés en des configurations $\underline{t}$ et $\underline{t}'$ disjointes (pour lesquelles on choisit des bouquets), on définit un recollement de ces revêtements (Définition 2.4.18). Cette opération de recollement correspond, en termes de uplets d'éléments de G (c'est-à-dire de la description des cycles de branchement) à la concaténation des uplets :

$$(g_1, \dots, g_n)(g'_1, \dots, g'_{n'}) = (g_1, \dots, g_n, g'_1, \dots, g'_{n'}).$$

Le nombre de points de branchement du G-revêtement marqué ainsi obtenu est la somme des nombres de points de branchements des revêtements originaux, et son groupe de monodromie est le sous-groupe de G engendré par leurs groupes de monodromie.

2.2. Généralités sur les revêtements topologiques

2.2.1. **Revêtements topologiques**

Définition: *Revêtement topologique*

Définition 2.2.1. Soit $d \geq 1$ un entier. Un *revêtement* (de degré d) d'un espace topologique X est une application continue $p : Y \to X$ telle que tout point $x \in X$ admette un voisinage ouvert N au-dessus duquel il y a un homéomorphisme :

$$p^{-1}(N) \simeq N \times \{1, \ldots, d\}$$

dont la projection sur la première coordonnée coïncide avec la restriction de p à $p^{-1}(N)$.

Tout revêtement est une surjection ouverte. Les revêtements de degré 1 sont exactement les homéomorphismes.

Définition: *Fibre d'un revêtement*

Définition 2.2.2. La *fibre* d'un revêtement $p : Y \to X$ au-dessus d'un point $x \in X$ est l'ensemble $p^{-1}(x) \subseteq Y$ des points de Y que p envoie sur x. C'est un ensemble fini, dont le cardinal est le degré du revêtement p.

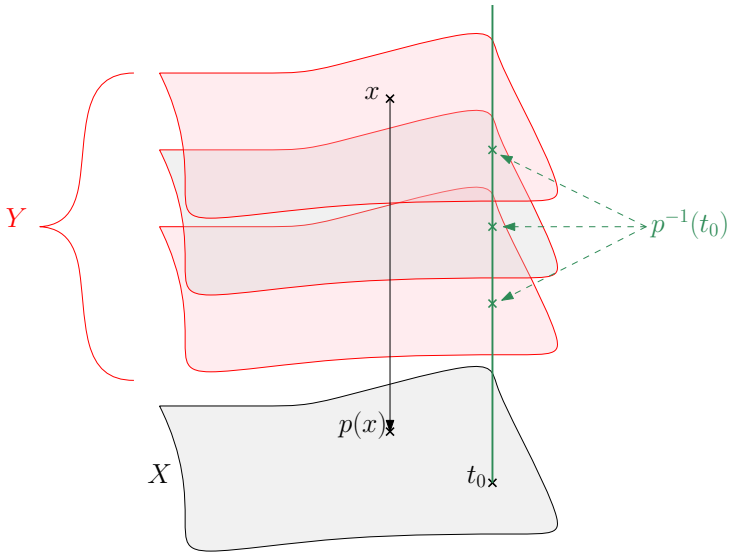


Figure 2.2.3. Un revêtement p de degré 3, dessiné sur un voisinage de t_0 au-dessus duquel il est trivial. La fibre $p^{-1}(t_0)$ de p au-dessus du point t_0 est représentée par les trois points verts au-dessus de t_0.

Définition: *Morphisme de revêtements*

Définition 2.2.4. Si $p : Y \to X$ et $p' : Y' \to X$ sont deux revêtements d'un même espace X, un *morphisme de revêtements* $p \to p'$ est une application continue $f : Y \to Y'$ telle que $p' \circ f = p$. Cette notion de morphisme définit une catégorie des revêtements de X, ainsi que des notions naturelles d'*isomorphismes entre revêtements* et de *groupe des automorphismes* du revêtement p:

$$\mathrm{Aut}(p) \overset{\text{def}}{=} \{\sigma \in \mathrm{Aut}(Y) \mid p \circ \sigma = p\}.$$

Définition: *Revêtement connexe*

Définition 2.2.5. Un revêtement $p : Y \to X$ est *connexe* si son domaine Y est connexe.

Définition: *Revêtement galoisien*

Définition 2.2.6. Un revêtement $p : Y \to X$ est *galoisien* si l'action de son groupe des automorphismes $\mathrm{Aut}(p)$ sur la fibre $p^{-1}(x)$ est transitive, quel que soit $x \in X$.

Fait: *Le groupe des automorphismes d'un revêtement agit librement sur les fibres*

Fait 2.2.7. Soit $p : Y \to X$ un revêtement connexe, avec X séparé. L'action du groupe des automorphismes $\mathrm{Aut}(p)$ sur chaque fibre $p^{-1}(x)$ est libre.

Fait 2.2.8. Pour qu'un revêtement connexe $p : Y \to X$ soit galoisien, il suffit que l'action de $\mathrm{Aut}(p)$ sur une fibre donnée soit transitive.

Définition: *Revêtement marqué*

Définition 2.2.9. Un *revêtement marqué* de l'espace topologique marqué (X, t_0) est un couple $(p, \star)$ où $p : Y \to X$ est un revêtement et $\star \in p^{-1}(t_0)$. Les *morphismes* entre deux revêtements marqués $(p, \star)$ et $(p', \star')$ sont les morphismes de revêtements $f : p \to p'$ satisfaisant $f(\star) = \star'$.

2.2.2. G-revêtements

Définition: *G-revêtement*

Définition 2.2.10. Un *G-revêtement* est un revêtement $p : Y \to X$ muni d'un morphisme de groupes $\alpha : G \to \mathrm{Aut}(p)$ tel que l'action de G sur les fibres de p (induite par α) soit libre et transitive.

Si (p, α) est un G-revêtement, alors le morphisme α est nécessairement injectif (puisque l'action de G est libre) et p est un revêtement galoisien de degré $|G|$ (puisque l'action de G est transitive et se factorise par l'action de $\mathrm{Aut}(p)$, qui est donc également transitive).

Proposition: *Le groupe d'automorphismes d'un G-revêtement connexe est G*

Proposition 2.2.11. *Si (p, α) est un G-revêtement connexe, alors α est un isomorphisme entre G et* $\mathrm{Aut}(p)$.

Démonstration. Via le morphisme α, le groupe G s'injecte dans le groupe $\mathrm{Aut}(p)$. Ces deux groupes agissent librement (voir le fait 2.2.7) et transitivement sur les fibres de p, ils sont donc de même ordre (le degré de p). Par conséquent, α est un isomorphisme. □

Définition: *Morphisme de G-revêtements*

Définition 2.2.12. Si (p, α) et (p', α') sont deux G-revêtements, un *morphisme de G-revêtements* entre eux est un morphisme de revêtements $f : p \to p'$ qui commute avec l'action de G, c'est-à-dire qu'il satisfait $f \circ \alpha(g) = \alpha'(g) \circ f$ pour tout $g \in G$.

Soit (p, α) un G-revêtement, avec $p : Y \to X$. Si $g \in G$, $y \in Y$, et s'il n'y a aucune ambiguïté sur le G-revêtement, nous désignons par $g.y$ l'élément $\alpha(g)(y)$ de Y :

$$g.y = \alpha(g)(y).$$

Définition: *G-revêtement marqué*

Définition 2.2.13. Un *G-revêtement marqué* de l'espace topologique pointé (X, t_0) est un triplet $(p, \star, \alpha)$ où p est un revêtement $Y \to X$, le point $\star$ est un point de la fibre $p^{-1}(t_0)$, et α est un morphisme $G \to \mathrm{Aut}(p)$ induisant une action libre et transitive de G sur les fibres. Un *morphisme de G-revêtements marqués* entre $(p, \star, \alpha)$ et $(p', \star', \alpha')$ est un morphisme de revêtements marqués $f : (p, \star) \to (p', \star')$ qui commute avec l'action de G.

Le plus souvent, on n'écrit pas explicitement le morphisme α et on dit que $(p, \star)$ est un G-revêtement marqué. Par ailleurs, dans la définition 2.2.13, $\mathrm{Aut}(p)$ désigne bien le groupe des automorphismes du revêtement *non-marqué* p.

2.2.3. Morphisme de monodromie

Le but de cette sous-section est de définir le morphisme de monodromie d'un G-revêtement marqué. La proposition suivante, qui établit l'existence de relèvement de chemins par un revêtement, est classique ([Sza09, Lemma 2.3.2]) :

Proposition: *Relèvement unique des chemins*

Proposition 2.2.14. *Soit $p : Y \to X$ un revêtement. Soit $\gamma : [0,1] \to X$ un chemin continu. Soit $x = \gamma(0)$, $F = p^{-1}(x)$, $x' = \gamma(1)$ et $F' = p^{-1}(x')$. Alors :*

1. *Pour tout point $\star \in F$, il existe un unique chemin continu $\widetilde{\gamma} : [0,1] \to Y$ dans Y qui relève γ, c'est-à-dire que $p \circ \widetilde{\gamma} = \gamma$, et tel que $\widetilde{\gamma}(0) = \star$. On désigne par $\star[\gamma]$ le point $\widetilde{\gamma}(1)$, qui se trouve dans la fibre $F' = p^{-1}(x')$.*
2. *L'application $\star \mapsto \star[\gamma]$ définit une bijection $F \xrightarrow{\sim} F'$ qui ne dépend que de la classe d'homotopie de γ. Par ailleurs, si γ, γ' sont deux chemins concaténables et $\star \in F$, on a $(\star[\gamma])\,[\gamma'] = \star[\gamma\gamma']$.*
3. *Pour tout automorphisme $\sigma \in \mathrm{Aut}(p)$ et pour tout point $\star \in F$, on a l'égalité $\sigma(\star[\gamma]) = (\sigma(\star))[\gamma]$.*

En utilisant la proposition 2.2.14, on montre l'existence de ce qui sera le morphisme de monodromie (Définition 2.2.17) :

Proposition: *Existence du morphisme de monodromie*

Proposition 2.2.15. *Soit $(p, \star, \alpha)$ un G-revêtement marqué de l'espace pointé (X, t_0). Il existe un unique morphisme $\varphi : \pi_1(X, t_0) \to G$ satisfaisant, pour tout $\gamma \in \pi_1(X, t_0)$, l'égalité :*

$$\varphi(\gamma).\star = \star[\gamma].$$

Pour un $\gamma \in \pi_1(X, t_0)$ donné, l'existence et l'unicité de $\varphi(\gamma)$ résulte du fait que l'action de G sur la fibre au-dessus de t_0 est libre et transitive :

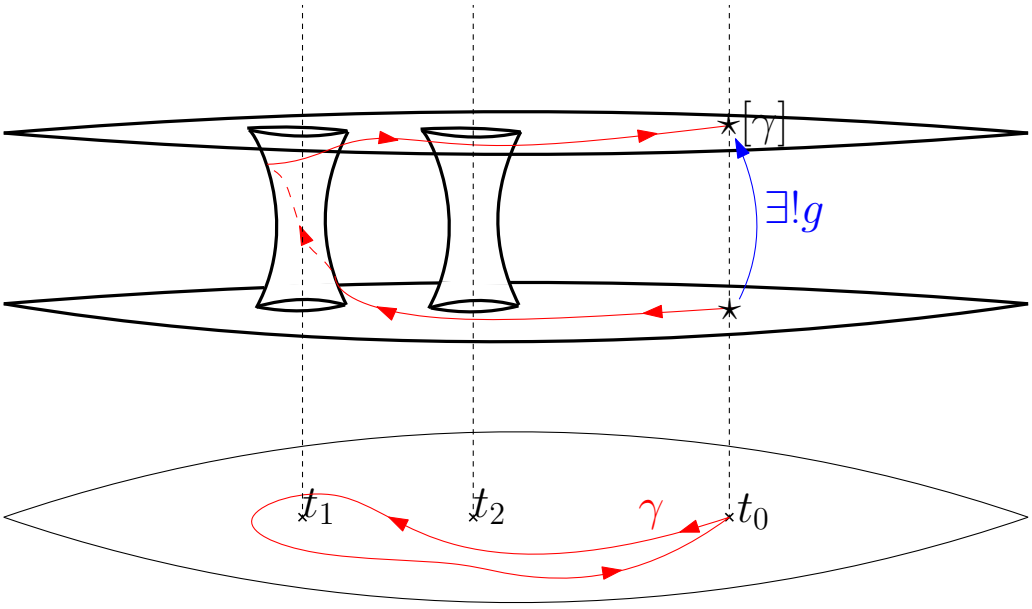


Figure 2.2.16. Une illustration de la définition de $\varphi(\gamma)$

Le fait que φ soit un morphisme de groupes découle de l'unicité.

Définition: *Morphisme de monodromie d'un G-revêtement marqué*

Définition 2.2.17. Le *morphisme de monodromie* du G-revêtement marqué $(p, \star, \alpha)$ est le morphisme φ de la proposition 2.2.15.

Définition: *Groupe de monodromie d'un G-revêtement marqué*

Définition 2.2.18. Le *groupe de monodromie* d'un G-revêtement marqué est le sous-groupe de G obtenu comme image du morphisme de monodromie associé $\varphi : \pi_1(X, t_0) \to G$.

Proposition: *Groupe fondamental d'un G-revêtement*

Proposition 2.2.19. *Soit $(p, \star, \alpha)$ un G-revêtement marqué de (X, t_0), avec $p : (Y, \star) \to (X, t_0)$, et soit $\varphi : \pi_1(X, t_0) \to G$ son morphisme de monodromie. Alors le groupe fondamental $\pi_1(Y, \star)$ de Y est isomorphe à $\ker(\varphi)$. Autrement dit, nous avons la suite exacte suivante :*

$$1 \to \pi_1(Y, \star) \overset{p\circ -}{\to} \pi_1(X, t_0) \overset{\varphi}{\to} G.$$

Démonstration. La formule $\gamma \mapsto p \circ \gamma$ induit un morphisme de groupes :

$$f : \gamma \in \pi_1(Y, \star) \to \pi_1(X, t_0)$$

qui est injectif et bien défini au regard de la proposition 2.2.14.

Montrons que l'image de f est incluse dans $\ker(\varphi)$. Soit γ un lacet de Y basé en $\star$. Alors $f(\gamma)$ est un lacet de X basé en t_0. De plus, puisque γ est un relèvement de $f(\gamma)$ qui débute au point $\star$, nous avons :

$$\varphi(f(\gamma)).\star = \star[f(\gamma)] = \gamma(1) = \star = 1.\star\,.$$

L'action de G sur la fibre au-dessus de t_0 étant libre, cela entraîne $\varphi(f(\gamma)) = 1$. Donc $\mathrm{Im}(f) \subseteq \ker(\varphi)$.

Considérons à présent un lacet γ' de X basé en t_0 et tel que $\varphi(\gamma') = 1$. Soit γ le chemin dans Y qui relève γ' dans Y et débute au point $\star$, dont l'existence est assurée par la proposition 2.2.14. Nous avons :

$$\gamma(1) = \star[\gamma'] = \varphi(\gamma').\star = 1.\star = \star$$

Ainsi, γ est un lacet basé en $\star$ et la classe d'homotopie de γ' est image par f de celle de γ puisque $p \circ \gamma = \gamma'$.

On a montré que l'image de f est exactement $\ker(\varphi)$. Ainsi, f induit par corestriction l'isomorphisme souhaité $\pi_1(Y, \star) \simeq \ker(\varphi)$. □

Proposition: *Un changement de point marqué correspond à la conjugaison du morphisme de monodromie par un élément de G*

Proposition 2.2.20. *Soit deux G-revêtements marqués $(p, \star_1, \alpha)$ et $(p, \star_2, \alpha)$ d'un même espace topologique pointé (X, t_0), correspondant tous deux au même G-revêtement non-marqué (p, α). Soit $\varphi_1, \varphi_2 : \pi_1(X, t_0) \to G$ leurs morphismes de monodromie respectifs. Alors :*

— *Les morphismes φ_1 et φ_2 sont conjugués par un élément de G.*

— *S'il existe un chemin reliant $\star_1$ et $\star_2$ dans Y, alors les morphismes φ_1 et φ_2 ont la même image H et sont conjugués par un élément de H.*

Démonstration. Pour tout lacet $\gamma \in \pi_1(X, t_0)$, nous avons par définition du morphisme de monodromie :

$$\varphi_1(\gamma).\star_1 = \star_1[\gamma] \qquad \text{et} \qquad \varphi_2(\gamma).\star_2 = \star_2[\gamma].$$

Par transitivité de l'action de G sur la fibre $p^{-1}(t_0)$, il existe un élément $g \in G$ tel que $g.\star_1 = \star_2$. On a alors pour tout lacet $\gamma \in \pi_1(X, t_0)$:

$$g.(\star_1[\gamma]) = (g.\star_1)[\gamma] = \star_2[\gamma] = \varphi_2(\gamma).\star_2 = (\varphi_2(\gamma)g).\star_1$$

ainsi que :

$$g.(\star_1[\gamma]) = g.(\varphi_1(\gamma).\star_1) = (g\varphi_1(\gamma)).\star_1\,.$$

L'action de G sur la fibre étant libre, ces deux égalités entraînent l'égalité $\varphi_2(\gamma)g = g\varphi_1(\gamma)$ dans G et les morphismes φ_1, φ_2 sont bien conjugués par $g \in G$.

Supposons maintenant qu'il existe un chemin γ dans Y reliant $\star_1$ et $\star_2$. Le chemin γ relève le chemin $p \circ \gamma$, débute au point $\star_1$, et aboutit au point $\star_2$. On a donc :

$$\star_2 = \star_1[p \circ \gamma] = \varphi_1(p \circ \gamma).\star_1 .$$

Cela montre que, dans la preuve du premier point, l'élément $g = \varphi_1(p \circ \gamma)$ se trouve dans $\mathrm{Im}(\varphi_1)$. Puisque φ_2 est conjugué au morphisme φ_1 par un élément de son image, les deux morphismes ont la même image. □

Corollaire: *« Morphisme » de monodromie d'un G-revêtement non-marqué (défini à conjugaison près)*

Corollaire 2.2.21. *Si (p, α) est un G-revêtement non-marqué de (X, t_0), on peut lui associer un morphisme de monodromie qui est bien défini à conjugaison par un élément de G près. Autrement dit, les G-revêtements non-marqués donnent lieu à des éléments du quotient $\mathrm{Hom}(\pi_1(X, t_0), G)/\mathrm{Inn}(G)$.*

2.2.4. G-revêtements non-connexes

Dans cette sous-section, on décrit certaines particularités des G-revêtements liées à la prise en compte des revêtements non connexes. Dans la proposition 2.2.23 et la remarque 2.2.24, on montre qu'un G-revêtement marqué non connexe de groupe de monodromie H est formé de $|G| / |H|$ composantes connexes toutes isomorphes, et que la composante connexe du point marqué est un H-revêtement connexe. Finalement, la proposition 2.2.25 décrit le groupe d'automorphismes d'un G-revêtement marqué non-connexe.

Fait: *Décomposition des revêtements galoisiens non-connexes*

Fait 2.2.22. Soit $p : Y \to X$ un revêtement galoisien, avec X connexe. Soit $\widetilde{Y}$ une quelconque des composantes connexes de Y et $\widetilde{p} : \widetilde{Y} \to X$ la restriction de p à $\widetilde{Y}$. Alors $\widetilde{p}$ est un revêtement galoisien connexe, et la restriction de p à une quelconque des composantes connexes de Y est isomorphe à $\widetilde{p}$.

Dorénavant, on suppose X localement connexe par arcs, de sorte que les composantes connexes soient connexes par arcs.

Proposition: *Composantes connexes des G-revêtements non-connexes*

Proposition 2.2.23. *Soit $(p, \star, \alpha)$ un G-revêtement marqué de (X, t_0) et H son groupe de monodromie. Soit $(\widetilde{p}, \star)$ le revêtement connexe marqué obtenu en restreignant p à la composante connexe C du point marqué $\star$. Alors $\widetilde{p}$ est un H-revêtement connexe et $H \simeq \mathrm{Aut}(\widetilde{p})$.*

Démonstration. Soit x un point de X et $F = p^{-1}(x)$ la fibre de p au-dessus du point x. Alors, la fibre $\widetilde{F}$ du revêtement connexe $\widetilde{p}$ au-dessus de x est donnée par $F \cap C = \widetilde{p}^{-1}(x)$.

Le groupe G agit librement sur F. Si $y \in \widetilde{F}$, on demande quels sont les éléments $g \in G$ tels que $g.y \in \widetilde{F}$:

— Si $g.y$ est dans $\widetilde{F}$, il existe un chemin $\widetilde{\gamma}$ dans $\widetilde{Y}$ reliant y à $g.y$. Ce chemin est un relèvement du lacet $\gamma = \widetilde{p} \circ \widetilde{\gamma}$. Alors :

$$g.y = y[\gamma] = \varphi(\gamma).y$$

ce qui entraîne $g = \varphi(\gamma)$ puisque l'action de G est libre. En particulier, g se trouve dans le sous-groupe $H = \mathrm{Im}(\varphi)$.

— Si, réciproquement, g est un élément du sous-groupe $H = \mathrm{Im}(\varphi)$, alors on écrit $g = \varphi(\gamma)$ pour un lacet γ dans X. Soit alors $\widetilde{\gamma}$ le relèvement de γ débutant au point y. On a :
$$g.y = \varphi(\gamma).y = y[\gamma] = \widetilde{\gamma}(1).$$
Les points y et $g.y$ étant reliés par le chemin $\widetilde{\gamma}$, ils se trouvent dans la même composante connexe et donc $g.y \in \widetilde{F}$.

Ainsi, $g.y$ se trouve dans $\widetilde{F}$ si et seulement si $g \in H$. On en déduit que l'action de G sur F se restreint en une action, libre et transitive, de H sur $\widetilde{F}$. Ainsi, $\widetilde{p}$ est un H-revêtement connexe. L'isomorphisme $H \simeq \mathrm{Aut}(\widetilde{p})$ découle de la proposition 2.2.11. □

Remarque: *Égalité entre l'indice du groupe de monodromie d'un G-revêtement et son nombre de composantes connexes*

Remarque 2.2.24. On suppose X connexe. Soit $(p, \star) : (Y, \star) \to (X, t_0)$ un G-revêtement marqué de groupe de monodromie H. La proposition 2.2.23 montre que $(\widetilde{p}, \star)$ est un H-revêtement connexe marqué, et le fait 2.2.22 montre que Y est homéomorphe à l'union disjointe de m copies de C, où m est le nombre de composantes connexes de Y et C est la composante connexe du point marqué $\star$. Si d est le degré de $\widetilde{p}$, alors le degré de p est md. Ainsi :
$$|G| = m\,|H|\,.$$
En particulier, p est connexe si et seulement si $m = 1$, si et seulement si son groupe de monodromie est égal à G, si et seulement si le morphisme de monodromie de p est surjectif.

Proposition: *Groupe des automorphismes d'un G-revêtement non-connexe*

Proposition 2.2.25. *Soit $(p; \star) : (Y, \star) \to (X, t_0)$ un G-revêtement marqué de groupe de monodromie H. On désigne par m l'indice du sous-groupe H dans G. Notons C la composante connexe du point marqué $\star$, et $\widetilde{p} : C \to X$ le H-revêtement connexe marqué correspondant. Alors, le groupe des automorphismes* $\mathrm{Aut}(p)$ *(du revêtement non-marqué) est isomorphe au produit semi-direct $H^m \rtimes \mathfrak{S}_m$:*
$$\mathrm{Aut}(p) \simeq H^m \rtimes \mathfrak{S}_m$$
où $\mathfrak{S}_m$ agit sur H^m par permutation des coordonnées. Il s'agit également du produit en couronne $H \wr \mathfrak{S}_m$.

Démonstration. Notons $C_1, \ldots, C_m$ les composantes connexes de Y, avec $C_1 = C$, et fixons des homéomorphismes $\Phi_i : C_i \xrightarrow{\sim} C$.

Soit $\sigma \in \mathrm{Aut}(p)$ un automorphisme de p. L'automorphisme σ permute les composantes connexes de Y: désignons par $\psi \in \mathfrak{S}_m$ la permutation telle que $\sigma(C_i) = C_{\psi(i)}$. On définit alors :
$$\sigma_i = \Phi_{\psi(i)} \circ \sigma \circ \Phi_i^{-1}$$
qui est l'automorphisme de C obtenu en regardant à l'action de σ sur la composante C_i de manière « interne ». D'après la proposition 2.2.11, les automorphismes $\sigma_i \in \mathrm{Aut}(\widetilde{p})$ correspondent à des éléments h_i du groupe de monodromie H. Cette correspondance donne lieu à une application :
$$f : \sigma \mapsto (h_1, \ldots, h_m, \psi)$$
de $\mathrm{Aut}(p)$ dans l'ensemble $H^m \times \mathfrak{S}_m$. L'automorphisme σ peut être reconstruit à partir du uplet $(h_1, \ldots, h_m, \psi)$ correspondant puisqu'on a, pour $x \in C_i$:
$$\sigma(x) = \Phi_{\psi(i)}^{-1}\left(\alpha(h_i)\left(\Phi_i(x)\right)\right).$$

Cela montre que f est une bijection. Soit alors deux automorphismes $\sigma_1, \sigma_2 \in \mathrm{Aut}(p)$ et $(h_{1,1}, \ldots, h_{1,m}, \psi_1)$, $(h_{2,1}, \ldots, h_{2,m}, \psi_2)$ leurs images par f dans $H^m \times \mathfrak{S}_m$. Décrivons l'action de $\sigma_1\sigma_2$ sur les composantes connexes de Y :

$$(\sigma_1\sigma_2)(C_i) = \sigma_1(\sigma_2(C_i)) = \sigma_1(C_{\psi_2(i)}) = C_{(\psi_1\circ\psi_2)(i)}.$$

À présent, pour un élément $x \in C_i$, on a :

$$\sigma_2(x) = \Phi^{-1}_{\psi_2(i)}\left(\alpha(h_{2,i})\left(\Phi_i(x)\right)\right) \in C_{\psi_2(i)},$$

puis :

$$\begin{aligned}\sigma_1(\sigma_2(x)) &= \Phi^{-1}_{(\psi_1\circ\psi_2)(i)}\left(\alpha(h_{1,\psi_2(i)})\left(\Phi_{\psi_2(i)}\left(\Phi^{-1}_{\psi_2(i)}\left(\alpha(h_{2,i})\left(\Phi_i(x)\right)\right)\right)\right)\right)\\ &= \Phi^{-1}_{(\psi_1\circ\psi_2)(i)}\left(\alpha(h_{1,\psi_2(i)})\left(\alpha(h_{2,i})\left(\Phi_i(x)\right)\right)\right)\\ &= \Phi^{-1}_{(\psi_1\circ\psi_2)(i)}\left(\alpha(h_{1,\psi_2(i)}h_{2,i})\left(\Phi_i(x)\right)\right) \in C_{(\psi_1\circ\psi_2)(i)}.\end{aligned}$$

Il découle de ce calcul que la composition des automorphismes de p correspondant aux uplets :

$$(h_{1,1}, \ldots, h_{1,m}, \psi_1) \text{ et } (h_{2,1}, \ldots, h_{2,m}, \psi_2)$$

est l'automorphisme correspondant au uplet suivant :

$$(h_{1,\psi_2(1)}h_{2,1}, \ldots, h_{1,\psi_2(m)}h_{2,m}, \psi_1 \circ \psi_2)$$

qui est le produit des uplets $(h_{1,1}, \ldots, h_{1,m}, \psi_1)$ et $(h_{2,1}, \ldots, h_{2,m}, \psi_2)$ dans le produit semi-direct $H^m \rtimes \mathfrak{S}_m$. Cela conclut la preuve. □

2.2.5. Les G-revêtements vus comme morphismes

On suppose à présent que (X, t_0) est un espace topologique pointé connexe et satisfaisant les trois propriétés suivantes – toujours satisfaites lorsque X est une variété topologique, et qui garantissent l'existence du revêtement universel (voir la proposition 2.2.27) :

— X est *séparé* ;

— X est *localement connexe par arcs* : tout point $x \in X$ admet un voisinage connexe par arcs. Ainsi, les composantes connexes de X coïncident avec les composantes connexes par arcs ;

— X est *semi-localement simplement connexe* : tout point $x \in X$ admet un voisinage N dont le groupe fondamental $\pi_1(N, x)$ a une image triviale dans $\pi_1(X, x)$ sous le morphisme induit par l'inclusion $N \subseteq X$. Autrement dit, un lacet « suffisamment proche » de x doit être homotopiquement trivial, quitte à utiliser des points « loin de x » pour construire les homotopies.

Le théorème suivant établit une bijection entre les G-revêtements marqués de (X, t_0) et les morphismes de groupes entre le groupe fondamental de (X, t_0) et G.

Théorème 2.2.26. *Pour tout morphisme de groupes $\varphi : \pi_1(X, t_0) \to G$, il existe un G-revêtement marqué de (X, t_0), unique à isomorphisme près, dont φ est le morphisme de monodromie.*

Théorème: *Équivalence entre G-revêtements marqués de (X, t_0) et morphismes $\pi_1(X, t_0) \to G$*

Sans démontrer ce théorème (voir [Sza09, Theorem 2.3.4]), donnons les étapes d'une démonstration possible :

1. D'abord, on construit le revêtement universel de X, qui correspond au morphisme identité $\pi_1(X, t_0) \to \pi_1(X, t_0)$:

   Proposition 2.2.27. *Il existe un $\pi_1(X, t_0)$-revêtement[1] connexe marqué $(\pi, e, \widetilde{\alpha}) : (\widetilde{X}, e) \to (X, t_0)$, avec $\pi : \widetilde{X} \to X$, tel que pour tout revêtement galoisien connexe marqué $(p, \star) : (Y, \star) \to (X, t_0)$, il existe un unique revêtement connexe marqué $(q, e) : (\widetilde{X}, e) \to (Y, \star)$ satisfaisant l'égalité $p \circ q = \pi$. De plus, parmi les revêtements satisfaisant les propriétés ci-dessus, le triplet $(\pi, e, \widetilde{\alpha})$ est unique à isomorphisme de $\pi_1(X, t_0)$-revêtements marqués près.*

   La preuve de cette proposition est classique : on construit un espace des chemins de X qu'on munit de la topologie compact-ouverte, et on montre qu'il satisfait les propriétés annoncées.

2. On démontre le théorème 2.2.26 dans le cas où le morphisme φ est surjectif. Pour construire le G-revêtement marqué souhaité, on quotiente le revêtement universel par le noyau de φ (qui, vu comme sous groupe de $\mathrm{Aut}(\widetilde{X})$, a une action naturelle sur le revêtement universel). L'unicité se montre en utilisant la propriété universelle du revêtement universel.

3. Pour le cas général, on applique le cas précédent à φ vu comme morphisme surjectif dans son image H. On obtient ainsi un H-revêtement connexe marqué. On considère l'union d'autant de copies de ce H-revêtement qu'il y a de classes à gauche de H dans G, et on définit une action de G sur le revêtement obtenu à partir de l'action de G sur les classes à gauche.

Proposition: *Existence et unicité du revêtement universel*

[1] Le groupe fondamental n'étant pas nécessairement fini, on n'est pas dans le cadre des définitions 2.2.1 et 2.2.10, mais les notions s'adaptent naturellement au cas infini.

On dispose d'une version du théorème 2.2.26 pour les G-revêtements non-marqués :

Théorème 2.2.28. *Soit $[\varphi]$ une orbite de morphismes de groupes $\pi_1(X, t_0) \to G$ pour l'action de conjugaison de $\mathrm{Inn}(G)$. Il existe un G-revêtement non-marqué (p, α) de X, unique à isomorphisme près, dont $[\varphi]$ est le « morphisme » de monodromie au sens du corollaire 2.2.21.*

Théorème: *Équivalence entre G-revêtements non-marqués de X et morphismes $\pi_1(X, t_0) \to G$ considérés à conjugaison près*

En vertu des théorèmes 2.2.26 et 2.2.28, nous confondons à partir de ce point les G-revêtements avec les morphismes d'un groupe fondamental dans G (à conjugaison près dans le cas non-marqué). En particulier, les G-revêtements sont considérés à isomorphisme près, le plus souvent de façon implicite. Ce changement de paradigme est essentiel, puisqu'il rend aisées des constructions qu'il est malcommode de définir en termes topologiques. Cela vaut notamment pour l'opération de recollement que nous définissons dans la sous-section 2.4.2.

Remarque 2.2.29. Le théorème 2.2.26 peut être vu comme une propriété universelle du groupe fondamental de X basé en t_0 : c'est un « représentant » du foncteur qui à un groupe fini G associe les classes d'isomorphismes de G-revêtements de X avec un point marqué au-dessus de t_0. Bien sûr, le groupe fondamental n'étant généralement pas fini, il ne s'agit pas d'un vrai représentant du foncteur ; en revanche, le complété profini de $\pi_1(X, t_0)$ est effectivement un pro-représentant du foncteur.

On peut ainsi définir le groupe fondamental, ou au moins son complété profini[2], à partir de cette propriété universelle plutôt qu'à partir de lacets. Cette définition a notamment l'intérêt de ne pas faire référence à l'intervalle $[0, 1]$ ou au cercle unité,

[2] Si on s'autorise à regarder les G-revêtements lorsque G n'est pas fini, on peut caractériser le groupe fondamental ordinaire. Cependant, cela rompt l'analogie avec le groupe fondamental étale.

objets qui n'ont pas d'équivalents dans des contextes algébriques ou arithmétiques : en remplaçant les revêtements par des revêtements étales, ce point de vue conduit à la définition du groupe fondamental étale (voir [Sza09, Definition 4.6.3 & Theorem 4.6.4]).

2.3. Ramification et monodromie locale

Dans cette section, (X, t_0) est une surface pointée[3]. Notamment, tout point de X admet un voisinage homéomorphe à $\mathbb{R}^2$. En pratique, les cas qui nous intéressent sont le plan $\mathbb{R}^2$, c'est-à-dire la droite affine complexe $\mathbb{A}^1(\mathbb{C})$, et la sphère de Riemann, c'est-à-dire la droite projective complexe $\mathbb{P}^1(\mathbb{C})$.

Notre objectif est d'étudier les revêtements ramifiés, que nous introduisons de façon informelle dans la sous-section 2.3.1. Dans les sous-sections suivantes, nous précisons les définitions des configurations de points de X et des G-revêtements ramifiés de X, puis nous étudions certaines propriétés fondamentales des G-revêtements ramifiés.

[3] Par *surface*, on entend « variété topologique connexe de dimension 2 ». Dans le chapitre 7, il est principalement question de revêtements de *courbes* algébriques ; il faut avoir en tête que la situation « fondamentale » est celle des courbes complexes, qui sont de dimension réelle 2.

2.3.1. **Motivations pour l'étude de la ramification**

Au lieu de considérer les G-revêtements de la seule surface X, nous considérons les G-revêtements de versions « trouées » de X. Spécifiquement, les G-revêtements de $X \setminus \underline{t}$, où $\underline{t}$ est un sous-ensemble fini[4] de X dont les points seront les *points de branchement* de nos revêtements. Ces revêtements seront nommés *G-revêtements ramifiés* (ou *branchés*) de la surface X. Le fait de considérer les revêtements ramifiés a un intérêt double :

[4] Plus précisément, une *configuration* telle que définie dans les Définitions 2.3.4 et 2.3.8

— D'abord, dans le cas où X est simplement connexe comme $\mathbb{A}^1(\mathbb{C})$ ou $\mathbb{P}^1(\mathbb{C})$, la théorie des G-revêtements de X est pauvre : puisque le groupe fondamental $\pi_1(X, t_0)$ est trivial, il n'y a qu'un seul morphisme $\pi_1(X, t_0) \to G$, et par suite tous les G-revêtements de X sont triviaux, et isomorphes les uns aux autres. En enlevant des points à X, on fait grossir[5] progressivement son groupe fondamental par l'adjonction de générateurs. La théorie des G-revêtements ramifiés de X est alors d'autant plus riche que le nombre de points de branchement croît.

[5] On voit l'intérêt de supposer que X est une surface : en dimension 1, la suppression d'un nombre fini de points ne préserve même pas nécessairement la connexité ; en dimension 3 et plus, elle n'affecte pas le groupe fondamental.

— Ensuite et surtout, l'étude des revêtements ramifiés permet d'observer des phénomènes intéressants lorsque les points de branchement se déplacent sur la surface X – typiquement, on peut déformer un G-revêtement continûment. Cette idée centrale mène à la définition des espaces de Hurwitz et de leurs composantes.

Géométriquement, on voit les points de branchement comme des points de X en lesquels on autorise les feuillets du G-revêtement à s'intersecter. En particulier, au-dessus d'un point $t_i \in \underline{t}$, il y a généralement strictement moins de $|G|$ points distincts dans la fibre, puisque certains d'entre eux appartiennent à plusieurs des $|G|$ feuillets qui existent localement autour de t_i. On en donne une illustration schématique :

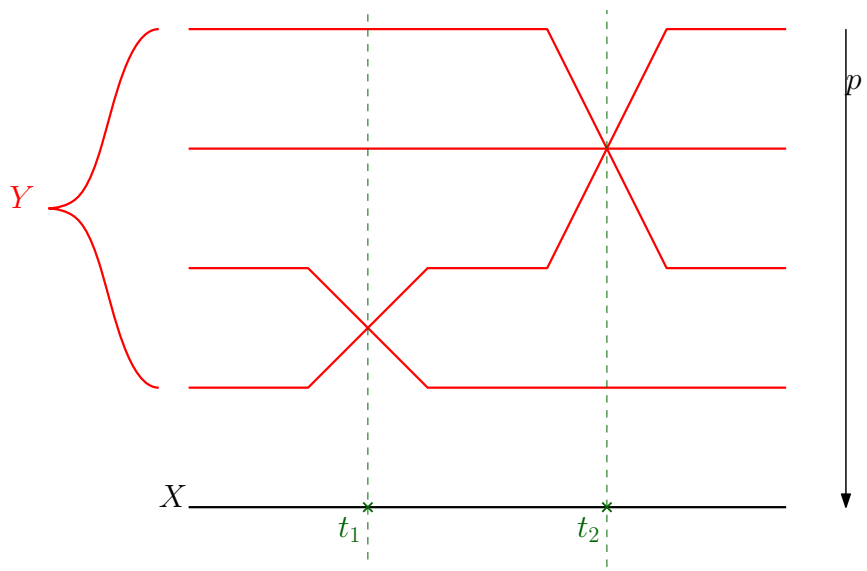


Figure 2.3.1. Illustration d'un revêtement de degré 4, ramifié en deux points t_1 et t_2.

Une autre façon de considérer un revêtement de degré d est de le voir comme une forme de fonction multivaluée : les d points de la fibre au-dessus d'un point x sont les d « images » de x, et on demande à ce que sur un voisinage assez petit d'un point x (non ramifié) cette fonction multivaluée soit donnée par d fonctions continues. Dans ce cas, un point de branchement est un point en lequel ces d fonctions continues n'ont pas des valeurs distinctes : le point a donc strictement moins de d images.

Exemple 2.3.2. L'exemple typique d'un revêtement ramifié est donné par l'application suivante :

$$f_n : \begin{cases} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & z^n \end{cases}.$$

Dans la fibre au-dessus de chaque nombre complexe non nul, il y a n points, qui sont ses racines n-ièmes, et au-dessus de chaque ouvert simplement connexe U de $\mathbb{C} \setminus \{0\}$, on construit un homéomorphisme $f_n^{-1}(U) \simeq U \times \{1, \dots, n\}$ à l'aide d'une détermination de la racine n-ième complexe. Cependant, les n feuillets s'intersectent au point de branchement 0.

Décrivons le morphisme de monodromie dans cette situation. Le groupe fondamental $\pi_1(\mathbb{C} \setminus \{0\}, 1)$ est engendré par la classe d'homotopie du lacet unité $\gamma : t \in [0,1] \mapsto \exp(2i\pi t)$, et le relèvement de ce lacet en un chemin débutant en $\exp\left(2i\pi\frac{k}{n}\right)$ est le chemin :

$$t \in [0,1] \mapsto \exp\left(2i\pi\frac{k+t}{n}\right)$$

dont le point d'arrivée est $\exp\left(2i\pi\frac{k+1}{n}\right)$. Cela montre que $f_n|_{\mathbb{C}\setminus\{0\}}$ est un $\mathbb{Z}/n\mathbb{Z}$-revêtement connexe, dont le morphisme de monodromie est :

$$\varphi_n : \begin{cases} \pi_1(\mathbb{C} \setminus \{0\}, 1) & \to & \mathbb{Z}/n\mathbb{Z} \\ \gamma & \mapsto & 1 \end{cases}.$$

En termes de fonctions multivaluées, le revêtement f_n correspond à la fonction multivaluée qui à un nombre complexe associe ses n racines n-ièmes, qui sont effectivement distinctes en général. Cependant, cette fonction est univaluée en 0 puisque 0 n'a qu'une seule racine n-ième.

Exemple: *Construction de revêtements à partir de polynômes*

Exemple 2.3.3. On considère un polynôme $P(x,t)$ en deux variables à coefficients complexes, de degré d en t. Cette situation généralise l'exemple 2.3.2 qui correspond au polynôme $t^d - x$.

Soit V le lieu d'annulation de P dans $\mathbb{C}^2$, $p : V \to \mathbb{C}$ l'application de projection sur la première coordonnée. En un point $x^* \in \mathbb{A}^1(\mathbb{C})$ suffisamment général, la spécialisation $P(x^*,t)$ est un polynôme de degré d dont les d racines sont distinctes, et alors $p^{-1}(x^*)$ est fini de cardinal d. Il est donc tentant de définir un revêtement de degré d de $\mathbb{A}^1(\mathbb{C})$ à partir de p. Cependant, il y a deux types de situations dans lesquelles $P(x^*,t)$ aura moins de d racines distinctes :

— **Le polynôme $P(x^*,t)$ est de degré $< d$:**

Soit $P_d(x)$ le « coefficient de tête » de $P(x,t)$ devant t^d, qui est un polynôme non nul. Son lieu d'annulation, qui est un ensemble fini de points de $\mathbb{C}$, correspond aux points $x^* \in \mathbb{C}$ en lesquels la spécialisation $P(x^*,t)$ est de degré strictement inférieur à d.

— **Le polynôme $P(x^*,t)$ est de degré d mais a des racines doubles :**

Soit x^* un nombre complexe n'annulant pas P_d. Alors la spécialisation $P(x^*,t)$ est un polynôme en t de degré d, dont le discriminant est un nombre complexe qui dépend polynomialement de x^*. On note $\mathrm{Disc}_t(P)$ le polynôme en x correspondant. Son lieu d'annulation, qui est un ensemble fini de points de $\mathbb{A}^1(\mathbb{C})$, correspond aux points x^* en lesquels $P(x^*,t)$ a des racines multiples.

En dehors de l'ensemble fini $\underline{t}$ de ces points problématiques, l'application p définit effectivement un revêtement de degré d. Autrement dit, p définit un revêtement de $\mathbb{A}^1(\mathbb{C})$ ramifié en $\underline{t}$.

Cet exemple est généralisé par les $\mathbb{C}$-G-revêtements algébriques que nous définirons dans la section 7.1. Le théorème d'existence de Riemann, dont nous parlons dans la sous-section 7.1.4, a alors un sens très concret : tout revêtement ramifié de $\mathbb{P}^1(\mathbb{C})$ (de degré fini) est algébrique, c'est-à-dire isomorphe à un revêtement défini par des polynômes à coefficients complexes. La question de savoir si un revêtement ramifié de $\mathbb{P}^1(\mathbb{C})$ est défini sur un corps $K \subseteq \mathbb{C}$, que nous définissons plus soigneusement dans la sous-section 7.1.5, correspond à la question naturelle suivante : peut-on choisir ces polynômes à coefficients dans le corps K ?

2.3.2. Configurations et groupe des tresses

Dans cette sous-section, on définit les espaces de configurations de n points de $X \setminus \{t_0\}$ et les groupes de tresses $\mathrm{B}_{n,X}$, qui sont leurs groupes fondamentaux.

Définition: *Configuration ordonnée, l'espace* $\mathrm{PConf}_{n,X}$ *des configurations ordonnées de n points de* $X \setminus \{t_0\}$

Définition 2.3.4. Une *configuration ordonnée* de n points est un n-uplet de points distincts de $X \setminus \{t_0\}$. L'*espace des configurations ordonnées de n points* $\mathrm{PConf}_{n,X}$ est l'espace topologique dont les points sont les configurations ordonnées de n points, muni de la topologie de sous-espace héritée de celle de X^n.

Une première propriété importante de l'espace $\mathrm{PConf}_{n,X}$ est la suivante :

Proposition 2.3.5. *L'espace* $\mathrm{PConf}_{n,X}$ *est connexe.*

Proposition: *Connexité de* $\mathrm{PConf}_{n,X}$

Démonstration. Considérons deux configurations ordonnées $\underline{t} = (t_0, \ldots, t_n)$ et $\underline{t}' = (t'_0, \ldots, t'_n)$.

Si on a une égalité du type $t'_i = t_j$, on choisit un voisinage connexe N de t'_i tel que $N \cap \{t_0, \ldots, t_n, t'_0, \ldots, t'_n\} = \{t'_i\}$. On prend un point quelconque $\widetilde{t}_j \in N \setminus \{t'_i\}$, puis un chemin dans N reliant t_j et $\widetilde{t}_j$. On peut utiliser ce chemin pour relier $\underline{t} = (t_0, \ldots, t_n)$ et $(t_0, \ldots, t_{j-1}, \widetilde{t}_j, t_{j+1}, \ldots, t_n)$. En répétant cette opération pour chaque égalité de la forme $t'_i = t_j$, on se ramène à la situation où $t_i \neq t'_j$ pour tous i et j. On se place désormais dans cette situation.

L'espace $X \setminus \{t_1, \ldots, t_n, t'_1, \ldots, t'_n\}$ est connexe par arcs puisque X est une variété topologique connexe de dimension 2. On peut donc trouver des chemins γ_i reliant t_i et t'_i et évitant tous les points t_j et t'_j pour $j \neq i$. En concaténant successivement les chemins obtenus en appliquant le chemin γ_i à la i-ième coordonnée de $\underline{t}$, on obtient un chemin dans $\mathrm{PConf}_{n,X}$ qui relie $\underline{t}$ et $\underline{t}'$. □

Remarque 2.3.6. Tout point $\underline{t} \in \mathrm{PConf}_{n,X}$ admet un voisinage ouvert homéomorphe à $\mathbb{R}^{2n}$, obtenu comme produit cartésien de voisinages ouverts disjoints, chacun homéomorphe à $\mathbb{R}^2$, des points t_i. En particulier, $\mathrm{PConf}_{n,X}$ est une variété topologique de dimension $2n$.

Définition 2.3.7. Si $\underline{t} = (t_1, \ldots, t_n) \in \mathrm{PConf}_{n,X}$ est une configuration ordonnée de points de X, et si $\psi \in \mathfrak{S}_n$ est une permutation, on note :

Définition: *Action du groupe symétrique sur les configurations ordonnées*

$$\psi.\underline{t} \stackrel{\text{def}}{=} (t_{\psi(1)}, t_{\psi(2)}, \ldots, t_{\psi(n)}) \in \mathrm{PConf}_{n,X}.$$

Cette formule définit une action libre et continue du groupe symétrique $\mathfrak{S}_n$ sur l'espace topologique $\mathrm{PConf}_{n,X}$. L'orbite d'une configuration ordonnée $\underline{t}$ sous cette action est notée $[\underline{t}]$.

Définition 2.3.8. Une *configuration de n points* est l'orbite sous l'action du groupe symétrique $\mathfrak{S}_n$ d'une configuration ordonnée de n points. L'*espace des configurations de n points* $\mathrm{Conf}_{n,X}$ est l'espace topologique quotient :

Définition: *Configuration (non-ordonnée), l'espace* $\mathrm{Conf}_{n,X}$ *des configurations de n*

$$\mathrm{Conf}_{n,X} \stackrel{\text{def}}{=} \mathrm{PConf}_{n,X}/\mathfrak{S}_n.$$

Une *configuration* est implicitement non-ordonnée. Comme quotient d'une variété topologique de dimension $2n$ par l'action libre et continue d'un groupe fini, l'espace $\mathrm{Conf}_{n,X}$ est une variété topologique de dimension $2n$.

Fait 2.3.9. L'application $\pi : \mathrm{PConf}_{n,X} \to \mathrm{Conf}_{n,X}$ qui à une configuration ordonnée $\underline{t}$ associe sa $\mathfrak{S}_n$-orbite $[\underline{t}]$ définit un $\mathfrak{S}_n$-revêtement connexe de $\mathrm{Conf}_{n,X}$.

Fait: $\mathrm{PConf}_{n,X}$ *est un* $\mathfrak{S}_n$*-revêtement de* $\mathrm{Conf}_{n,X}$

À présent, on fixe une configuration ordonnée $\underline{t} \in \mathrm{PConf}_{n,X}$, dont on se sert comme d'un point base dans l'espace des configurations ordonnées. Souvent, cette « configuration-base » est implicite.

Définition 2.3.10. Le *n-ième groupe des tresses pures* de X (basé en $\underline{t}$) est le groupe fondamental :

Définition: *Groupe des tresses (pures) de X*

$$\mathrm{PB}_{n,X} \stackrel{\text{def}}{=} \pi_1(\mathrm{PConf}_{n,X}, \underline{t}).$$

et le *n-ième groupe des tresses* (basé en $[\underline{t}]$) est :

$$\mathrm{B}_{n,X} \stackrel{\text{def}}{=} \pi_1(\mathrm{Conf}_{n,X}, [\underline{t}]).$$

On nomme *tresse* (resp. *tresse pure*) les éléments de $\mathrm{B}_{n,X}$ (resp. $\mathrm{PB}_{n,X}$).

Une tresse $\sigma \in \mathrm{B}_{n,X}$ est une collection de n chemins paramétrés, qui à chaque instant prennent des valeurs distinctes (il n'y a donc pas de collision), et qui retrouvent finalement les positions de départ en ayant possiblement échangé leurs places.

Remarque 2.3.11. Les groupes des tresses (pures) $(\mathrm{P})\mathrm{B}_{n,X}$ de la définition 2.3.10 ne sont pas les groupes des tresses (pures) à n brins dans X, mais ce sont les groupes des tresses (pures) à n brins dans $X \setminus \{t_0\}$. Plutôt que de faire ce choix, on aurait aussi pu permettre au point base de se déplacer, en en faisant un point particulier des configurations. On retrouverait alors le groupe des tresses pures de X au sens usuel. Cependant, dans ce modèle, les espaces de configuration non-ordonnés sont de la forme $(X^{n+1} \setminus \Delta)/\mathfrak{S}_n$ où $\mathfrak{S}_n$ agit par permutation sur les coordonnées $2, \dots, n+1$: le groupe fondamental correspondant est le groupe des tresses à $n+1$ brins fixant un des points, qui est isomorphe au groupe $\mathrm{B}_{n,X}$ défini plus haut

Fait:
Suite exacte reliant $\mathrm{B}_{n,X}$ *et* $\mathrm{PB}_{n,X}$

Fait 2.3.12. Le $\mathfrak{S}_n$-revêtement connexe $\pi : \mathrm{PConf}_{n,X} \to \mathrm{Conf}_{n,X}$ du fait 2.3.9, qu'on marque en la configuration ordonnée $\underline{t}$, possède un morphisme de monodromie surjectif $\pi^* : \mathrm{B}_{n,X} \twoheadrightarrow \mathfrak{S}_n$. Ce morphisme décrit la façon dont un lacet basé en $[\underline{t}]$ dans l'espace des configurations non-ordonnées change l'ordre des points de $\underline{t}$ quand on le relève dans PConf_n. Son noyau correspond aux lacets dans $\mathrm{Conf}_{n,X}$ qui, une fois relevés, ramènent la configuration $\underline{t}$ à elle-même sans changer l'ordre de ses points, c'est-à-dire les lacets de $\mathrm{PConf}_{n,X}$ basés en $\underline{t}$. Cela montre que $\ker(\pi^*) \simeq \mathrm{PB}_{n,X}$. Nous avons donc la suite exacte suivante :

$$1 \to \mathrm{PB}_{n,X} \to \mathrm{B}_{n,X} \to \mathfrak{S}_n \to 1.$$

Ces observations sont un cas particulier de la proposition 2.2.19.

2.3.3. **Revêtements ramifiés**

Commençons par une définition générale des revêtements ramifiés, qu'on peut décliner pour divers types de revêtements :

Définition:
Revêtements ramifiés

Définition 2.3.13. Soit $\underline{t} \in \mathrm{Conf}_{n,X}$ une configuration. Un *revêtement ramifié en* $\underline{t}$ est un revêtement de $X \setminus \underline{t}$. On appelle alors les points de $\underline{t}$ les *points de branchement* du revêtement.

Cette définition s'applique à tous types de revêtements : revêtements marqués, G-revêtements, etc., mais on n'écrit pas la définition dans chacun des cas. On donne cependant des définitions précises dans deux situations importantes :

Définition:
G-revêtement marqué de (X, t_0), ramifié en une configuration ordonnée

Définition 2.3.14. Un *G-revêtement marqué de (X, t_0) avec des points de branchement ordonnés* est un couple $(\underline{t}, \varphi)$ où $\underline{t} \in \mathrm{PConf}_{n,X}$ est une configuration ordonnée et φ est un morphisme de groupes $\pi_1(X \setminus \underline{t}, t_0) \to G$.

Définition: *G-revêtement ramifié marqué de* (X, t_0)

Définition 2.3.15. Un *G-revêtement ramifié marqué de* (X, t_0) est un couple $(\underline{t}, \varphi)$ où $\underline{t} \in \mathrm{Conf}_{n,X}$ est une configuration (non-ordonnée), et φ est un morphisme de groupes $\pi_1(X \setminus \underline{t}, t_0) \to G$.

On ne donne pas toutes les variantes possibles de ces définitions. Par exemple, pour les G-revêtements ramifiés non-marqués, on considère le morphisme $\varphi : \pi_1(X \setminus \underline{t}, t_0) \to G$ à conjugaison par un élément de G près.

Remarque 2.3.16. Les G-revêtements ramifiés en une configuration $\underline{t}$, tels qu'on les a définis dans les définitions 2.3.13,2.3.14 et 2.3.15, pourraient plus précisément s'appeler *revêtements ramifiés, non-ramifiés hors de la configuration* $\underline{t}$. En effet, on n'impose pas aux revêtements de ne pas s'étendre en des revêtements avec moins de points de branchement : il n'y a pas forcément de « vraie » ramification. Avec notre définition, il est tout à fait possible qu'au-dessus d'un point « de branchement » t_i de $\underline{t}$, le nombre de points de la fibre soit égal au degré du G-revêtement. On fait ce choix afin d'obtenir des définitions parcimonieuses[6] et une structure algébrique plus simple dans la sous-section 3.4.1. La proposition 2.3.26 donne une condition nécessaire et suffisante pour déterminer si un G-revêtement est effectivement ramifié en un point de la configuration $\underline{t}$ ou si, au contraire, il s'agit d'un point de branchement *factice* au sens de la définition 2.3.27.

[6] En termes de morphismes de monodromie, l'hypothèse de non-extension des G-revêtements s'écrit ainsi : si $\underline{t} \in \mathrm{Conf}_n(X)$, il faut se restreindre aux morphismes $\varphi : \pi_1(X \setminus \underline{t}, t_0) \to G$ qui ne se factorisent par aucun $\pi_1(X \setminus \underline{t}', t_0)$ pour $\underline{t}' \in \mathrm{Conf}_m(X)$ avec $m < n$.
En termes de la description combinatoire des G-revêtements qu'on verra dans la sous-section 2.3.6, il faut remplacer les n-uplets d'éléments de G par des n-uplets d'éléments de $G \setminus \{1\}$ (voir la proposition 2.3.26).

2.3.4. **Bouquets topologiques**

Dans cette sous-section, on définit les *bouquets topologiques* (Définition 2.3.19). Pour une référence, on peut consulter [DE06, Paragraph 1.1]. On suppose la surface X orientée, et on considère une configuration ordonnée $\underline{t} = (t_1, \dots, t_n) \in \mathrm{PConf}_{n,X}$. On note D le disque unité ouvert de $\mathbb{R}^2$ et $\overline{D}$ le disque unité fermé.

On décrit une construction qu'on utilise pour énoncer la définition 2.3.19. Soit $(V_i, \Phi_i)_{i=0,\dots,n}$ une famille telle que :

— les ensembles V_i sont des fermés disjoints de X ;

— l'application Φ_i est un homéomorphisme *positivement orienté* entre V_i et le disque fermé $\overline{D}$, et tel que l'image de l'intérieur de V_i par Φ_i soit égale au disque ouvert D ;

— pour tout $i \in \{0, \dots, n\}$, le point t_i appartient au fermé V_i, et est égal à $\Phi_i^{-1}(0,0)$.

On définit alors les points et chemins suivants, pour $i \in \{1, \dots, n\}$:

— $S_i \in X$ est le point suivant de ∂V_0 :

$$S_i = \Phi_0^{-1}\left(\cos\left(\frac{2\pi i}{n}\right), \sin\left(\frac{2\pi i}{n}\right)\right) ;$$

— σ_i est le chemin suivant dans V_0, qui va de t_0 à S_i en « ligne droite » :

$$\sigma_i : t \in [0,1] \mapsto \Phi_0^{-1}\left(t\cos\left(\frac{2\pi i}{n}\right), t\sin\left(\frac{2\pi i}{n}\right)\right) ;$$

— T_i est le point suivant de ∂V_i:

$$T_i = \Phi_i^{-1}(1,0) ;$$

— τ_i est le lacet suivant dans V_i, basé en T_i, et qui fait le tour du point t_i une unique fois dans le sens inverse des aiguilles d'une montre :

$$\tau_i : t \in [0,1] \mapsto \Phi_i^{-1}\left(\cos(t), \sin(t)\right).$$

On résume ces définitions par un dessin :

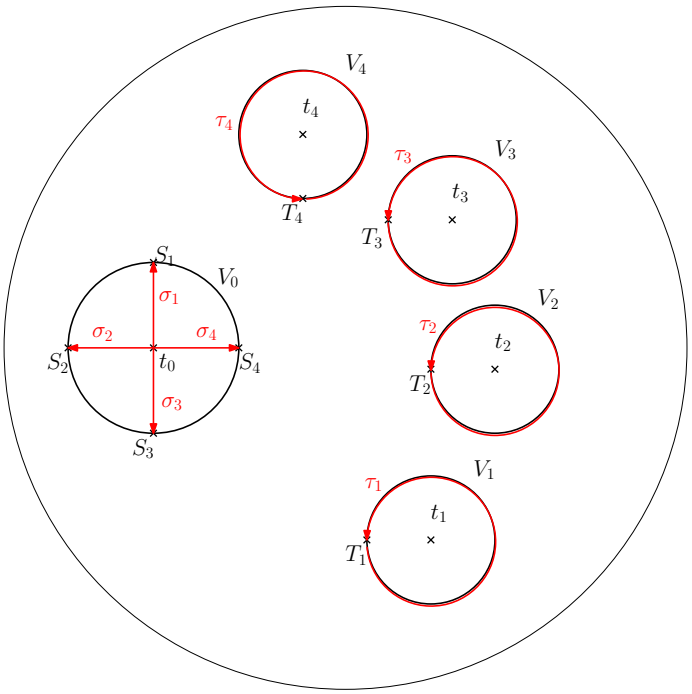


Figure 2.3.17.
Une illustration de la construction quand $n = 4$. (1/2)

On considère à présent des chemins $p_1, \dots, p_n$ tels que :

— le chemin p_i part de S_i et arrive à T_i ;

— excepté en son point final T_i qui se trouve sur le bord de V_i, la trajectoire du chemin p_i est entièrement contenue dans $X \setminus (V_1 \sqcup V_2 \sqcup \dots \sqcup V_n)$;

— les trajectoires des chemins $p_1, \dots, p_n$ n'ont pas d'auto-intersections (la fonction p_i est injective), et ne se croisent pas deux-à-deux (les images de p_i et p_j sont disjointes pour $i \neq j$).

On complète le dessin avec ces chemins :

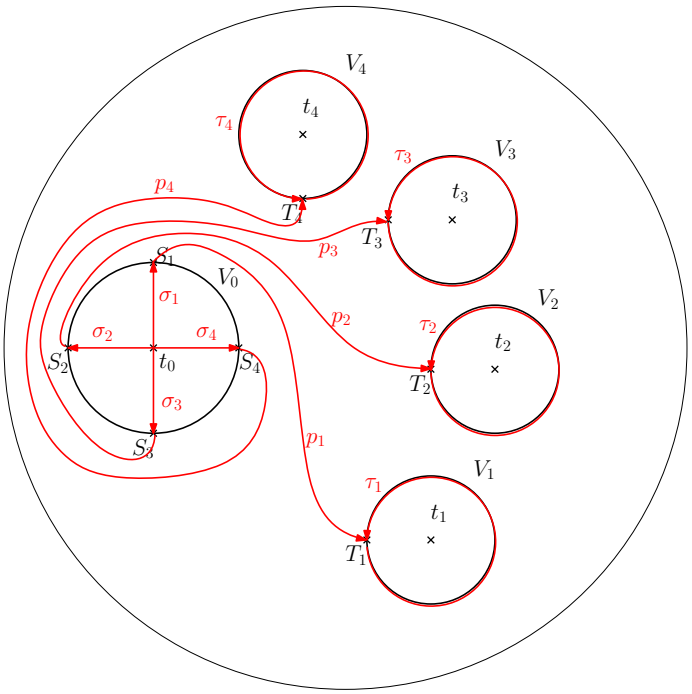


Figure 2.3.18.
Une illustration de la construction quand $n = 4$. (2/2)

On définit alors, pour tout $i = 1, 2, \ldots, n$, le lacet basé en t_0 suivant :

$$\gamma_i = \sigma_i * p_i * \tau_i * p_i^{-1} * \sigma_i^{-1}.$$

Définition: *Bouquet topologique*

Définition 2.3.19. Un *bouquet topologique* associé à la configuration ordonnée $\underline{t} \in \mathrm{PConf}_{n,X}$ est une liste ordonnée de n éléments de $\pi_1(X \setminus \underline{t}, t_0)$:

$$([\gamma_1], [\gamma_2], \ldots, [\gamma_n])$$

telle que, pour un certain choix de fermés $(V_i)_{i\in\{0,\ldots,n\}}$, d'homéomorphismes $(\Phi_i)_{i\in\{0,\ldots,n\}}$ et de chemins $(p_i)_{i\in\{1,\ldots,n\}}$ comme ci-dessus, les éléments $[\gamma_i]$ sont les classes d'homotopie des lacets $\gamma_1, \ldots, \gamma_n$ obtenus par la construction précédente.

Définition: *Bouquet topologique associé à une configuration non-ordonnée*

Définition 2.3.20. Si $\underline{t} \in \mathrm{Conf}_n$ est une configuration (non-ordonnée), un *bouquet topologique associé à* $\underline{t}$ est une liste non-ordonnée $\underline{\gamma}$ d'éléments de $\pi_1(X \setminus \underline{t}, t_0)$ telle qu'il existe une configuration ordonnée $\widetilde{\underline{t}} \in \mathrm{PConf}_{n,X}$ dont $\underline{t}$ soit la $\mathfrak{S}_n$-orbite, et un bouquet topologique $\widetilde{\underline{\gamma}}$ associé à $\widetilde{\underline{t}}$ dont $\underline{\gamma}$ soit la $\mathfrak{S}_n$-orbite.

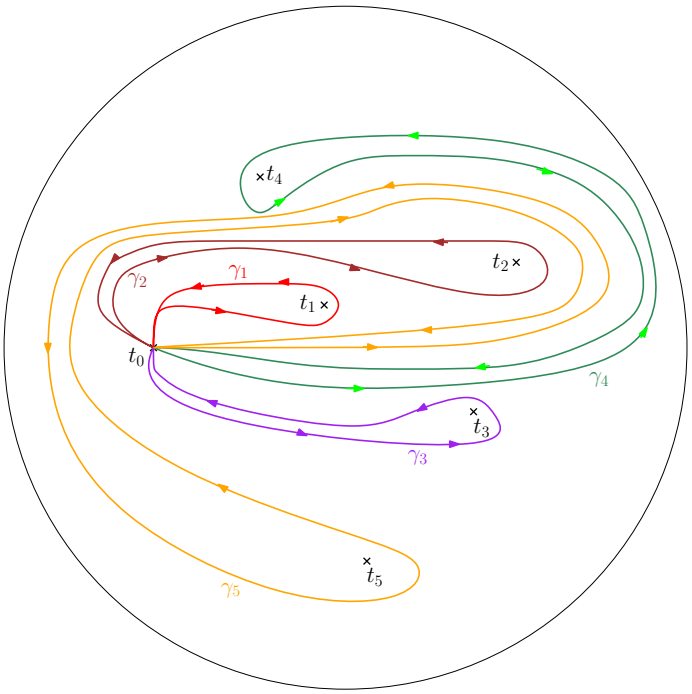


Figure 2.3.21. Un exemple de bouquet dans le cas $n = 5$, où on a déformé les lacets γ_i de sorte qu'ils ne s'auto-intersectent pas.

Les deux points à retenir de la définition sont les suivants :

— le lacet γ_i fait exactement une fois le tour du point t_i, dans le sens inverse des aiguilles d'une montre, et il ne tourne pas autour des autres points[7] ;

— autour du point base t_0, les lacets γ_i apparaissent « dans l'ordre ». Autrement dit, si on fait le tour du point t_0 dans le sens inverse des aiguilles d'une montre, on croise d'abord le lacet γ_1, puis γ_2, puis γ_3, etc.

[7] Cela a un sens précis : le lacet devient homotopiquement trivial quand on le regarde dans $X \setminus \{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n\}$.

Proposition: *Toute configuration admet un bouquet*

Proposition 2.3.22. *Pour toute configuration ordonnée $\underline{t} \in \mathrm{PConf}_{n,X}$, il existe un bouquet associé à $\underline{t}$.*

Démonstration (esquissée). On choisit (V_i, Φ_i) comme ci-dessus arbitrairement. On reprend les notations de la construction qui précède la définition 2.3.20. Montrons qu'il existe des chemins $p_1, \dots, p_n$ de S_i à T_i, injectifs, de trajectoires disjointes, et qui évitent les fermés V_i. On peut construire un tel chemin p_1 car $X \setminus \bigsqcup V_i$ est connexe par arcs, puis on peut construire p_2 car $X \setminus (\bigsqcup \mathrm{Im}(p_1) \sqcup V_i)$ est homotopiquement équivalent à X privé de n points et donc connexe par arcs, puis on peut construire p_3 car $X \setminus (\mathrm{Im}(p_1) \sqcup \mathrm{Im}(p_2) \sqcup \bigsqcup V_i)$ est homotopiquement équivalent à X privé de $n-1$ points qui est connexe par arcs, et ainsi de suite. □

Proposition: *Tous les bouquets sont conjugués (lacet par lacet)*

Proposition 2.3.23. *Si $(\gamma_{i,1})$ et $(\gamma_{i,2})$ sont deux bouquets associés à la configuration ordonnée $\underline{t}$, alors il existe des éléments $g_i \in \pi_1(X \setminus \underline{t}, t_0)$ tels que :*

$$\gamma_{i,1} = g_i \, \gamma_{i,2} \, g_i^{-1}.$$

Démonstration. Soit deux bouquets $(\gamma_{i,1})$ et $(\gamma_{i,2})$, et soit $i \in \{1, \dots, n\}$. Par définition, il existe des voisinages fermés $V_{i,1}, V_{i,2}$ de t_i homéomorphes au disque fermé $\overline{D}$, des points $T_{i,1} \in V_{i,1}$ et $T_{i,2} \in V_{i,2}$, des lacets $\tau_{i,1}, \tau_{i,2}$ dans $V_{i,1} \setminus \{t_i\}$ (resp. $V_{i,2} \setminus \{t_i\}$) basés en $T_{i,1}$ (resp. $T_{i,2}$) et qui font le tour de t_i une fois dans le sens direct, et des chemins $q_{i,1}$ (resp. $q_{i,2}$) reliant t_0 à $T_{i,1}$ (resp. $T_{i,2}$) obtenus en concaténant σ_i et p_i, satisfaisant :

$$\gamma_{i,1} = \left[q_{i,1} * \tau_{i,1} * (q_{i,1})^{-1} \right] \quad \text{et} \quad \gamma_{i,2} = \left[q_{i,2} * \tau_{i,2} * (q_{i,2})^{-1} \right].$$

Soit $V_{i,3}$ un voisinage fermé de t_i homéomorphe à $\overline{D}$ via un homéomorphisme positivement orienté, et inclus dans l'intersection $V_{i,1} \cap V_{i,2}$. Soit $T_{i,3}$ un point de $\partial V_{i,3}$, et un lacet $\tau_{i,3}$ basé en $T_{i,3}$ qui tourne une fois autour de t_i dans le sens antihoraire (voir la construction de la définition 2.3.19).

Soit deux chemins w_1 et w_2 dans $V_{i,1}$ (resp. $V_{i,2}$), reliant le point $T_{i,1}$ (resp. $T_{i,2}$) au point $T_{i,3}$, et qui évitent t_i. Le lacet $w_1 * \tau_{i,3} * w_1^{-1}$ est un lacet de $V_{i,1}$ basé en $T_{i,1}$, qui tourne une fois dans le sens antihoraire autour de t_i. Puisque $V_{i,1} \setminus \{t_i\}$ est homotopiquement équivalent au cercle de groupe fondamental $\mathbb{Z}$, son groupe fondamental n'a qu'un seul générateur positivement orienté. On a donc les homotopies suivantes :

$$w_1 * \tau_{i,3} * w_1^{-1} \simeq \tau_{i,1}, \qquad \text{et de même :} \qquad w_2 * \tau_{i,3} * w_2^{-1} \simeq \tau_{i,2}.$$

Finalement :

$$\begin{aligned}
\gamma_{i,1} &= \left[q_{i,1} * \tau_{i,1} * (q_{i,1})^{-1} \right] \\
&= \left[q_{i,1} * w_1 * \tau_{i,3} * w_1^{-1} * (q_{i,1})^{-1} \right] \\
&= \left[q_{i,1} * w_1 * w_2^{-1} * \tau_{i,2} * w_2 * w_1^{-1} * (q_{i,1})^{-1} \right] \\
&= \left[q_{i,1} * w_1 * w_2^{-1} * (q_{i,2})^{-1} \right] \gamma_{i,2} \left[q_{i,2} * w_2 * w_1^{-1} * (q_{i,1})^{-1} \right] \\
&= \underbrace{\left[q_{i,1} * w_1 * w_2^{-1} * (q_{i,2})^{-1} \right]}_{\in \pi_1(X \setminus \underline{t}, t_0)} \gamma_{i,2} \left[q_{i,1} * w_1 * w_2^{-1} * (q_{i,2})^{-1} \right]^{-1}.
\end{aligned}$$

Cela conclut la preuve. □

La proposition 2.3.23 a le corollaire suivant :

Corollaire 2.3.24. *Soit un G-revêtement marqué de (X, t_0) ramifié en $\underline{t} \in \mathrm{PConf}_{n,X}$. Soit $\varphi : \pi_1(X \setminus \underline{t}, t_0) \to G$ son morphisme de monodromie et $H = \mathrm{Im}(\varphi)$ son groupe de monodromie. Alors la classe de conjugaison dans H de l'élément $\varphi(\gamma_i)$ est indépendante du choix d'un bouquet $(\gamma_i)_{i\in\{1,\dots,n\}}$ associé à $\underline{t}$.*

Démonstration. Si $(\gamma_{i,1})_i$ et $(\gamma_{i,2})_i$ sont deux bouquets, alors les lacets $\gamma_{i,1}$ et $\gamma_{i,2}$ sont conjugués d'après la proposition 2.3.23, et leurs images par φ sont donc conjuguées par un élément de H. □

2.3.5. **Classes de monodromie**

Dans cette sous-section, on introduit la notion de classe de monodromie d'un G-revêtement marqué en un de ses points de branchement :

Définition 2.3.25. La *classe de monodromie en t_i* d'un G-revêtement marqué de (X, t_0) ramifié en une configuration $\underline{t}$ contenant t_i est la classe de conjugaison, dans le groupe de monodromie, de l'élément $\varphi(\gamma_i)$ pour un bouquet $\underline{\gamma}$ quelconque associé à $\underline{t}$. Cette classe de conjugaison est bien définie d'après le corollaire 2.3.24.

Définition:
Classe de monodromie d'un G-revêtement ramifié marqué en un de ses points de branchement

La classe de monodromie d'un G-revêtement non-marqué en un de ses points de branchement t_i, vue comme classe de conjugaison de G, est également bien définie.

Proposition 2.3.26. *Soit $\underline{t} \in \mathrm{PConf}_{n,X}$ une configuration ordonnée et un bouquet topologique $(\gamma_i)_{i\in\{1,\dots,n\}}$ qui lui soit associé. Soit $(p, \star, \alpha)$ un G-revêtement marqué de $X \setminus \underline{t}$, et $\varphi : \pi_1(X \setminus \underline{t}, t_0) \to G$ son morphisme de monodromie. Alors $\varphi(\gamma_i) = 1$ si et seulement si le G-revêtement marqué $(p, \star)$ s'étend en un G-revêtement marqué de $X \setminus \{t_1, \dots, t_{i-1}, t_{i+1}, \dots, t_n\}$.*

Proposition:
Les « vrais » points de branchement sont ceux en lesquels la classe de monodromie est non-triviale

Démonstration.

($\Leftarrow$) Supposons que le G-revêtement marqué $(p, \star, \alpha)$ s'étende en un G-revêtement marqué $(p', \star, \alpha')$ de $X \setminus \{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n\}$. On désigne par φ' le morphisme de monodromie du revêtement étendu :

$$\varphi' : \pi_1(X \setminus \{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n\}, t_0) \to G.$$

Soit i l'inclusion $(X \setminus \underline{t}, t_0) \to (X \setminus \{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n\}, t_0)$. Puisqu'il est équivalent de relever un chemin dans $X \setminus \underline{t}$ par p ou par p', on a :

$$\varphi = \varphi' \circ \pi_1(i).$$

Remarquons que le lacet γ_i est homotopiquement trivial lorsqu'on le regarde dans $X \setminus \{t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n\}$ puisque le lacet τ_i utilisé dans la définition des bouquets topologiques l'est. Ainsi, on a $\pi_1(i)(\gamma_i) = 1$ et par conséquent $\varphi(\gamma_i) = \varphi'(\pi_1(i)(\gamma_i)) = 1$.

($\Rightarrow$) Supposons désormais que $\varphi(\gamma_i) = 1$. On choisit un ouvert U de X homéomorphe à $\mathbb{R}^2$, contenant les points t_0 et t_i ainsi que la trajectoire du lacet γ_i, mais aucun des autres points $t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n$. L'ouvert $U \setminus \{t_i\}$ est homéomorphe au plan épointé, et il a donc un groupe fondamental isomorphe à $\mathbb{Z}$, engendré par la classe d'homotopie de γ_i. La restriction $p|_{U\setminus\{t_i\}}$ du revêtement p à $U \setminus \{t_i\}$ satisfait toujours l'hypothèse, à savoir que l'image de γ_i par son morphisme de monodromie est triviale. Puisque γ_i engendre $\pi_1(U \setminus \{t_i\}, t_0)$, cela entraîne que le morphisme de monodromie de $p|_{U\setminus\{t_i\}}$ est trivial. D'après le théorème 2.2.26, la trivialité du morphisme de monodromie entraîne la trivialité du revêtement $p|_{U\setminus\{t_i\}}$. Le revêtement trivial s'étendant bien entendu à U, c'est le cas de $p|_{U\setminus\{t_i\}}$ et, par conséquent, de p.

□

Définition: *Point de branchement factice*

Définition 2.3.27. Un point de branchement t_i d'un G-revêtement ramifié est *factice* si le revêtement s'étend en un G-revêtement ramifié dont t_i n'est plus un point de branchement.

D'après la proposition 2.3.26, les points de branchements factices sont exactement ceux en lesquels la classe de monodromie est triviale.

2.3.6. **Description des cycles de branchement et multidiscriminant**

Soit $(p, \star)$ un G-revêtement marqué de (X, t_0) ramifié en une configuration ordonnée $\underline{t} \in \mathrm{PConf}_{n,X}$. Fixons un bouquet topologique $\underline{\gamma} = (\gamma_1, \ldots, \gamma_n)$ associé à $\underline{t}$. On définit un n-uplet d'éléments de G à partir du G-revêtement $(p, \star)$:

Définition: *Description des cycles de branchement d'un G-revêtement marqué*

Définition 2.3.28. La *description des cycles de branchement* (*branch cycle description* en anglais) du G-revêtement marqué $(p, \star)$ pour le bouquet $\underline{\gamma}$ est le n-uplet suivant d'éléments de G :

$$\mathrm{BCD}_{\underline{\gamma}}(p, \star) = (\varphi(\gamma_1), \ldots, \varphi(\gamma_n))$$

où φ est le morphisme de monodromie du G-revêtement marqué $(p, \star)$. Les éléments de ce n-uplet sont les *éléments locaux de monodromie* du revêtement $(p, \star)$ pour le bouquet $\underline{\gamma}$.

Lorsque les éléments $\gamma_1, \ldots, \gamma_n$ engendrent le groupe fondamental $\pi_1(X \setminus \underline{t}, t_0)$, la description des cycles de branchement d'un G-revêtement marqué caractérise entièrement son morphisme de monodromie, et donc (d'après le théorème 2.2.26) sa classe d'isomorphisme. Ce n'est en général pas le cas (si X n'est pas simplement connexe, le cas $n = 0$ donne un contre-exemple), mais la proposition 2.4.12 assure que cette propriété est vérifiée dans le cas des droites complexes $\mathbb{A}^1(\mathbb{C})$ et $\mathbb{P}^1(\mathbb{C})$.

Soit H un sous-groupe de G contenant le groupe de monodromie de $(p, \star)$, et soit c un sous-ensemble de H invariant par conjugaison et contenant toutes les classes de monodromie de $(p, \star)$. On note D^* l'ensemble des classes de conjugaison de H contenues dans c.

Définition: *(H, c)-multidiscriminant d'un G-revêtement marqué*

Définition 2.3.29. Le (H, c)-*multidiscriminant* $\mu_{H,c}(p, \star)$ du G-revêtement marqué $(p, \star)$ est l'application $D^* \to \{0, 1, \ldots\}$ qui à une classe de conjugaison $\gamma \in D^*$ associe le nombre de points de $\underline{t}$ en lesquels la classe de monodromie de $(p, \star)$ est γ.

Le (H, c)-multidiscriminant vérifie l'égalité suivante :

$$\sum_{\gamma \in D^*} \mu_{H,c}(p, \star)(\gamma) = n.$$

Par la définition 2.3.25, la classe de monodromie associée au point de branchement t_i est la classe de conjugaison du i-ième élément local de monodromie du G-revêtement $(p, \star)$, quel que soit le bouquet $\underline{\gamma}$. On peut ainsi déterminer le (H, c)-multidiscriminant du G-revêtement marqué $(p, \star)$ à partir de la description de ses cycles de branchement :

$$\mu_{H,c}(p, \star) = \mu_{H,c}(\mathrm{BCD}_{\underline{\gamma}}(p, \star))$$

où le (H, c)-multidiscriminant du n-uplet $\mathrm{BCD}_{\underline{\gamma}}(p, \star)$ est pris au sens de la définition 1.4.6.

Par ailleurs, si φ est le morphisme de monodromie de $(p, \star)$, alors le groupe de monodromie de $(p, \star)$ satisfait l'inclusion suivante :

$$\mathrm{Im}(\varphi) = \varphi(\pi_1(X \setminus \underline{t}, t_0)) \supseteq \varphi(\langle \gamma_1, \ldots, \gamma_n \rangle) = \left\langle \mathrm{BCD}_{\underline{\gamma}}(p, \star) \right\rangle$$

avec égalité lorsque le bouquet $\gamma_1, \ldots, \gamma_n$ engendre $\pi_1(X \setminus \underline{t}, t_0)$.

2.4. Description combinatoire des revêtements

Dans cette section, on se concentre sur la situation où X est la droite complexe affine $\mathbb{A}^1(\mathbb{C})$ ou projective $\mathbb{P}^1(\mathbb{C})$. Nous mettons l'accent sur la description combinatoire des G-revêtements ramifiés dans ce contexte (Théorème 2.4.14). On utilise cette description pour définir une opération de recollement des G-revêtements ramifiés marqués (Sous-section 2.4.2).

2.4.1. Le cas des droites complexes

2.4.1.1. Le groupe des tresses. Dans ce paragraphe, on donne une présentation du groupe des tresses $\mathrm{B}_{n,X}$ lorsque $X = \mathbb{A}^1(\mathbb{C})$ ou $X = \mathbb{P}^1(\mathbb{C})$. On commence pour cela par définir le groupe des tresses d'Artin B_n, qui est le « vrai » groupe des tresses à n brins dans $\mathbb{A}^1(\mathbb{C})$ (voir la remarque 2.3.11) :

Définition: *Groupes des tresses d'Artin*

Définition 2.4.1. Le *groupe des tresses d'Artin* B_n est le groupe défini par la présentation suivante :

$$B_n = \left\langle \sigma_1, \sigma_2, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{lcll} \sigma_i\sigma_j & = & \sigma_j\sigma_i & \text{si } |i-j|>2 \\ \sigma_i\sigma_{i+1}\sigma_i & = & \sigma_{i+1}\sigma_i\sigma_{i+1} & \text{si } i<n-1 \end{array} \right\rangle.$$

Le générateur σ_i du groupe des tresses d'Artin correspond à la i-ième tresse élémentaire :

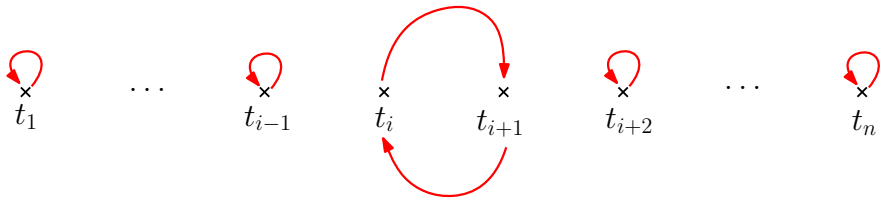


Figure 2.4.2. La i-ième tresse élémentaire.

On représente aussi cette tresse de la façon suivante :

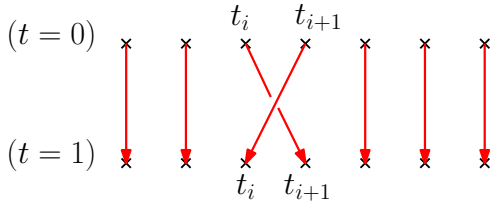


Figure 2.4.3. Une autre représentation de la i-ième tresse élémentaire.

Sur la figure 2.4.3, l'axe vertical représente le temps (de haut en bas) et la « profondeur » (incarnée par le fait qu'un brin de la tresse passe « devant » un autre lors d'un croisement) correspond à l'axe vertical de la figure 2.4.2 – il faut imaginer qu'on assiste au déplacement des points en regardant depuis le bas de la feuille :

En utilisant cette convention, on représente graphiquement les relations qui définissent B_n :

— La *relation de localité* :

$$\sigma_i\sigma_j = \sigma_j\sigma_i \text{ lorsque } |i-j|>1,$$

signifie que les tresses élémentaires qui ne sont pas consécutives commutent les unes avec les autres :

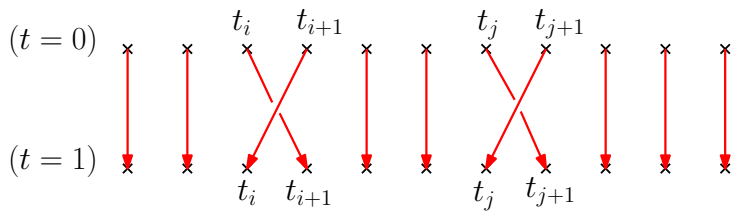


Figure 2.4.4. Une tresse équivalente à la fois à $\sigma_i\sigma_j$ et à $\sigma_j\sigma_i$.

— La *relation de tresse* :

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \text{ pour tout } i \in \{1, \ldots, n-2\}$$

s'illustre similairement :

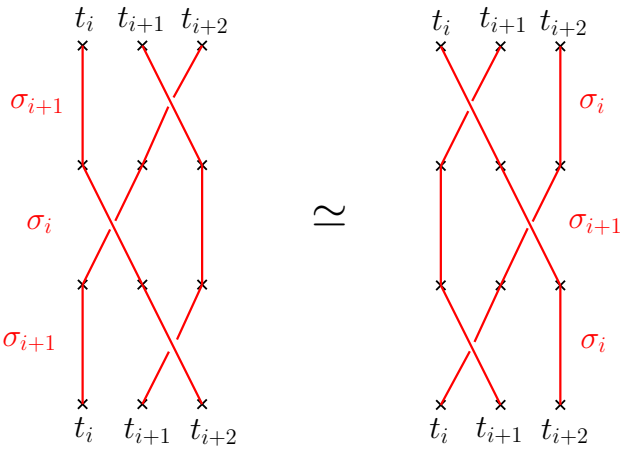


Figure 2.4.5.
Les tresses $\sigma_{i+1}\sigma_i\sigma_{i+1}$ et $\sigma_i\sigma_{i+1}\sigma_i$ respectivement.

Le fait que les deux tresses de la figure 2.4.5 soient équivalentes se voit de la manière suivante : dans les deux cas, le brin reliant t_{i+2} à t_i passe en-dessous des deux autres ; parmi les deux du dessus, le brin reliant t_{i+1} à lui-même passe en-dessous de celui reliant t_i à t_{i+2}.

Proposition:
Une autre présentation du groupe des tresses d'Artin

Proposition 2.4.6. *Le groupe des tresses d'Artin* B_n *est engendré par deux tresses : la tresse élémentaire* σ_1 *et la tresse de « décalage »* (shift *en anglais):*

$$\mathrm{sh} = \sigma_1\sigma_2\cdots\sigma_{n-1}.$$

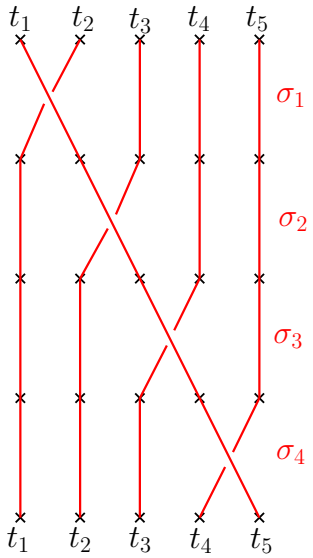


Figure 2.4.7.
La tresse sh dans le cas $n = 5$.

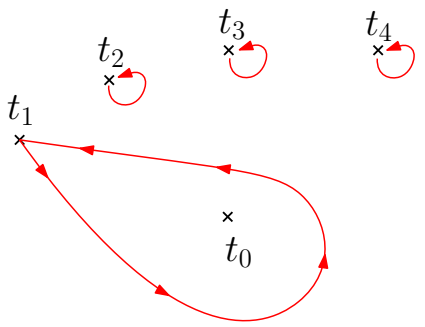
Démonstration. Il suffit d'exprimer σ_i en fonction de σ_1 et de sh. Pour $i \in \{1, \ldots, n-2\}$:

$$\begin{aligned}
\mathrm{sh}\,\sigma_i &= (\sigma_1\sigma_2\ldots\sigma_{n-1})\,\sigma_i \\
&= \sigma_1\sigma_2\ldots\sigma_{i-1}\,(\sigma_i\sigma_{i+1}\sigma_i)\,\sigma_{i+2}\sigma_{i+3}\ldots\sigma_{n-1} \\
&= \sigma_1\sigma_2\ldots\sigma_{i-1}\,(\sigma_{i+1}\sigma_i\sigma_{i+1})\,\sigma_{i+2}\sigma_{i+3}\ldots\sigma_{n-1} \\
&= \sigma_{i+1}\,(\sigma_0\sigma_1\ldots\sigma_{i-1}\sigma_i\sigma_{i+1}\sigma_{i+2}\sigma_{i+3}\ldots\sigma_{n-1}) \\
&= \sigma_{i+1}\,\mathrm{sh}.
\end{aligned}$$

On en déduit $\sigma_{i+1} = \mathrm{sh}^i \sigma_1 \mathrm{sh}^{-i}$, ce qui conclut la preuve. □

Enfin, on décrit les groupes des tresses $B_{n,X}$ (au sens de la définition 2.3.10) lorsque $X = \mathbb{A}^1(\mathbb{C})$ ou $X = \mathbb{P}^1(\mathbb{C})$. Pour une preuve de la proposition 2.4.8, voir les cas $p = 1$ (pour $X = \mathbb{P}^1(\mathbb{C})$) et $p = 2$ (pour $X = \mathbb{A}^1(\mathbb{C})$) de [Belo3, Theorem 5.1].

Proposition 2.4.8. *Le groupe des tresses* $\mathrm{B}_{n,\mathbb{P}^1(\mathbb{C})}$ *est isomorphe au groupe des tresses d'Artin*[8] B_n. *Le groupe des tresses* $\mathrm{B}_{n,\mathbb{A}^1(\mathbb{C})}$, *quant à lui, possède (en plus des tresses élémentaires* $\sigma_1, \dots, \sigma_{n-1}$*) un générateur additionnel* z_1, *correspondant à la rotation dans le sens antihoraire du point* t_1 *autour du point base* t_0 *:*



Ce générateur satisfait les relations suivantes qui – prises avec les relations définissant B_n *– entraînent toutes les relations entre éléments de* $\mathrm{B}_{n,\mathbb{A}^1(\mathbb{C})}$ *:*

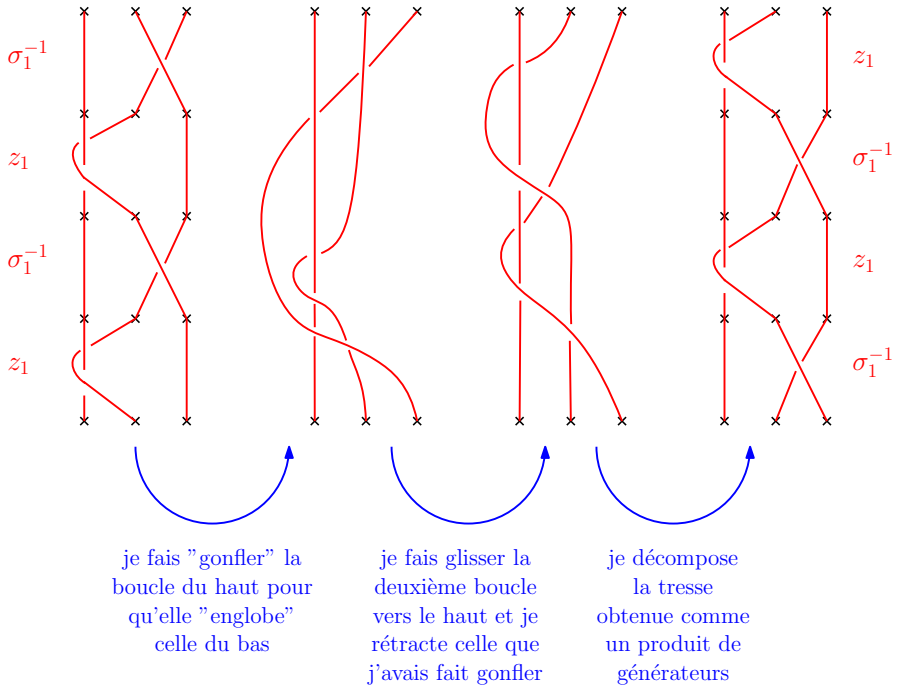
— *Le générateur* z_1 *commute avec les tresses élémentaires* $\sigma_2, \dots, \sigma_{n-1}$ *(toutes exceptée* σ_1*) :*

$$z_1\sigma_i = \sigma_i z_1 \text{ pour tout } i \in \{2, \dots, n-1\}.$$

— *On a :*

$$\sigma_1^{-1} z_1 \sigma_1^{-1} z_1 = z_1 \sigma_1^{-1} z_1 \sigma_1^{-1}.$$

On représente cette relation graphiquement :



Proposition: *Groupe des tresses dans le cas* $\mathbb{A}^1(\mathbb{C})$ *ou* $\mathbb{P}^1(\mathbb{C})$

[8] On peut s'étonner de ne pas retrouver le groupe des tresses « sphériques », qui est le « vrai » groupe des tresses à n brins de $\mathbb{P}^1(\mathbb{C})$, et qui satisfait la relation additionnelle :

$$\sigma_1\sigma_2 \dots \sigma_{n-1}^2 \sigma_{n-2} \dots \sigma_1 = 1.$$

Cependant, cela s'éclaire à la lumière de la remarque 2.3.11 : puisque le point base est fixé, il est normal qu'on retrouve le groupe des tresses d'Artin.

Figure 2.4.9. La générateur additionnel z_1

Figure 2.4.10. Une illustration de la relation $\sigma_1^{-1} z_1 \sigma_1^{-1} z_1 = z_1 \sigma_1^{-1} z_1 \sigma_1^{-1}$

L'espace de configurations $\mathrm{Conf}_{n,X}$ est connexe (voir la proposition 2.3.5) et son groupe fondamental est $\mathrm{B}_{n,X}$ (Définition 2.3.10). Le fait suivant prolonge la description du type d'homotopie de $\mathrm{Conf}_{n,X}$:

Fait: *L'espace de configurations est un espace classifiant du groupe des tresses*

Fait 2.4.11. Les groupes d'homotopie π_k des espaces de configurations $\mathrm{Conf}_{n,X}$ sont triviaux pour $k \geq 2$ [FN62a ; FN62b ; Wil19]. En conséquence, l'espace $\mathrm{Conf}_{n,X}$ est faiblement homotopiquement équivalent à l'espace d'Eilenberg-Maclane $K(\mathrm{B}_{n,X}, 1) = B\mathrm{B}_{n,X}$.

2.4.1.2. Bouquets, groupe fondamental de $X \setminus \underline{t}$, et description des cycles de branchement Dans le cas des droites complexes, le groupe fondamental de $X \setminus \underline{t}$ est engendré par un bouquet associé à $\underline{t}$. Plus précisément :

Proposition: *Générateurs et relations du groupe fondamental $\pi_1(X \setminus \underline{t}, t_0)$*

Proposition 2.4.12. *Soit $\underline{\gamma} = (\gamma_1, \ldots, \gamma_n)$ un bouquet topologique associé à la configuration $\underline{t}$. Alors :*

— *Si $X = \mathbb{A}^1(\mathbb{C})$, les lacets γ_i engendrent $\pi_1(X \setminus \underline{t}, t_0)$ librement.*

— *Si $X = \mathbb{P}^1(\mathbb{C})$, les lacets γ_i engendrent $\pi_1(X \setminus \underline{t}, t_0)$ et satisfont la relation :*

$$\gamma_1 \gamma_2 \cdots \gamma_n = 1$$

qui engendre toutes les autres relations.

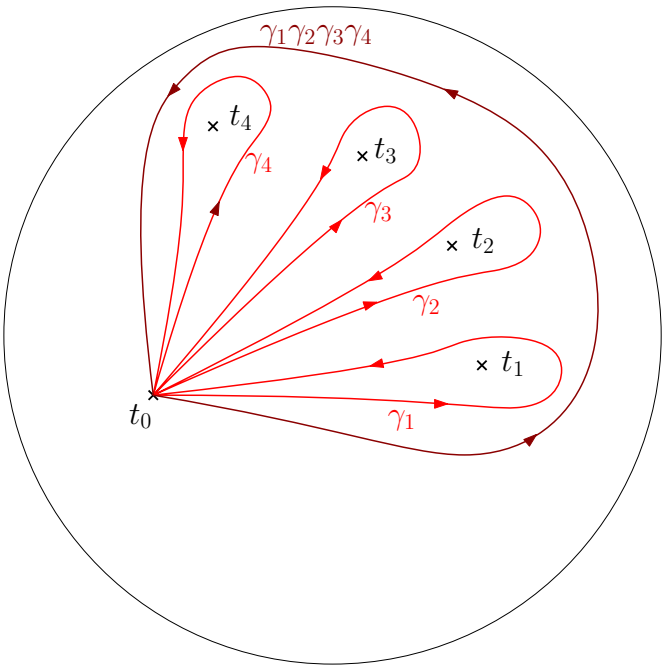


Figure 2.4.13. Le lacet $\gamma_1\gamma_2\cdots\gamma_n$ dans le cas $n = 4$. Lorsque $X = \mathbb{P}^1(\mathbb{C})$, puisqu'on est sur une sphère, on peut contracter ce lacet en passant « derrière la sphère », là où il n'y a pas de points de $\underline{t}$. Cela illustre la relation $\gamma_1\gamma_2\cdots\gamma_n = 1$.

Il suit de la proposition 2.4.12 que, les éléments $\gamma_1, \ldots, \gamma_n$ engendrant $\pi_1(X \setminus \underline{t}, t_0)$, le morphisme de monodromie φ d'un G-revêtement marqué (et, donc, le G-revêtement marqué à isomorphisme près) est entièrement déterminé par ses éléments locaux de monodromie $\varphi(\gamma_i) \in G$, et donc par la description des cycles de branchement (Définition 2.3.28) du G-revêtement marqué. Ainsi :

Théorème: *Description combinatoire des G-revêtements*

Théorème 2.4.14. *Soit $\underline{t} \in \mathrm{PConf}_{n,X}$ une configuration ordonnée et $\underline{\gamma} = (\gamma_1, \ldots, \gamma_n)$ un bouquet topologique associé à $\underline{t}$.*

— *Si $X = \mathbb{A}^1(\mathbb{C})$, l'application $\mathrm{BCD}_{\underline{\gamma}}$ définit une bijection entre les classes d'isomorphismes de G-revêtements marqués de $\mathbb{A}^1(\mathbb{C})$ ramifiés en $\underline{t}$ et les n-uplets $(g_1, \ldots, g_n)$ d'éléments de G.*

— *Si $X = \mathbb{P}^1(\mathbb{C})$, l'application $\mathrm{BCD}_{\underline{\gamma}}$ définit une bijection entre les classes d'isomorphismes de G-revêtements marqués de $\mathbb{P}^1(\mathbb{C})$ ramifiés en $\underline{t}$ et les n-uplets $(g_1, \ldots, g_n)$ d'éléments de G satisfaisant $g_1 g_2 \cdots g_n = 1$.*

Dans les deux cas, le groupe de monodromie d'un G-revêtement marqué ramifié en n points est égal au sous-groupe de G engendré par les éléments $g_1, \ldots, g_n$ du n-uplet correspondant.

En particulier, les classes d'isomorphisme de G-revêtements connexes marqués ramifiés en $\underline{t}$ sont en bijection avec les n-uplets $\underline{g}$ d'éléments de G dont le groupe engendré $\left\langle \underline{g} \right\rangle$ est G tout entier, avec de plus la condition $\pi\underline{g} = 1$ dans le cas $X = \mathbb{P}^1(\mathbb{C})$.

Remarque 2.4.15. Pour les classes d'isomorphisme de G-revêtements non-marqués, le théorème 2.4.14 reste vrai en remplaçant les n-uplets d'éléments de G par des n-uplets considérés à conjugaison (simultanée de tous leurs éléments) près.

Remarque 2.4.16. Un G-revêtement marqué de $\mathbb{A}^1(\mathbb{C})$ ramifié en une configuration $\underline{t} \in \mathrm{Conf}_{n,\mathbb{A}^1(\mathbb{C})}$ s'étend en un G-revêtement ramifié marqué de $\mathbb{P}^1(\mathbb{C})$ si et seulement si son morphisme de monodromie φ satisfait :

$$\varphi(\gamma_1 \gamma_2 \cdots \gamma_n) = 1.$$

pour un bouquet $\underline{\gamma} = (\gamma_1, \ldots, \gamma_n)$ quelconque associé à $\underline{t}$. En effet, un regard attentif au lacet de la figure 2.4.13 dans le cas $X = \mathbb{A}^1(\mathbb{C}) = \mathbb{P}^1(\mathbb{C}) \setminus \{\infty\}$ montre que la classe de conjugaison de $\varphi\left((\gamma_1 \cdots \gamma_n)^{-1}\right)$ est la classe de monodromie en l'infini. On applique alors la proposition 2.3.26.

Une conséquence du théorème 2.4.14 est le corollaire 2.4.17. Ce résultat entraîne que tout groupe fini est isomorphe au groupe des automorphismes d'un revêtement galoisien de $\mathbb{A}^1(\mathbb{C})$ ou de $\mathbb{P}^1(\mathbb{C})$; ce fait acquiert une importance nouvelle à la lumière du théorème d'existence de Riemann (voir la sous-section 7.1.4).

Corollaire 2.4.17. *Il existe un G-revêtement connexe de X.*

Démonstration. En vertu du théorème 2.4.14, il suffit de construire un uplet $\underline{g}$ d'éléments de G qui engendre G, et tel que $\pi\underline{g} = 1$ dans le cas où $X = \mathbb{P}^1(\mathbb{C})$. On peut par exemple prendre n'importe quelle énumération $g_1, \ldots, g_{|G|}$ des éléments de G. Le $|G| + 1$-uplet suivant convient alors :

$$\left(g_1, \ldots, g_{|G|}, \left(g_1 \cdots g_{|G|}\right)^{-1}\right).$$

□

Dans la suite du texte, on ne considère que des G-revêtements ramifiés de la droite, affine ou projective. En vertu du théorème 2.4.14, on assimile donc régulièrement les G-revêtements marqués en une configuration $\underline{t}$ fixée (pour laquelle un bouquet est implicitement choisi) et les n-uplets d'éléments de G, avec la condition que ces uplets soient de produit 1 dans le cas des revêtements de la droite projective.

2.4.2. L'opération de recollement

2.4.2.1. Définition combinatoire de l'opération de recollement. Soit deux entiers n et n', et deux configurations ordonnées $\underline{t} \in \mathrm{PConf}_{n,X}$ et $\underline{t}' \in \mathrm{PConf}_{n',X}$. On suppose que l'ensemble des points de la configuration $\underline{t}$ et l'ensemble des points de la configuration $\underline{t}'$ sont disjoints, de sorte que la concaténation des deux configurations, qu'on note $\underline{t} \cup \underline{t}'$, appartienne à $\mathrm{PConf}_{n+n',X}$. On fixe un bouquet $\underline{\gamma} \cdot \underline{\gamma'} = (\gamma_1, \dots, \gamma_n, \gamma'_1, \dots, \gamma'_n)$ associé à la configuration $\underline{t} \cup \underline{t}'$, obtenu comme concaténation de deux bouquets $\underline{\gamma}$, resp. $\underline{\gamma'}$, associés aux configurations $\underline{t}$, resp. $\underline{t}'$.

Définition: *Recollement de deux G-revêtements marqués*

Définition 2.4.18. Soit deux G-revêtements marqués $(p, \star)$ et $(p', \star')$ de (X, t_0) ramifiés respectivement en $\underline{t}$ et en $\underline{t}'$. Le *recollement* de $(p, \star)$ et $(p', \star')$ est le G-revêtement marqué de (X, t_0) ramifié en $\underline{t} \cup \underline{t}'$, unique à isomorphisme près, dont la description des cycles de branchement pour le bouquet $\underline{\gamma} \cdot \underline{\gamma'}$ est la concaténation (au sens de la définition 1.4.7) des descriptions des cycles de branchement $\mathrm{BCD}_{\underline{\gamma}}(p, \star)$ et $\mathrm{BCD}_{\underline{\gamma'}}(p', \star')$.

Le fait que ce recollement existe et soit unique à isomorphisme près est une conséquence du théorème 2.4.14. Il faut aussi remarquer qu'une concaténation de uplets $(g_1, \dots, g_n)$ et $(g'_1, \dots, g'_{n'})$ vérifiant $g_1 \cdots g_n = g'_1 \cdots g'_{n'} = 1$ est un uplet $(g_1, \dots, g_n, g'_1, \dots, g'_{n'})$ vérifiant $g_1 \cdots g_n g'_1 \cdots g'_{n'} = 1$: cela assure que le recollement est bien défini dans le cas de $\mathbb{P}^1(\mathbb{C})$.

Proposition: *Groupe de monodromie d'un recollement de revêtements*

Proposition 2.4.19. *Si H, H' sont les groupes de monodromie respectifs de $(p, \star)$ et $(p', \star')$, le groupe de monodromie de leur recollement est le sous-groupe $\langle H, H' \rangle$ de G engendré par H et H'*

2.4.2.2. Interprétation géométrique de l'opération de recollement. Réinterprétons la construction précédente d'une façon géométrique, en l'illustrant.

— **Cas $X = \mathbb{A}^1(\mathbb{C})$:** Fixons un ouvert $U \subseteq X$ homéomorphe à $\mathbb{R}^2$ qui contient t_0 et $t_1, \dots, t_n$ et qui ne contient pas $t'_1, \dots, t'_{n'}$, et un ouvert $V \subseteq X$ homéomorphe à $\mathbb{R}^2$ qui contient t_0 et $t'_1, \dots, t'_{n'}$ et qui ne contient pas $t_1, \dots, t_n$, et tels que l'intersection $U \cap V$ soit un voisinage de t_0 homéomorphe à $\mathbb{R}^2$.

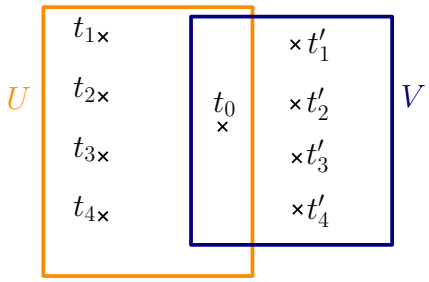


Figure 2.4.20.
Les ouverts U et V

On définit aussi $U' = U \setminus \underline{t}$ et $V' = V \setminus \underline{t}'$. On a alors les homéomorphismes suivants :

$$\begin{array}{ll} (U', t_0) \simeq (\mathbb{A}^1(\mathbb{C}) \setminus \underline{t}, t_0) & (V', t_0) \simeq (\mathbb{A}^1(\mathbb{C}) \setminus \underline{t}', t_0) \\ (U' \cup V', t_0) \simeq (\mathbb{A}^1(\mathbb{C}) \setminus (\underline{t} \cup \underline{t}'), t_0) & (U' \cap V', t_0) \simeq (\mathbb{A}^1(\mathbb{C}), t_0) \end{array}$$

En appliquant le théorème de van Kampen, on obtient un isomorphisme de groupes :

$$\begin{aligned} \pi_1(\mathbb{A}^1(\mathbb{C}) \setminus (\underline{t} \cup \underline{t}'), t_0) &\simeq \pi_1(U' \cup V', t_0) \\ &\simeq \pi_1(U', t_0) \underset{\pi_1(U' \cap V', t_0)}{*} \pi_1(V', t_0) \\ &\simeq \pi_1(\mathbb{A}^1(\mathbb{C}) \setminus \underline{t}, t_0) * \pi_1(\mathbb{A}^1(\mathbb{C}) \setminus \underline{t}', t_0). \end{aligned}$$

La propriété universelle des produits libres entraîne que la donnée d'un morphisme $\pi_1(\mathbb{A}^1(\mathbb{C}) \setminus \underline{t}) \to G$ et d'un morphisme $\pi_1(\mathbb{A}^1(\mathbb{C}) \setminus \underline{t}', t_0) \to G$ est équivalente à la donnée d'un morphisme $\pi_1(\mathbb{A}^1(\mathbb{C}) \setminus (\underline{t} \cup \underline{t}'), t_0)$. En voyant ces morphismes comme les morphismes de monodromie de G-revêtements marqués, on retrouve l'opération de recollement.

— **Cas $X = \mathbb{P}^1(\mathbb{C})$:** Plaçons-nous dans la situation suivante : à gauche, nous avons une sphère privée de n de ses points $\underline{t}$, tandis qu'à droite, nous avons une sphère privée de n' de ses points $\underline{t}'$. De chacune de ces sphères, on retire un petit disque centré en le point base qui ne contient aucun des points que nous avons retirés. On recolle alors les deux sphères en utilisant un cylindre $S^1 \times [0,1]$, ayant pour bord l'union des deux cercles obtenus comme bords des disques qu'on a enlevés. Enfin, on place un nouveau point base t_0 quelque part sur le cylindre. Nous obtenons ainsi un nouvel espace, homéomorphe à une sphère pointée privée de $n + n'$ de ses points $\underline{t} \cup \underline{t}'$.

On considère alors un ouvert U de l'espace construit qui contient la sphère de gauche et le cylindre mais qui ne contient pas la sphère de droite, ainsi qu'un ouvert V qui contient la sphère de droite et le cylindre mais pas la sphère de gauche.

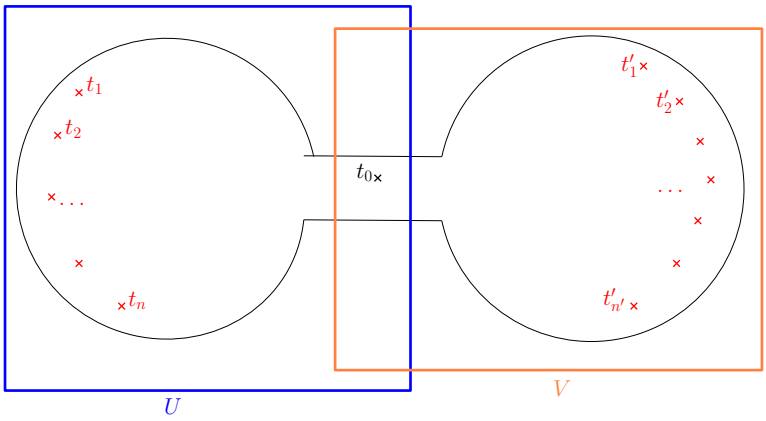


Figure 2.4.21.
Les ouverts U et V.

Décrivons désormais le type d'homotopie des différents ouverts obtenus :

– L'ouvert U est homotopiquement équivalent à une sphère privée de $n+1$ de ses points : d'un part, les n points de la configuration $\underline{t}$, et un point additionnel t_∞ qui correspond au bord droit du cylindre.

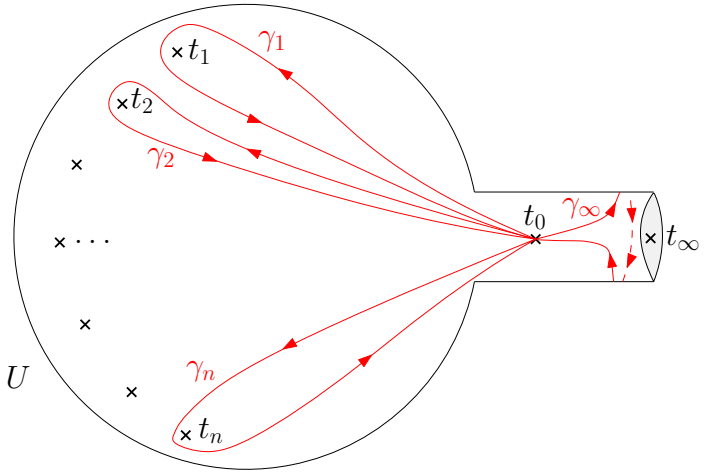


Figure 2.4.22.
L'ouvert U sur lequel on a tracé un bouquet $(\gamma_1, \dots, \gamma_n, \gamma_\infty)$.

– De même, l'ouvert V est homotopiquement équivalent à une sphère privée de $n'+1$ de ses points : les n' points de $\underline{t}'$ et un point t'_∞.

– L'union $U \cup V$ est homéomorphe à une sphère privée de $n+n'$ de ses points, donnés par la configuration $\underline{t} \cup \underline{t}'$.

– L'intersection $U \cap V$, c'est-à-dire le cylindre, est homotopiquement équivalent à une sphère privée de deux de ses points t_∞, t'_∞, dont le groupe fondamental est $\mathbb{Z}$. Soit γ_c le générateur du groupe fondamental qui tourne dans le sens décrit par le dessin suivant :

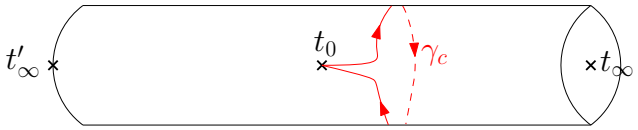


Figure 2.4.23.
Le générateur γ_c.

Le lacet γ_c est homotope au lacet γ_∞, mais il est homotope à *l'inverse* de γ'_∞, puisque γ_c tourne dans le sens *horaire* autour du « point » de gauche t'_∞:

$$\gamma_c = \gamma_\infty = (\gamma'_\infty)^{-1}.$$

À présent, nous utilisons comme précédemment le théorème de van Kampen :

$$\begin{aligned}\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus (\underline{t} \cup \underline{t}'), t_0) &\simeq \pi_1(U \cup V, t_0) \\ &\simeq \pi_1(U, t_0) \underset{\pi_1(U\cap V, t_0)}{*} \pi_1(V, t_0)\end{aligned}$$

et le groupe fondamental $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus (\underline{t} \cup \underline{t}'), t_0)$ est donc isomorphe au groupe :

$$\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \dots, t_n, t_\infty\}, t_0) \underset{\mathbb{Z}}{*} \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t'_1, \dots, t'_{n'}, t'_\infty\}, t_0)$$

où le morphisme $\mathbb{Z} \to \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \dots, t_n, t_\infty\}, t_0)$ est induit par $1 \mapsto \gamma_\infty$ tandis que le morphisme $\mathbb{Z} \to \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t'_1, \dots, t'_{n'}, t'_\infty\}, t_0)$ est induit par $1 \mapsto (\gamma'_\infty)^{-1}$.

Une classe d'isomorphisme de G-revêtements de $\mathbb{P}^1(\mathbb{C}) \setminus (\underline{t} \cup \underline{t}')$ correspond à un morphisme $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus (\underline{t} \cup \underline{t}'), t_0) \to G$. Par la propriété universelle du produit amalgamé, cela correspond à un couple de morphismes :

- $\varphi_1 : \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \dots, t_n, t_\infty\}, t_0) \to G$,
- $\varphi_2 : \pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t'_1, \dots, t'_{n'}, t'_\infty\}, t_0) \to G$

satisfaisant la condition $\varphi_1(\gamma_\infty) = \varphi_2(\gamma'_\infty)^{-1}$.

Si on part d'un G-revêtement de la sphère de gauche ramifié en $\underline{t}$ et d'un G-revêtement de la sphère de droite ramifié en $\underline{t}'$, et qu'on les voit comme des G-revêtements de U et V respectivement, alors les points t_∞ et t'_∞ sont des points de branchement *factices* au sens de la définition 2.3.27. Le morphisme de monodromie φ_1 (resp. φ_2) du G-revêtement marqué de U (resp. de V), ramifié en $\underline{t} \cup \{t_\infty\}$ (resp. $\underline{t}' \cup \{t'_\infty\}$), satisfait donc $\varphi_1(\gamma_\infty) = 1$ (resp. $\varphi_2(\gamma'_\infty) = 1$). En particulier, la condition $\varphi_1(\gamma_\infty) = \varphi_2(\gamma'_\infty)^{-1}$ est bien vérifiée et le recollement est donc possible : on obtient un G-revêtement de $\mathbb{P}^1(\mathbb{C}) \setminus (\underline{t} \cup \underline{t}')$.

Remarque:
Recollement des revêtements et théorème de van Kampen

Remarque 2.4.24. Dans un cas comme dans l'autre, on constate que l'outil central de la construction est le théorème de van Kampen, théorème qu'on envisage *a priori* comme un énoncé sur les lacets. En fait, dans l'esprit de la remarque 2.2.29, on peut envisager l'existence du recollement des revêtements comme étant *précisément* le théorème de van Kampen : si le groupe fondamental est défini par le fait qu'il classifie les revêtements marqués, alors un isomorphisme entre un groupe fondamental et un produit amalgamé (c'est-à-dire, un coproduit) de groupes fondamentaux de sous-espaces n'est rien d'autre qu'une affirmation sur la possibilité de recoller deux revêtements marqués. Dans l'article de blog `https://terrytao.wordpress.com/2012/10/28/van-kampens-theorem-via-covering-spaces/`, Tao propose une

démonstration du théorème de van Kampen en suivant ce point de vue, c'est-à-dire en construisant des recollements explicites.

Cette façon d'envisager le recollement des revêtements se généralise au cas des revêtements algébriques : sur tout corps algébriquement clos, un théorème de van Kampen vaut pour les groupes fondamentaux étales de schémas (quoiqu'il faille prendre la complétion profinie des produits amalgamés). On peut lire à cet usage la discussion à l'adresse suivante : `https://mathoverflow.net/questions/110511/an-etale-version-of-the-van-kampen-theorem`. On verra dans les chapitres 7 et 8 que la question de la possibilité (dans certaines situations) de recoller des revêtements sur des corps qui ne sont pas algébriquement clos est centrale pour le problème de Galois inverse sur les corps de fonctions. Si K est un corps valué complet, par exemple, Harbater a défini une opération de *patching* entre revêtements ramifiés de $\mathbb{P}^1_K$: on peut envisager cette construction comme une forme du théorème de van Kampen pour les droites projectives sur K privées d'un nombre fini de points. Les interrogations de la question 8.1.1, puis nos réponses partielles du théorème 8.1.2, sont motivées par la recherche de formes affaiblies du théorème de van Kampen sur les corps de nombres.

2.5. Summary of the chapter in English

In this section, we summarize some of the content of Chapter 2 in English. The focus is on stating only key definitions and results which are used later in the text.

— Let the topological space X be either the affine complex line $\mathbb{A}^1(\mathbb{C})$ or the projective complex line $\mathbb{P}^1(\mathbb{C})$. In both cases, we fix a basepoint t_0 (the point at infinity if $X = \mathbb{P}^1(\mathbb{C})$). A *configuration* (Definition 2.3.8) is an unordered list of points $\underline{t}$ of $X \setminus \{t_0\}$. Configurations form a topological space $\mathrm{Conf}_{n,X}$, whose fundamental group is the *braid group* $\mathrm{B}_{n,X}$ (Definition 2.3.10).

  If $X = \mathbb{P}^1(\mathbb{C})$, this braid group is isomorphic (Proposition 2.4.8) to the Artin braid group B_n (Definition 2.4.1), which admits the following presentation:

$$\mathrm{B}_n = \left\langle \sigma_1, \sigma_2, \dots, \sigma_{n-1} \;\middle|\; \begin{array}{rcll} \sigma_i\sigma_j & = & \sigma_j\sigma_i & \text{if } |i-j|>2 \\ \sigma_i\sigma_{i+1}\sigma_i & = & \sigma_{i+1}\sigma_i\sigma_{i+1} & \text{if } i<n-1 \end{array} \right\rangle.$$

  When $X = \mathbb{A}^1(\mathbb{C})$, the braid group $\mathrm{B}_{n,\mathbb{A}^1(\mathbb{C})}$ admits the following presentation (Proposition 2.4.8):

$$\left\langle \sigma_1, \sigma_2, \dots, \sigma_{n-1}, z_1 \;\middle|\; \begin{array}{rcll} \sigma_i\sigma_j & = & \sigma_j\sigma_i & \text{if } |i-j|>2 \\ \sigma_i\sigma_{i+1}\sigma_i & = & \sigma_{i+1}\sigma_i\sigma_{i+1} & \text{if } i\in\{1,\dots,n-2\} \\ \sigma_i z_1 & = & z_1\sigma_i & \text{if } i\in\{2,\dots,n-1\} \\ \sigma_1^{-1}z_1\sigma_1^{-1}z_1 & = & z_1\sigma_1^{-1}z_1\sigma_1^{-1} & \end{array} \right\rangle.$$

— We consider branched G-covers of X. A G-cover of X, branched at some configuration $\underline{t} \in \mathrm{Conf}_{n,X}$, is a covering map $p : Y \to X \setminus \underline{t}$ equipped with a morphism α from the group G to the group $\mathrm{Aut}(p)$ of deck transformations of the cover, such that α induces a free transitive action of G on each fiber (Definitions 2.2.10 and 2.3.15). A G-cover of X is necessarily a Galois cover of degree $|G|$.

  A *marked* G-cover is moreover equipped with a marked point in the unramified fiber above the basepoint $t_0 \in X$. (Definition 2.2.13)

  We allow trivial ramification at the "branch points", even if the G-cover can be extended into a G-cover with less branch points. Moreover, we do not require that

G-covers be connected. In particular, a G-cover does not necessarily have G as its automorphism group (see Proposition 2.2.25).

— Consider a marked G-cover of (X, t_0) branched at a configuration $\underline{t}$. One can consider its *monodromy morphism* φ (Definition 2.2.17), which is a group morphism:

$$\varphi : \pi_1(X \setminus \underline{t}, t_0) \to G.$$

This morphism is surjective exactly when the G-cover is connected. In general, its image is a subgroup of G: the *monodromy group* of the marked G-cover (Definition 2.2.18). The marked G-cover is uniquely characterized up to isomorphism by its monodromy morphism: this defines a bijection and even an equivalence of categories (Theorem 2.2.26).

— Let $\underline{t} = \{t_1, \dots, t_n\}$ be a configuration. When X is the affine line $\mathbb{A}^1(\mathbb{C})$, the fundamental group $\pi_1(X \setminus \underline{t}, t_0)$ is freely generated by a particular family $(\gamma_1, \dots, \gamma_n)$ of loops (a *topological bouquet* associated to the configuration $\underline{t}$, cf. Definition 2.3.19 and Proposition 2.4.12). The element $\gamma_i \in \pi_1(X \setminus \underline{t}, t_0)$ is the homotopy class of a loop which rotates once counterclockwise around t_i, and does not rotate around other branch points.

The choice of a topological bouquet induces a bijection between isomorphism classes of marked G-covers of the affine line $\mathbb{A}^1(\mathbb{C})$, branched at $\underline{t} = \{t_1, \dots, t_n\}$, and n-tuples $\underline{g} = (g_1, \dots, g_n)$ of elements of G (Theorem 2.4.14). The tuple $\underline{g}$ is the *branch cycle description* of the marked G-cover; the elements $g_1, \dots, g_n$ are its *local monodromy elements*; the conjugacy classes of these elements (which do not depend on the choice of a bouquet, cf. Corollary 2.3.24) are the *monodromy classes* of the marked branched G-cover (Definitions 2.3.25 and 2.3.28).

The monodromy group of a marked G-cover whose branch cycle description is $\underline{g}$, i.e. the automorphism group of the connected component of its marked point, is $\left\langle \underline{g} \right\rangle = \langle g_1, \dots, g_n \rangle$. In particular, the G-cover is connected exactly when $g_1, \dots, g_n$ generate G.

When X is the complex projective line $\mathbb{P}^1(\mathbb{C})$, a topological bouquet $(\gamma_1, \dots, \gamma_n)$ still generates the whole fundamental group $\pi_1(X \setminus \underline{t}, t_0)$, but there is one nontrivial generating relation:

$$\gamma_1 \cdots \gamma_n = 1.$$

Therefore, the combinatorial description of G-covers as tuples still holds, but one must consider only tuples $\underline{g} = (g_1, \dots, g_n)$ whose product $\pi\underline{g} = g_1 \cdots g_n$ is equal to 1. These tuples are in bijection with isomorphism classes of marked G-covers of $\mathbb{P}^1(\mathbb{C})$ which are branched at a given configuration.

For unmarked G-covers, tuples must be considered up to the conjugation action of the G (acting on all elements of a tuple simultaneously) – this action corresponds to a change of marked point (Proposition 2.2.20, Corollary 2.2.21, Theorem 2.2.28 and Remark 2.4.15).

— Given two marked G-covers of $\mathbb{P}^1(\mathbb{C})$, ramified at disjoint configurations $\underline{t}$ and $\underline{t}'$ (for which bouquets are chosen), we define the gluing of these covers (Definition 2.4.18). In terms of tuples of elements of G (i.e. branch cycle description), the gluing operation corresponds to the concatenation of tuples:

$$(g_1, \dots, g_n)(g'_1, \dots, g'_{n'}) = (g_1, \dots, g_n, g'_1, \dots, g'_{n'}).$$

The number of branch points of the resulting marked G-cover is the sum of the numbers of branch points of the original covers, and its monodromy group is the subgroup of G generated by their monodromy groups.

Chapitre 3

Théorie topologique des espaces de Hurwitz

(A summary of this chapter in English may be found in Section 3.5)

Résumé du chapitre

Dans ce chapitre, nous définissons les espaces de Hurwitz, vus comme espaces topologiques. On insiste sur la description combinatoire de leurs composantes connexes et sur la possibilité de recoller ces composantes. On définit également les monoïdes et anneaux des composantes qui sont au cœur des chapitres suivants.

Organisation du chapitre

Une aube affaiblie
Verse par les champs
La mélancolie
Des soleils couchants.
— P. Verlaine,
Soleils couchants, in *Poèmes saturniens*, 1866.

Pour tout le chapitre, on fixe un groupe fini G.

3.1. Introduction

Ce chapitre consiste en la définition des espaces de Hurwitz (Section 3.2), la description combinatoire de leurs composantes connexes (Section 3.3) puis la définition des monoïdes et anneaux des composantes (Section 3.4) accompagnée de faits les concernant.

Remarque: *Théorie analytique des G-revêtements et des espaces de Hurwitz*

Remarque 3.1.1. Dans ce chapitre et dans le précédent, les revêtements et les espaces de Hurwitz sont considérés d'un point de vue topologique. Cependant, un revêtement topologique d'une variété complexe (telle que $\mathbb{P}^1(\mathbb{C})$, ainsi que les espaces de configurations de points de $\mathbb{P}^1(\mathbb{C})$) hérite d'une structure analytique canonique. Cela montre, d'une part, que les G-revêtements topologiques de la droite complexe (affine ou projective), ramifiés en n points, sont aussi des revêtements *analytiques* de la droite complexe – et, d'autre part, que les espaces de Hurwitz qui classifient ces revêtements, comme revêtements des espaces de configuration de n points de $\mathbb{P}^1(\mathbb{C})$, ont une structure naturelle de variété complexe (de dimension complexe n, voir la remarque 3.2.6).

3.2. Espaces de Hurwitz topologiques

Les espaces de Hurwitz sont des espaces topologiques dont les points correspondent aux classes d'isomorphisme de G-revêtements ramifiés de X, de sorte que la topologie tienne compte de la possibilité de déformer « continûment » un G-revêtement en déplaçant ses points de branchement. Selon la nature précise des revêtements qu'on classifie, on obtient une multitude d'espaces différents. Dans cette section, nous définissons les espaces de Hurwitz des G-revêtements ramifiés de X ainsi que la topologie sur ces espaces.

Des références possibles sont [EVW16, Section 2] pour $X = \mathbb{A}^1(\mathbb{C})$, ou [Völ96, Sous-section 10.1] pour $X = \mathbb{P}^1(\mathbb{C})$.

3.2.1. Une première définition de l'espace de Hurwitz

Définition: *L'espace de Hurwitz* $\mathrm{PHur}^*_X(G,n)$ *vu comme ensemble*

Définition 3.2.1. L'ensemble $\mathrm{PHur}^*_X(G,n)$ est l'ensemble des couples $(\underline{t},\varphi)$ où $\underline{t} \in \mathrm{PConf}_{n,X}$ est une configuration ordonnée de $X \setminus t_0$ et φ est un morphisme de groupes $\pi_1(X \setminus \underline{t}, t_0) \to G$.

D'après le théorème 2.2.26, les éléments de l'ensemble $\mathrm{PHur}^*_X(G,n)$ correspondent aux G-revêtements marqués de (X,t_0) ramifiés en une configuration ordonnée de n points.[1]

On souhaite munir l'ensemble $\mathrm{PHur}^*_X(G,n)$ d'une topologie.

On donne une construction, qu'on utilise plus bas pour définir les ouverts de $\mathrm{PHur}^*_X(G,n)$. Soit U un ouvert de $\mathrm{PConf}_{n,X}$ de la forme $V_1 \times \ldots \times V_n$ où les V_i sont des ouverts disjoints de $X \setminus \{t_0\}$ tous homéomorphes à $\mathbb{R}^2$, et soit φ un morphisme de groupes :

$$\varphi : \pi_1\left(X \setminus \bigcup_i V_i, t_0\right) \to G.$$

Pour chaque configuration $\underline{t} \in U$, l'inclusion définit une équivalence d'homotopie $J_{\underline{t}}$ entre les espaces topologiques pointés suivants :

$$J_{\underline{t}} : \left(X \setminus \bigcup_i V_i, t_0\right) \to (X \setminus \underline{t}, t_0).$$

Puisque $J_{\underline{t}}$ est une équivalence d'homotopie, le morphisme de groupes $\pi_1(J_{\underline{t}})$ qu'elle induit entre les groupes fondamentaux est un isomorphisme :

$$\pi_1(J_{\underline{t}}) : \pi_1\left(X \setminus \bigcup_i V_i, t_0\right) \xrightarrow{\sim} \pi_1(X \setminus \underline{t}, t_0).$$

On note alors $W_{U,\varphi}$ le sous-ensemble suivant de $\mathrm{PHur}^*_X(G,n)$:

$$W_{U,\varphi} \overset{\text{def}}{=} \left\{ \left(\underline{t},\ \varphi \circ (\pi_1(J_{\underline{t}}))^{-1}\right) \,\middle|\, \underline{t} \in U \right\}.$$

Définition: *Ouverts de l'espace de Hurwitz* $\mathrm{PHur}^*_X(G,n)$

Définition 3.2.2. Un sous-ensemble de $\mathrm{PHur}^*_X(G,n)$ est *ouvert* s'il est une union d'ensembles de la forme $W_{U,\varphi}$ pour des choix d'ouverts U et de morphismes φ comme ci-dessus.

Proposition: $\mathrm{PHur}^*_X(G,n)$ *est un revêtement topologique de* $\mathrm{PConf}_{n,X}$

Proposition 3.2.3. *Les sous-ensembles ouverts de* $\mathrm{PHur}^*_X(G,n)$ *forment une topologie de* $\mathrm{PHur}^*_X(G,n)$. *Pour cette topologie, l'application* pr_1 *de projection sur la première coordonnée est un revêtement :*

$$\mathrm{pr}_1 : \begin{cases} \mathrm{PHur}^*_X(G,n) & \to & \mathrm{PConf}_{n,X} \\ (\underline{t},\varphi) & \mapsto & \underline{t} \end{cases}.$$

Démonstration. Il suit directement de la définition que l'ensemble vide est ouvert et que les unions d'ouverts sont des ouverts.

— Montrons que l'espace entier $\mathrm{PHur}^*_X(G,n)$ est ouvert. Pour cela, considérons un de ses points $(\underline{t},\varphi) \in \mathrm{PHur}^*_X(G,n)$. Choisissons des voisinages ouverts V_i de chaque point t_i qui sont homéomorphes à $\mathbb{R}^2$, et tels que les ensembles V_i sont disjoints. On définit alors :

$$U = \prod_i V_i.$$

[1] Le fait de classifier les G-revêtements ramifiés en des configurations ordonnées est non-traditionnel, mais nous introduisons ces espaces comme objets intermédiaires pour arriver à la définition 3.2.4. Dans sa thèse [Cad04], Cadoret les appelle *espaces de Hurwitz dessymétrisés*.

L'inclusion suivante est une équivalence d'homotopie :

$$J_{\underline{t}} : \left(X \setminus \bigcup_i V_i, t_0 \right) \to (X \setminus \underline{t}, t_0)$$

et elle induit donc un isomorphisme de groupes :

$$\pi_1(J_{\underline{t}}) : \pi_1 \left(X \setminus \bigcup_i V_i, t_0 \right) \xrightarrow{\sim} \pi_1(X \setminus \underline{t}, t_0).$$

Si on définit $\widetilde{\varphi}$ comme étant le morphisme $\varphi \circ \pi_1(J_{\underline{t}})$, on a :

$$(\underline{t}, \varphi) \in W_{U,\widetilde{\varphi}}.$$

Le fait que tout point de $\mathrm{PHur}^*_X(G,n)$ appartienne à un ouvert élémentaire $W_{U,\widetilde{\varphi}}$ entraîne que $\mathrm{PHur}^*_X(G,n)$ est ouvert.

— Montrons que l'intersection de deux ouverts est un ouvert. Il suffit de considérer le cas de deux ouverts élémentaires $W_{U,\varphi}$ et $W_{U',\varphi'}$, pour des choix arbitraires de U, φ, U', φ'. On a :

$$U \cap U' = \left(\prod_i V_i \right) \cap \left(\prod_i V'_i \right) = \prod_i (V_i \cap V'_i).$$

Soit $W_i = V_i \cap V'_i$. Si l'un des ouverts W_i est vide, alors il n'y a rien à montrer puisque l'intersection $W_{U,\varphi} \cap W_{U',\varphi'}$ est vide. On se place donc dans le cas où les ouverts W_i sont des ouverts non-vides disjoints de $X \setminus \{t_0\}$. Les deux inclusions suivantes sont des équivalences d'homotopie :

$$\iota_1 : \left(X \setminus \bigcup_i W_i, t_0 \right) \to \left(X \setminus \bigcup_i V_i, t_0 \right),$$

$$\iota_2 : \left(X \setminus \bigcup_i W_i, t_0 \right) \to \left(X \setminus \bigcup_i V'_i, t_0 \right)$$

et elles induisent donc des isomorphismes $\pi_1(\iota_1)$ et $\pi_1(\iota_2)$ entre les groupes fondamentaux correspondants. On définit les deux morphismes $\pi_1 \left(X \setminus \bigcup_i W_i, t_0 \right) \to G$ suivants :

$$\widetilde{\varphi}_1 = \varphi \circ \pi_1(\iota_1),$$
$$\widetilde{\varphi}_2 = \varphi' \circ \pi_1(\iota_2)$$

Pour une configuration $\underline{t} \in U \cap U'$ donnée, on note $J_{\underline{t}}$ et $J'_{\underline{t}}$, respectivement, les inclusions de $X \setminus \bigcup V_i$ (respectivement $X \setminus \bigcup V'_i$) dans $X \setminus \underline{t}$. Ce sont des équivalences d'homotopie.

Si l'intersection $W_{U,\varphi} \cap W_{U',\varphi'}$ est non vide, il existe par définition une configuration $\underline{t} \in U \cap U'$ satisfaisant $\varphi \circ \pi_1(J_{\underline{t}})^{-1} = \varphi' \circ \pi_1(J'_{\underline{t}})^{-1}$. Cela entraîne $\widetilde{\varphi}_1 = \widetilde{\varphi}_2$. On se place dans le cas $\widetilde{\varphi}_1 = \widetilde{\varphi}_2$, puisqu'autrement $W_{U,\varphi} \cap W_{U',\varphi'}$ est vide et donc ouvert. On peut alors écrire l'intersection explicitement comme un ouvert élémentaire, et en particulier elle est ouverte :

$$W_{U,\varphi} \cap W_{U',\varphi'} = W_{\prod_i W_i, \widetilde{\varphi}_1} = W_{\prod_i W_i, \widetilde{\varphi}_2}.$$

— Montrons que l'application $\mathrm{pr}_1 : \mathrm{PHur}^*_X(G,n) \to \mathrm{PConf}_{n,X}$ de projection sur la première coordonnée est un revêtement. Soit V un ouvert de $\mathrm{PConf}_{n,X}$. Si x est un point de V, il existe des ouverts non vides disjoints $N_i(x)$ de $X \setminus \{t_0\}$, chacun homéomorphe à $\mathbb{R}^2$, tels que :

$$x \in \prod_i N_i(x) \qquad \text{et} \qquad \prod_i N_i(x) \subseteq V.$$

et l'image inverse de l'ouvert $\prod_i N_i(x)$ par pr_1 est égale à l'ensemble suivant :

$$\left\{ \left(\underline{t}, \varphi \circ \pi_1(J_{\underline{t}})^{-1} \right) \;\middle|\; \begin{array}{c} \underline{t} \in \prod_i N_i(x) \\ \varphi : \pi_1\left(X \setminus \bigcup_i N_i(x), t_0\right) \to G \end{array} \right\}.$$

On peut alors décrire l'image inverse de V par pr_1 :

$$\begin{aligned} \mathrm{pr}_1^{-1}(V) &= \mathrm{pr}_1^{-1}\left(\bigcup_{x \in V} \prod_i N_i(x) \right) \\ &= \bigcup_{x \in V} \mathrm{pr}_1^{-1}\left(\prod_i N_i(x) \right) \\ &= \bigcup_{x \in V} \left(\bigcup_{\varphi : \pi_1(X \setminus \bigcup_i N_i(x), t_0) \to G} W_{\prod_i N_i(x), \varphi} \right). \end{aligned}$$

C'est un ouvert de $\mathrm{PHur}^*_X(G,n)$, et cela montre que pr_1 est continue.

Soit $\underline{t}_0$ un point de $\mathrm{PConf}_{n,X}$. Il admet un voisinage ouvert de la forme $\prod_i V_i$, où les V_i sont des ouverts non vides disjoints de $X \setminus \{t_0\}$ homéomorphes à $\mathbb{R}^2$. On a alors :

$$\begin{aligned} \mathrm{pr}_1^{-1}(V) &= \bigcup_{\varphi : \pi_1(X \setminus \bigcup_i V_i, t_0) \to G} W_{V,\varphi} \\ &= \bigcup_{\varphi : \pi_1(X \setminus \bigcup_i V_i, t_0) \to G} \left\{ \left(\underline{t}, \varphi \circ \pi_1(J_{\underline{t}})^{-1} \right) \;\middle|\; \underline{t} \in V \right\} \\ &\simeq \bigcup_{\varphi : \pi_1(X \setminus \bigcup_i V_i, t_0) \to G} \{ (\underline{t}, \varphi) \mid \underline{t} \in V \} && \text{en composant } \phi \text{ par } \pi_1(J_{\underline{t}}) \\ &= \bigcup_{\varphi : \pi_1(X \setminus \bigcup_i V_i, t_0) \to G} V \times \{\varphi\} \\ &\simeq \mathrm{Hom}\left(\pi_1\left(X \setminus \bigcup_i V_i, t_0 \right), G \right) \times V \\ &\simeq \mathrm{Hom}\left(\pi_1\left(X \setminus \underline{t}_0, t_0 \right), G \right) \times V && \text{en composant par } \pi_1(J_{\underline{t}_0})^{-1}. \end{aligned}$$

Cela montre que $\mathrm{pr}_1 : \mathrm{PHur}^*_X(G,n) \to \mathrm{PConf}_{n,X}$ est un revêtement dont la fibre est isomorphe à $\mathrm{Hom}\left(\pi_1\left(X \setminus \underline{t}_0, t_0 \right), G \right)$.

□

L'action du groupe symétrique $\mathfrak{S}_n$ sur l'espace $\mathrm{PConf}_{n,X}$ induit une action continue de chaque permutation $\psi \in \mathfrak{S}_n$ sur $\mathrm{PHur}^*_X(G,n)$, correspondant à une réindexation des points de branchement :

$$\psi.\left((t_1, \ldots, t_n), \varphi \right) = \left(\left(t_{\psi(1)}, \ldots, t_{\psi(n)} \right), \varphi \right).$$

Définition 3.2.4. L'*espace de Hurwitz* $\mathrm{Hur}^*_X(G,n)$ *des G-revêtements marqués de (X,t_0) ramifiés en n points non-ordonnés* est le quotient de l'espace topologique $\mathrm{PHur}^*_X(G,n)$ par l'action (libre) du groupe symétrique $\mathfrak{S}_n$, muni de la topologie quotient :

$$\mathrm{Hur}^*_X(G,n) \overset{\text{def}}{=} \mathrm{PHur}^*_X(G,n)/\mathfrak{S}_n.$$

Définition: *L'espace de Hurwitz* $\mathrm{Hur}^*_X(G,n)$ *des G-revêtements marqués de (X,t_0) ramifiés en n points (non-ordonnés)*

L'application $\mathrm{pr}_1 : \mathrm{Hur}^*_X(G,n) \to \mathrm{Conf}_{n,X}$ de projection sur la première coordonnée est un revêtement, et la fibre au-dessus d'une configuration $\underline{t} \in \mathrm{Conf}_{n,X}$ est en bijection avec l'ensemble des morphismes de groupes $\pi_1(X \setminus \underline{t}, t_0) \to G$.

Le fait que $\mathrm{Hur}^*_X(G,n)$ soit un revêtement de $\mathrm{Conf}_{n,X}$ traduit le fait qu'il existe une unique manière de déformer « continûment » un G-revêtement marqué lorsque ses points de branchement se déplacent en restant distincts à chaque instant (voir le lemme 3.2.7).

On récapitule les liens entre $\mathrm{Hur}^*_X(G,n)$, $\mathrm{PHur}^*_X(G,n)$, $\mathrm{Conf}_{n,X}$ et $\mathrm{PConf}_{n,X}$ par le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathrm{PHur}^*_X(G,n) & \xrightarrow{/\mathfrak{S}_n} & \mathrm{Hur}^*_X(G,n) \\ \downarrow{\scriptstyle \mathrm{pr}_1} & & \downarrow{\scriptstyle \mathrm{pr}_1} \\ \mathrm{PConf}_{n,X} & \xrightarrow[/\mathfrak{S}_n]{} & \mathrm{Conf}_{n,X} \end{array} .$$

Fait 3.2.5. Le diagramme ci-dessus est cartésien. Autrement dit, l'espace $\mathrm{PHur}^*_X(G,n)$ est homéomorphe au produit fibré suivant :

$$\mathrm{Hur}^*_X(G,n) \underset{\mathrm{Conf}_{n,X}}{\times} \mathrm{PConf}_{n,X}.$$

Remarque 3.2.6. En tant que revêtement de $\mathrm{Conf}_{n,X}$, l'espace de Hurwitz $\mathrm{Hur}^*_X(G,n)$ satisfait la propriété suivante : chaque point $(\underline{t},\varphi)$ admet un voisinage ouvert sur lequel la restriction de l'application $\mathrm{Hur}^*_X(G,n) \to \mathrm{Conf}_{n,X}$ est un homéomorphisme dans son image. En particulier, $\mathrm{Hur}^*_X(G,n)$ est une variété topologique de dimension $2n$, voir la remarque 2.3.6.

3.2.2. Les espaces de Hurwitz via la construction de Borel

3.2.2.1. L'isomorphisme de transport.

Lemme 3.2.7. *Soit $\Gamma : [0,1] \to \mathrm{Conf}_{n,X}$ un chemin continu reliant deux configurations $[\underline{t}]$ et $[\underline{t}']$. On peut définir un* isomorphisme de transport $\mathrm{T}\Gamma : \pi_1(X \setminus \underline{t}, t_0) \to \pi_1(X \setminus \underline{t}', t_0)$*, qui ne dépend que de la classe d'homotopie de Γ. De plus, cette construction est canonique au sens où $\mathrm{T}(\Gamma * \Gamma') = \mathrm{T}\Gamma' \circ \mathrm{T}\Gamma$ chaque fois que Γ et Γ' sont deux chemins concaténables dans l'espace de configurations $\mathrm{Conf}_{n,X}$.*

Lemme: *L'isomorphisme de transport* $\mathrm{T}\Gamma$

Démonstration. Fixons une configuration ordonnée $\underline{t} \in \mathrm{PConf}_{n,X}$ dont $[\underline{t}]$ est l'orbite sous $\mathfrak{S}_n$, et notons $\widetilde{\Gamma}$ le relèvement de Γ à $\mathrm{PConf}_{n,X}$ qui débute en $\underline{t}$.

Au cours de cette preuve, nous dirons d'un intervalle fermé $I \subseteq [0,1]$ qu'il est *assez petit*[2] lorsque $\widetilde{\Gamma}(I)$ est inclus dans un ouvert de la forme $\prod U_i$, où les ensembles U_i sont des ouverts disjoints de $X \setminus \{t_0\}$, chacun étant homéomorphe à $\mathbb{R}^2$.

[2] Cette notion ne dépend pas du choix de $\widetilde{\Gamma}$: si on permute les coordonnées des valeurs de $\widetilde{\Gamma}$, on n'a qu'à permuter les ouverts U_i de la même façon.

1. Définissons d'abord $\mathrm{T}\,\Gamma|_I$ lorsque $I = [a,b]$ est un intervalle *assez petit*. On fixe $V = \prod_i U_i$ un produit d'ouverts disjoints $U_i \subseteq X \setminus \{t_0\}$ homéomorphes à $\mathbb{R}^2$ tels

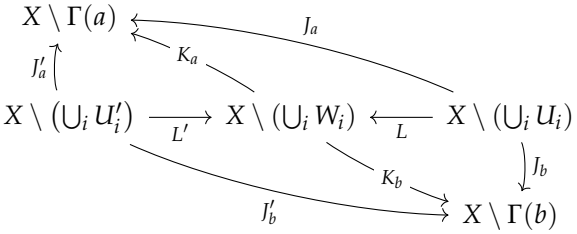
que $\widetilde{\Gamma}(I) \subseteq V$. Les inclusions suivantes sont alors des équivalences d'homotopie :

$$\begin{array}{rcccc} J_a & : & (X \setminus \bigcup_i U_i, t_0) & \to & (X \setminus \Gamma(a), t_0) \\ J_b & : & (X \setminus \bigcup_i U_i, t_0) & \to & (X \setminus \Gamma(b), t_0). \end{array}$$

On définit alors $\mathrm{T}\,\Gamma|_I$ comme étant l'isomorphisme suivant entre les groupes $\pi_1(X \setminus \Gamma(a), t_0)$ et $\pi_1(X \setminus \Gamma(b), t_0)$:

$$T\,\Gamma|_I = \pi_1(J_b) \circ \pi_1(J_a)^{-1}.$$

2. La définition qui précède ne dépend pas des ouverts U_i choisis. En effet, considérons un autre choix $(U_i')_{i\in\{1,\dots,n\}}$ d'ouverts vérifiant les mêmes propriétés que (U_i). Soit, pour chaque i, un ouvert W_i inclus dans $U_i \cap U_i'$, homéomorphe à $\mathbb{R}^2$, et tel que $\widetilde{\Gamma}(I) \subseteq \prod_i W_i$. Les diverses inclusions en présence, qui sont toutes des équivalences d'homotopie, sont désignées par les notations du diagramme suivant :



Remarquons que $K_a \circ L = J_a$, que $K_a \circ L' = J_a'$, que $K_b \circ L = J_b$ et que $K_b \circ L' = J_b'$. On calcule alors :

$$\begin{aligned} \pi_1(J_b) \circ \pi_1(J_a)^{-1} &= \pi_1(K_b) \circ \pi_1(L) \circ \pi_1(L)^{-1} \circ \pi_1(K_a)^{-1} \\ &= \pi_1(K_b) \circ \pi_1(K_a)^{-1} \\ &= \pi_1(K_b) \circ \pi_1(L') \circ \pi_1(L')^{-1} \circ \pi_1(K_a)^{-1} \\ &= \pi_1(J_b') \circ \pi_1(J_a')^{-1}. \end{aligned}$$

Cela montre effectivement que le choix des ouverts (U_i) est sans conséquence.

3. Supposons que $[a, b]$ est un intervalle *assez petit* et que c appartient à l'intervalle ouvert $]a, b[$. On choisit des ouverts U_i comme dans le premier point. L'inclusion suivante est alors une équivalence d'homotopie :

$$J_c : \left(X \setminus \bigcup_i U_i, t_0\right) \to (X \setminus \Gamma(c), t_0).$$

On a alors :

$$\begin{aligned} \mathrm{T}\,\Gamma|_{[c,b]} \circ \mathrm{T}\,\Gamma|_{[a,c]} &= \left(\pi_1(J_b) \circ \pi_1(J_c)^{-1}\right) \circ \left(\pi_1(J_c) \circ \pi_1(J_a)^{-1}\right) \\ &= \pi_1(J_b) \circ \pi_1(J_a)^{-1} \\ &= \mathrm{T}\,\Gamma|_{[a,b]}\,. \end{aligned}$$

4. Définissons désormais $\mathrm{T}\Gamma$ pour le chemin complet $\Gamma : [0, 1] \to \mathrm{Conf}_{n,X}$.

Pour tout point $s \in (0, 1)$, il existe un intervalle *assez petit* dont l'intérieur contient s. Par compacité de l'intervalle $[0, 1]$, cela entraîne qu'on peut choisir une famille fini d'intervalles *assez petit* $[t_i, t_{i+1}]$ avec $t_0 = 0$ et $t_N = 1$. On pose alors :

$$\mathrm{T}\Gamma = \mathrm{T}\,\Gamma|_{[t_{N-1},t_N]} \circ \mathrm{T}\,\Gamma|_{[t_{N-2},t_{N-1}]} \circ \dots \circ \mathrm{T}\,\Gamma|_{[t_1,t_2]} \circ \mathrm{T}\,\Gamma|_{[t_0,t_1]}\,.$$

5. Le fait que $\mathrm{T}\,\Gamma|_{[c,b]} \circ \mathrm{T}\,\Gamma|_{[a,c]} = \mathrm{T}\,\Gamma|_{[a,b]}$, lorsque $[a,b]$ un intervalle *assez petit* dont l'intérieur contient c, entraîne que la définition de $\mathrm{T}\Gamma$ ne dépend pas du choix des intervalles $[t_i, t_{i+1}]$. En effet, si on a deux collections d'intervalles $([t_i,t_{i+1}])_{i\in\{1,\dots,N-1\}}$ et $([t'_i,t'_{i+1}])_{i\in\{1,\dots,N'-1\}}$, on trie l'ensemble contenant tous les points t_i et t'_i. On obtient ainsi une collection d'intervalles $([t''_i,t''_{i+1}])_{i\in\{1,\dots,N''-1\}}$ qui raffine les deux collections à la fois, et alors :

$$\begin{aligned}\mathrm{T}\,\Gamma|_{[t_{N-1},t_N]} \circ \dots \circ \mathrm{T}\,\Gamma|_{[t_0,t_1]} &= \mathrm{T}\,\Gamma|_{[t''_{N''-1},t''_{N''}]} \circ \dots \circ \mathrm{T}\,\Gamma|_{[t''_0,t''_1]} \\ &= \mathrm{T}\,\Gamma|_{[t'_{N'-1},t'_{N'}]} \circ \dots \circ \mathrm{T}\,\Gamma|_{[t'_0,t'_1]}\,.\end{aligned}$$

6. De même, l'égalité $\mathrm{T}\,\Gamma|_{[c,b]} \circ \mathrm{T}\,\Gamma|_{[a,c]} = \mathrm{T}\,\Gamma|_{[a,b]}$, vraie dans le cas où $[a,b]$ est *assez petit*, entraîne l'égalité plus générale pour tous chemins concaténables Γ et Γ' dans $\mathrm{Conf}_{n,X}$:
$$\mathrm{T}(\Gamma * \Gamma') = \mathrm{T}\Gamma' \circ \mathrm{T}\Gamma.$$

7. Le fait que $\mathrm{T}\Gamma$ ne dépende que de la classe d'homotopie de Γ se montre en utilisant des méthodes similaires. On ne donne qu'une esquisse de la démonstration. Si H est une homotopie entre les chemins Γ et Γ' dans $\mathrm{Conf}_{n,X}$, et si γ est un lacet dans X basé en t_0, on peut déformer de manière unique des portions « suffisamment petites » du chemin γ le long de portions « suffisamment petites » de l'homotopie H. Par compacité du carré $[0,1]^2$, on n'a besoin d'appliquer ce raisonnement qu'un nombre fini de fois. On construit ainsi une homotopie entre des lacets représentant $\mathrm{T}\Gamma(\gamma)$ et $\mathrm{T}\Gamma'(\gamma)$, ce qui entraîne l'invariance par homotopie.

□

Remarque 3.2.8. Puisque $\mathrm{T}\Gamma$ ne dépend que de la classe d'homotopie de Γ, nous utilisons volontiers la notation $\mathrm{T}\Gamma$ lorsque Γ est une classe d'homotopie de chemins (ou de lacets) dans $\mathrm{Conf}_{n,X}$, et notamment si Γ est une tresse.

3.2.2.2. La construction de Borel. On s'intéresse à une autre définition (Définition 3.2.9) des espaces de Hurwitz qu'on trouve dans [EVW16, Definition 2.2], et on la compare à la définition précédente (Définition 3.2.4).

On fixe une configuration-base $\underline{t} \in \mathrm{Conf}_{n,X}$. On définit une action du groupe des tresses $\mathrm{B}_{n,X}$ basé en $\underline{t}$ (Définition 2.3.10) sur le groupe fondamental $\pi_1(X \setminus \underline{t}, t_0)$ par la formule suivante, pour $\Gamma \in \mathrm{B}_{n,X}$ et $\gamma \in \pi_1(X \setminus \underline{t}, t_0)$:

$$\Gamma.\gamma \overset{\text{def}}{=} \mathrm{T}\Gamma(\gamma)$$

où $\mathrm{T}\Gamma$ est l'isomorphisme du lemme 3.2.7. On définit également une action du groupe des tresses $\mathrm{B}_{n,X}$ sur l'ensemble $\mathrm{Hom}(\pi_1(X \setminus \underline{t}, t_0), G)$ par la formule:

$$\Gamma.\varphi \overset{\text{def}}{=} \varphi \circ \mathrm{T}\Gamma^{-1}.$$

Si $\underline{t}', \underline{t}'' \in \mathrm{Conf}_{n,X}$ sont deux configurations, on désigne par $[\underline{t}' \to \underline{t}'']$ l'ensemble des classes d'homotopie de chemins dans $\mathrm{Conf}_{n,X}$ reliant $\underline{t}'$ et $\underline{t}''$. En particulier, l'ensemble $[\underline{t} \to \underline{t}]$ est le groupe des tresses $\mathrm{B}_{n,X}$ débarrassé de sa structure de groupe. On désigne par $\widetilde{\mathrm{Conf}}_{n,X}$ le revêtement universel de $\mathrm{Conf}_{n,X}$ (Proposition 2.2.27), qu'on envisage comme l'ensemble des couples $(\underline{t}', \Gamma)$ avec $\underline{t}' \in \mathrm{Conf}_{n,X}$ et $\Gamma \in [\underline{t} \to \underline{t}']$, muni de la

topologie compacte-ouverte. Enfin, on définit une action de $B_{n,X}$ sur $\widetilde{\mathrm{Conf}_{n,X}}$ par la formule :

$$\Gamma.(\underline{t}', \Gamma') = (\underline{t}', \Gamma * \Gamma').$$

(Il s'agit de l'action de $B_{n,X} = \pi_1(\mathrm{Conf}_{n,X}, \underline{t})$, libre et transitive sur les fibres, qui fait de $\widetilde{\mathrm{Conf}_{n,X}}$ un $\pi_1(\mathrm{Conf}_{n,X}, \underline{t})$-revêtement)

Définition: *Construction de Borel des espaces de Hurwitz*

Définition 3.2.9. La *construction de Borel des espaces de Hurwitz* est l'espace topologique suivant, obtenu comme produit fibré :

$$\mathrm{BHur}^*_X(G,n) = \widetilde{\mathrm{Conf}_{n,X}} \times_{B_{n,X}} \mathrm{Hom}(\pi_1(X \setminus \underline{t}, t_0), G).$$

Cette construction est équivalente à celle de la sous-section 3.2.1 :

Proposition: *La construction de Borel définit le même espace de Hurwitz*

Proposition 3.2.10. *L'espace* $\mathrm{BHur}^*_X(G,n)$ *est homéomorphe à l'espace de Hurwitz* $\mathrm{Hur}^*_X(G,n)$.

Démonstration. On définit une application continue $F : \mathrm{BHur}^*_X(G,n) \to \mathrm{Hur}^*_X(G,n)$ dont on montre ensuite qu'elle est un homéomorphisme. Soit $(\underline{t}', \Gamma, \varphi) \in \mathrm{BHur}^*_X(G,n)$, avec $\underline{t}' \in \mathrm{Conf}_{n,X}$, $\Gamma \in [\underline{t} \to \underline{t}']$ et $\varphi : \pi_1(X \setminus \underline{t}, t_0) \to G$. On pose :

$$F(\underline{t}', \Gamma, \varphi) = (\underline{t}', \varphi \circ \mathrm{T}\Gamma^{-1}) \in \mathrm{Hur}^*_X(G,n).$$

Cette formule définit effectivement une application sur le produit fibré $\mathrm{BHur}^*_X(G,n) = \widetilde{\mathrm{Conf}_{n,X}} \times_{B_{n,X}} \mathrm{Hom}(\pi_1(X \setminus \underline{t}, t_0), G)$. En effet, pour tout $\Phi \in B_{n,X}$, on a :

$$F(\underline{t}', \Phi * \Gamma, \varphi) = (\underline{t}', \varphi \circ T\Phi^{-1} \circ \mathrm{T}\Gamma^{-1}) = F(\underline{t}', \Gamma, \varphi \circ T\Phi^{-1}).$$

Puisque F induit l'identité en projection sur $\mathrm{Conf}_{n,X}$, il s'agit d'un morphisme de revêtements entre les revêtements $\mathrm{BHur}^*_X(G,n)$ et $\mathrm{Hur}^*_X(G,n)$, qui ont le même degré $|\mathrm{Hom}(\pi_1(X \setminus \underline{t}, t_0), G)|$. De plus, l'application F est injective. En effet, si on a une égalité :

$$F(\underline{t}', \Gamma, \varphi) = F(\underline{t}'_2, \Gamma_2, \varphi_2)$$

alors il vient par définition :

$$(\underline{t}', \varphi \circ \mathrm{T}\Gamma^{-1}) = (\underline{t}'_2, \varphi_2 \circ \mathrm{T}\Gamma_2^{-1}),$$

en particulier, $\underline{t}' = \underline{t}'_2$; de plus, en notant Φ le lacet $\Gamma * \Gamma_2^{-1}$ basé en $\underline{t}$:

$$\varphi_2 = \varphi \circ \mathrm{T}\Gamma^{-1} \circ \mathrm{T}\Gamma_2 = \varphi \circ \mathrm{T}\Phi^{-1}.$$

Il en découle qu'on a les égalités suivantes dans $\mathrm{BHur}^*_X(G,n)$:

$$(\underline{t}'_2, \Gamma_2, \varphi_2) = (\underline{t}, \Phi^{-1} * \Gamma, \varphi \circ \mathrm{T}\Phi^{-1}) = (\underline{t}, \Gamma, \varphi \circ \mathrm{T}\Phi^{-1} \circ \mathrm{T}\Phi) = (\underline{t}, \Gamma, \varphi).$$

L'application F induit donc des injections entre les fibres, qui sont finies de même cardinal. On en déduit que F est bijective.

Soit p (respectivement q) le revêtement $\mathrm{BHur}^*_X(G,n) \to \mathrm{Conf}_{n,X}$ (respectivement $\mathrm{Hur}^*_X(G,n) \to \mathrm{Conf}_{n,X}$). Soit $\underline{t}' \in \mathrm{Conf}_{n,X}$ une configuration, et soit N un voisinage ouvert de $\underline{t}'$ dans $\mathrm{Conf}_{n,X}$ homéomorphe à $\mathbb{R}^{2n}$. On a :

$$\begin{aligned} p^{-1}(N) &\simeq N \times \mathrm{Hom}(\pi_1(X \setminus \underline{t}), G) \\ q^{-1}(N) &= \left\{ (\underline{t}'', \varphi) \;\middle|\; \begin{array}{c} \underline{t}'' \in N \\ \varphi \in \mathrm{Hom}(\pi_1(X \setminus \underline{t}'', t_0), G) \end{array} \right\}. \end{aligned}$$

Sous cette description, la restriction de F à $p^{-1}(N)$ est l'application :

$$(\underline{t}'', \varphi) \mapsto (\underline{t}'', \varphi \circ \mathrm{T}\Phi)$$

où Φ désigne l'unique classe d'homotopie de chemins dans N reliant $\underline{t}''$ et $\underline{t}'$. L'application ci-dessus est un homéomorphisme. Ainsi, toute configuration $\underline{t}'$ admet un voisinage ouvert N au-dessus duquel la restriction F est ouverte, et F est donc ouverte. Comme bijection continue et ouverte, F est un homéomorphisme. □

3.2.3. **Quelques espaces de Hurwitz plus spécifiques**

Définition: *Espace de Hurwitz des G-revêtements connexes*

Définition 3.2.11. L'*espace de Hurwitz* $\mathrm{CHur}^*_X(G,n)$ *des G-revêtements connexes* est le sous-espace suivant de $\mathrm{Hur}^*_X(G,n)$, muni de la topologie de sous-espace :

$$\mathrm{CHur}^*_X(G,n) \overset{\text{def}}{=} \left\{ (\underline{t}, \varphi) \;\middle|\; \begin{array}{c} \underline{t} \in \mathrm{Conf}_{n,X} \\ \varphi : \pi_1(X \setminus \underline{t}, t_0) \to G \text{ est surjectif} \end{array} \right\}.$$

Définition: *Espace de Hurwitz des G-revêtements non-marqués*

Définition 3.2.12. L'*espace de Hurwitz* $\mathrm{Hur}_X(G,n)$ *des G-revêtements non-marqués* est le quotient de $\mathrm{Hur}^*_X(G,n)$ par l'action de conjugaison de $\mathrm{Inn}(G)$, muni de la topologie quotient :

$$\mathrm{Hur}_X(G,n) \overset{\text{def}}{=} \left\{ (\underline{t}, \widetilde{\varphi}) \;\middle|\; \begin{array}{c} \underline{t} \in \mathrm{Conf}_{n,X} \\ \widetilde{\varphi} \in \mathrm{Hom}(\pi_1(X \setminus \underline{t}, t_0), G)/\mathrm{Inn}(G) \end{array} \right\}$$

On définit de même l'espace $\mathrm{CHur}_X(G,n) = \mathrm{CHur}_X(G,n)/\mathrm{Inn}(G)$ des G-revêtements connexes non-marqués.

Remarque 3.2.13. L'opération de corestriction, qui associe à un morphisme $\varphi : \pi_1(X \setminus \underline{t}, t_0) \to G$ d'image H le morphisme surjectif $\widetilde{\varphi} : \pi_1(X \setminus \underline{t}, t_0) \to H$, induit un homéomorphisme :

$$\mathrm{Hur}^*_X(G,n) \simeq \bigsqcup_{H \subseteq G} \mathrm{CHur}^*_X(H,n).$$

En revanche, on ne peut pas remplacer les espaces de Hurwitz de G-revêtements marqués par des espaces de revêtements non-marqués dans cet homéomorphisme. En effet, l'action de conjugaison par G, par laquelle on quotiente à gauche, ne préserve pas le groupe de monodromie H s'il est non-distingué.

3.2.4. **Contraintes sur la monodromie**

Un sous-ensemble c de G est *invariant par conjugaison* lorsqu'il s'agit d'une union de classes de conjugaison de G. On fixe un ensemble D de sous-ensembles de G tous invariants par conjugaison et deux à deux disjoints, ainsi qu'une application ξ de D dans $\{0,1,\ldots\}$. Enfin, on pose $|\xi| = \sum_{c \in D} \xi(c)$.

Remarque 3.2.14. Il faut voir l'application ξ comme une liste de multiplicités qu'on affecte aux éléments de D. Au lieu de considérer un ensemble D et une application $\xi : D \to \{0,1,\ldots\}$, on aurait pu prendre un *multiensemble* D d'ensembles disjoints invariants par conjugaison. Dans ce contexte, $|\xi|$ est le cardinal de D au sens des multiensembles.

On suppose toujours X orientée.

Définition: *Espace de Hurwitz avec des contraintes sur les classes de monodromie*

Définition 3.2.15. L'*espace de Hurwitz* $\mathrm{Hur}^*_X(G, D, \xi)$ est l'espace topologique obtenu en munissant le sous-ensemble suivant de $\mathrm{Hur}^*_X(G, |\xi|)$ de la topologie de sous-espace :

$$\mathrm{Hur}^*_X(G, D, \xi) \overset{\text{def}}{=} \left\{ (\underline{t}, \varphi) \;\middle|\; \begin{array}{c} \underline{t} \in \mathrm{Conf}_{|\xi|, X} \\ \varphi : \pi_1(X \setminus \underline{t}, t_0) \to G \\ |\{i \mid \varphi(\gamma_i) \in c\}| = \xi(c) \text{ pour tout } c \in D \end{array} \right\}$$

où $(\gamma_i)_{i \in \{1,\ldots,|\xi|\}}$ est un bouquet quelconque associé à $\underline{t}$. [3]

[3] Ce choix n'influence pas la définition. En effet, changer de bouquet ne fait que permuter et/ou conjuguer les éléments locaux de monodromie, ce qui n'affecte pas le nombre d'entre eux qui sont dans un ensemble $c \in D$ car c est invariant par conjugaison.

Si D est un ensemble de classes de conjugaison de G, alors les G-revêtements marqués ramifiés appartenant à $\mathrm{Hur}^*_X(G, D, \xi)$ sont exactement ceux dont le (G, G)-multidiscriminant évalué en une classe de conjugaison γ de G vaut $\begin{cases} \xi(\gamma) & \text{si } \gamma \in D \\ 0 & \text{sinon} \end{cases}$. De façon analogue, on définit des espaces de Hurwitz $\mathrm{CHur}^*_X(G, D, \xi)$, $\mathrm{Hur}_X(G, D, \xi)$ et $\mathrm{CHur}_X(G, D, \xi)$ classifiant les G-revêtements connexes et/ou non-marqués dont le multidiscriminant est contraint.

Remarque: *Classes de monodromie dans le cas non-orientable*

Remarque 3.2.16. Supposons X non-orientable. Si l'on essaie de répliquer la définition des bouquets et ce qui en découle, il s'avère impossible de faire une distinction entre la classe d'homotopie du lacet τ_i et celle de τ_i^{-1} dans la preuve de la proposition 2.3.23. Dans le cas non-orientable, on doit donc supposer que les éléments de D ne sont pas simplement des sous-ensembles invariants par conjugaison, mais des sous-ensembles de G invariants à la fois par conjugaison et par inversion (par exemple, l'ensemble des éléments de G ayant un ordre donné). Sous cette hypothèse, on peut définir l'espace $\mathrm{Hur}^*_X(G, D, \xi)$ comme précédemment, sans hypothèse d'orientabilité.

Remarque 3.2.17. L'espace de Hurwitz $\mathrm{Hur}^*_X(G, n)$ pris tout entier est un cas particulier de la construction de la définition 3.2.15. En effet, en prenant pour D le singleton $\{G\}$ et en notant n l'application qui envoie G sur n, on a :

$$\mathrm{Hur}^*_X(G, n) = \mathrm{Hur}^*_X(G, \{G\}, n).$$

Par conséquent, nous concentrons notre attention sur les espaces de Hurwitz $\mathrm{Hur}^*_X(G, D, \xi)$, qui sont le cas le plus général. Les énoncés valent automatiquement pour $\mathrm{Hur}^*_X(G, n)$.

3.2.5. **Fonctorialité des espaces de Hurwitz**

Dans cette sous-section, on examine la fonctorialité des espaces de Hurwitz. Pour cela, on définit la catégorie suivante :

Définition 3.2.18. La catégorie **ConjInv** (pour « **Conj**ugation **Inv**ariant ») est définie de la façon suivante :

— Les objets de **ConjInv** sont les triplets (H, D, ξ) où H est un groupe, D est un ensemble de sous-ensembles de H invariants par conjugaison et deux à deux disjoints, et ξ est une application de D dans $\{0, 1, \ldots\}$.

— Les morphismes entre deux objets (H, D, ξ) et (H', D', ξ') sont les couples (f, f_*) où f est un morphisme de groupes $H \to H'$ et f_* est une application $D \to D'$ satisfaisant :

- Pour tout $c \in D$ et $g \in c$, l'élément $f(g)$ se trouve dans le sous-ensemble $f_*(c)$.
- Pour tout $c' \in D'$, on a :
$$\xi'(c') = \sum_{c \in f_*^{-1}(c')} \xi(c).$$

Fait: *Fonctorialité de* Hur^*

Fait 3.2.19. Soit $(f, f_*) : (H, D, \xi) \to (H', D', \xi')$ un morphisme dans **ConjInv**. Alors f donne lieu à une application continue :
$$\mathrm{Hur}^*_X(f, f_*) : \begin{cases} \mathrm{Hur}^*_X(H, D, \xi) & \to & \mathrm{Hur}^*_X(H', D', \xi') \\ (\underline{t}, \varphi) & \mapsto & (\underline{t}, f \circ \varphi) \end{cases}.$$
En d'autres termes, Hur^*_X est un foncteur de **ConjInv** dans **Top**.
Par ailleurs :

— Si le morphisme f est injectif, l'application $\mathrm{Hur}^*_X(f, f_*)$ est également injective. En particulier, si H est un sous-groupe de H' et que f est l'inclusion $H \to H'$, on voit $\mathrm{Hur}^*_X(H, D, \xi)$ comme un sous-espace de $\mathrm{Hur}^*_X(H', D', \xi')$ (voir la remarque 3.2.13).

— Si le morphisme f est surjectif, il induit une application continue :
$$\mathrm{CHur}^*_X(H, D, \xi) \to \mathrm{CHur}^*_X(H', D', \xi')$$
puisqu'une composition de surjections est surjective.

3.2.6. **Sous-groupes D-engendrés**

Soit D un ensemble de sous-ensembles disjoints de G invariants par conjugaison, et ξ une application $D \to \{1, 2, \ldots\}$. Dans cette sous-section, on donne un critère permettant de déterminer si un sous-groupe de G est le groupe de monodromie d'un G-revêtement se trouvant dans $\mathrm{Hur}^*_X(G, D, n\xi)$ pour un entier $n \in \mathbb{N}$.

Définition: *Sous-groupe D-engendré*

Définition 3.2.20. Un sous-groupe H de G est *D-engendré* s'il est trivial ou si les deux conditions suivantes sont satisfaites :

— Le sous-groupe H est engendré par un sous-ensemble de $\bigcup_{c \in D} c$. De manière équivalente :
$$H = \left\langle \bigcup_{c \in D} (c \cap H) \right\rangle.$$

— Le sous-groupe H a une intersection non-vide avec chacun des ensembles $c \in D$:
$$\forall c \in D,\ c \cap H \neq \varnothing.$$

On note $\mathrm{Sub}_{G,D}$ l'ensemble des sous-groupes D-engendrés de G. La notation $\mathrm{Sub}_{G,D}$ est adaptée de [ETW17, Subsection 6.5], même si notre définition est un peu plus restrictive.

Fait 3.2.21. On fait les observations suivantes :

— Tout sous-groupe de G est $\{G\}$-engendré.

— Si H, H' sont des sous-groupes D-engendrés, alors le sous-groupe $\langle H, H' \rangle$ est D-engendré.

— Si un $H \subseteq G$ a une intersection non-vide avec chacun des ensembles $c \in D$, alors $\langle (c \cap H)_{c \in D} \rangle$ est le plus gros sous-groupe D-engendré inclus dans H.

Proposition 3.2.22. *Si $X = \mathbb{A}^1(\mathbb{C})$ ou $X = \mathbb{P}^1(\mathbb{C})$, alors un sous-groupe H de G est D-engendré si et seulement s'il est groupe de monodromie d'un revêtement se trouvant dans $\mathrm{Hur}^*_X(G, D, n\xi)$ pour un entier $n \geq 0$.*

Proposition:
Les groupes D-engendrés sont exactement les groupes de monodromie des revêtements dans $\mathrm{Hur}^*_X(G, D, n\xi)$ [Seg22, Proposition 2.10]

Démonstration. Dans le cas où H est le sous-groupe trivial, le revêtement trivial convient. Montrons qu'un groupe non-trivial est D-engendré si et seulement s'il est le groupe d'un revêtement dans $\mathrm{Hur}^*_X(G, D, n\xi)$ pour un entier $n \geq 1$:

($\Leftarrow$) Supposons que H soit le groupe de monodromie d'un revêtement se trouvant dans $\mathrm{Hur}^*_X(G, D, n\xi)$ avec $n \geq 1$, et soit $\underline{g}$ la description des cycles de branchement de ce revêtement pour un bouquet arbitraire. Alors $H = \left\langle \underline{g} \right\rangle$ est effectivement engendré par des éléments de $\bigcup_{c \in D} c$, et pour tout $c \in D$, l'ensemble $H \cap c$ est bien non-vide puisque le uplet $\underline{g}$ contient $n\xi(c) \geq 1$ éléments qui sont dans c. On a montré que H était D-engendré.

($\Rightarrow$) Soit H un sous-groupe D-engendré non-trivial de G. Pour chaque $c \in D$, fixons un élément $g_c \in H \cap c$. Soit $M = \max_{c \in D} |H \cap c|$. Pour chaque $c \in D$, fixons une énumération $h(c)_1, \ldots, h(c)_{|H \cap c|}$ des éléments de $H \cap c$, et complétons-la au besoin avec des copies de l'élément g_c de sorte que $\underline{h(c)}$ soit un M-uplet d'éléments de c contenant chaque élément de $H \cap c$.

On considère alors la concaténation suivante, effectuée dans un ordre arbitraire :

$$\underline{g} = \prod_{c \in D} \underline{h(c)}^{\exp(G)\xi(c)}.$$

Le uplet $\underline{g}$ vérifie $\pi\underline{g} = 1$, et de plus $\left\langle \underline{g} \right\rangle = H$ puisque H est engendré par les ensembles $H \cap c$ par hypothèse. Le G-revêtement marqué associé au uplet $\underline{g}$ a ainsi bien H pour groupe de monodromie, et appartient à $\mathrm{Hur}^*_X(G, D, M \exp(G)\, \xi)$.

□

3.3. Composantes connexes des espaces de Hurwitz

L'objet de cette section est de donner une description combinatoire des composantes connexes des espaces de Hurwitz dans les cas où X est la droite affine complexe $\mathbb{A}^1(\mathbb{C})$ ou la droite projective complexe $\mathbb{P}^1(\mathbb{C})$. Pour cela, nous sommes conduits à étudier l'action du groupe des tresses sur les n-uplets d'éléments de G et les propriétés de cette action.

3.3.1. Action du groupe des tresses sur les G-revêtements

Soit $\varphi, \varphi' : \pi_1(X \setminus \underline{t}, t_0) \to G$ les morphismes de monodromie de deux G-revêtements marqués, branchés en une même configuration $\underline{t} \in \mathrm{Conf}_{n,X}$. Ces deux G-revêtements sont reliés par un chemin dans l'espace de Hurwitz $\mathrm{Hur}^*_X(G, n)$ si et seulement s'il existe un lacet $\Phi \in \pi_1(\mathrm{Conf}_{n,X}, \underline{t})$ tel que $(\underline{t}, \varphi)[\Phi] = (\underline{t}, \varphi')$. Si $\Phi \in \pi_1(\mathrm{Conf}_{n,X}, \underline{t})$ est une tresse, le chemin suivant :

$$u \in [0,1] \mapsto \left(\Phi(u), \varphi \circ \mathrm{T}\, \Phi|^{-1}_{[0,u]} \right)$$

est le relèvement de Φ dans $\mathrm{Hur}^*_X(G, n)$ qui débute en $(\underline{t}, \varphi)$. On a donc $(\underline{t}, \varphi)[\Phi] = (\underline{t}, \varphi \circ \mathrm{T}\Phi^{-1})$ pour toute tresse Φ. Ainsi $(\underline{t}, \varphi)$ et $(\underline{t}, \varphi')$ sont dans la même composante

connexe de l'espace de Hurwitz si et seulement s'il existe une tresse $\Phi \in B_{n,X}$ (basée en $\underline{t}$) telle que :

$$\varphi \circ T\Phi^{-1} = \varphi'.$$

On suppose désormais que $X = \mathbb{A}^1(\mathbb{C})$ ou $X = \mathbb{P}^1(\mathbb{C})$. Fixons un bouquet topologique $(\gamma_i)_{i\in\{1,\dots,n\}}$ associé à la configuration $\underline{t}$. En vertu du théorème 2.4.14, nous savons que les éléments de $\mathrm{Hur}^*_X(G,n)$ branchés en $\underline{t} \in \mathrm{Conf}_{n,X}$ peuvent être décrits de manière combinatoire, comme des n-uplets d'éléments de G. Il ne reste plus, pour obtenir une description combinatoire des composantes connexes de $\mathrm{Hur}^*_X(G,n)$, qu'à comprendre ce que devient l'action du groupe des tresses $B_{n,X}$ sur les G-revêtements branchés en $\underline{t}$ quand on les voit comme des n-uplets d'éléments de G.

La proposition 2.4.8 donne une présentation du groupe des tresses $B_{n,X}$ par générateurs et relations. Il suffit donc de décrire l'action des générateurs de ce groupe sur les n-uplets d'éléments de G.

Réglons d'abord le cas du générateur additionnel z_1 qu'on obtient lorsque $X = \mathbb{A}^1(\mathbb{C})$. Celui-ci n'affecte bien sûr pas les lacets $\gamma_2, \dots, \gamma_n$ du bouquet, et il déforme le lacet γ_1 de la façon suivante :

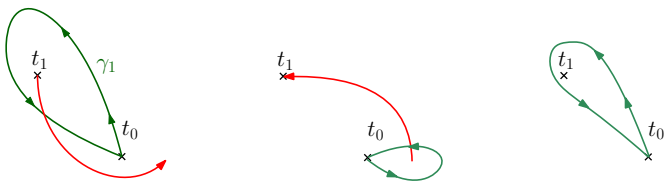


Figure 3.3.1. L'action du générateur z_1 sur γ_1. La figure illustre le calcul de $T(z_1)(\gamma_1)$.

Comme on le constate, cette action est triviale : le fait qu'un point de branchement tourne autour de t_0 ne change rien aux classes d'homotopie des lacets qui définissent les bouquets puisqu'on les regarde dans $X \setminus \underline{t}$, qui contient t_0. Cela « compense » les artefacts causés par notre choix d'exclure t_0 dans la définition des espaces de configuration (la remarque 2.3.11 est finalement secondaire).

Puisque l'action du générateur additionnel z_1 de $B_{n,\mathbb{A}^1(\mathbb{C})}$ sur les bouquets est triviale, on peut se concentrer dans tous les cas – pour $\mathbb{A}^1(\mathbb{C})$ comme pour $\mathbb{P}^1(\mathbb{C})$ –, sur l'action du groupe des tresses d'Artin B_n, et plus particulièrement sur les tresses élémentaires σ_i qui l'engendrent. Considérons la tresse élémentaire σ_i :

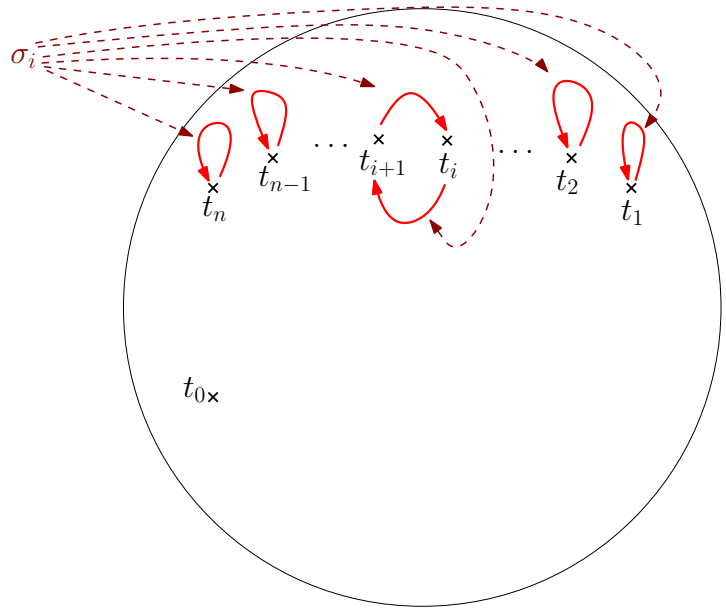


Figure 3.3.2. La i-ième tresse élémentaire.

On suit la déformation du bouquet au fur et à mesure du tressage des points de branchement selon σ_i :

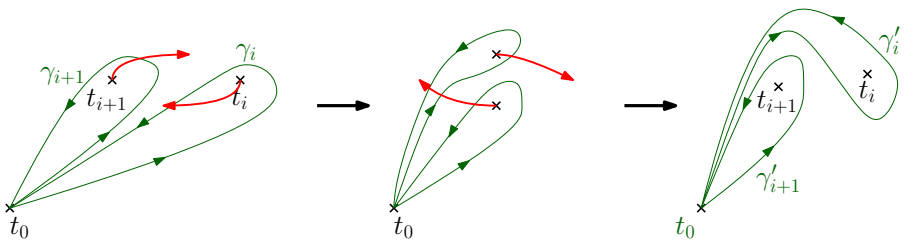


Figure 3.3.3. Déformation d'un bouquet selon la i-ième tresse élémentaire.

On obtient de cette façon un nouveau bouquet $(\gamma'_j)_{j\in\{1,\dots,n\}}$ qui vérifie :

$$\gamma'_j = \mathrm{T}\sigma_i(\gamma_{\psi^{-1}(j)})$$

où $\psi = \psi^{-1}$ est la transposition $(i, i+1)$. Pour $j \notin \{i, i+1\}$ on a naturellement :

$$\gamma'_j = \gamma_j$$

et, comme illustré par le dessin ci-dessus, on a aussi l'égalité $\gamma'_{i+1} = \gamma_{i+1}$. De plus, sur ce même dessin, on voit que les lacets $\gamma_i\gamma_{i+1}$ et $\gamma'_{i+1}\gamma'_i$ sont tous deux homotopes au lacet suivant :

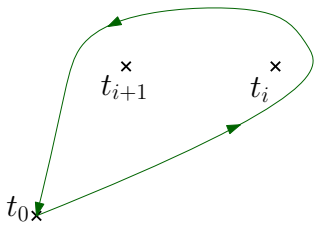


Figure 3.3.4. Un lacet homotope à la fois à $\gamma_i\gamma_{i+1}$ et $\gamma'_{i+1}\gamma'_i$.

Ces homotopies induisent l'égalité suivante dans le groupe fondamental :

$$\gamma_i = (\gamma'_{i+1}\gamma'_i)\,(\gamma_{i+1})^{-1} = \gamma'_{i+1}\gamma'_i\,(\gamma'_{i+1})^{-1} = (\gamma'_i)^{\gamma'_{i+1}}.$$

De cette discussion, on tire la conséquence suivante :

Proposition: *Description de l'action du groupe des tresses sur les G-revêtements marqués en termes de leur description des cycles de branchement*

Proposition 3.3.5. *Soit φ un morphisme de groupes $\pi_1(X \setminus \underline{t}, t_0) \to G$. Notons $\underline{g}$ la description des cycles de branchement du G-revêtement marqué $(\underline{t}, \varphi)$ pour le bouquet $\underline{\gamma}$; il s'agit d'un n-uplet d'éléments de G :*

$$\underline{g} = \mathrm{BCD}_{\underline{\gamma}}(\underline{t}, \varphi) = (g_1, \dots, g_n) \in G^n.$$

Soit un entier $i \in \{1, \dots, n-1\}$ et soit $(\underline{t}, \varphi') \in \mathrm{PHur}^*_X(G, n)$ l'élément de $\mathrm{PHur}^*_X(G, n)$ obtenu en laissant la i-ième tresse élémentaire $\sigma_i \in \mathrm{B}_{n,X}$ agir sur le G-revêtement marqué $(\underline{t}, \varphi)$, c'est-à-dire :

$$(\underline{t}, \varphi') = (\underline{t}, \varphi')[\sigma_i] = (\underline{t}, \varphi \circ \mathrm{T}\sigma_i^{-1}).$$

Alors la description des cycles de branchement du G-revêtement marqué $(\underline{t}, \varphi')$ pour le bouquet $\underline{\gamma}$ est :

$$\mathrm{BCD}_{\underline{\gamma}}(\underline{t}, \varphi') = (g_1, \dots, g_{i-1}, g_{i+1}^{g_i}, g_i, g_{i+2}, \dots, g_n).$$

Démonstration. Dans un premier temps, remarquons que :

$$\begin{aligned}
\varphi'(\gamma'_j) &= \varphi'(\mathrm{T}\sigma_i(\gamma_{\psi^{-1}(j)})) \\
&= (\varphi \circ \mathrm{T}\sigma_i^{-1})(\mathrm{T}\sigma_i(\gamma_{\psi^{-1}(j)}))) \\
&= \varphi(\gamma_{\psi^{-1}(j)}) \\
&= g_{\psi^{-1}(j)}.
\end{aligned}$$

Maintenant, distinguons les différents cas :

— Si j n'est égal ni à i ni à $i+1$, alors :

$$\varphi'(\gamma_j) = \varphi'(\gamma'_j) = g_j.$$

— Si maintenant $j = i+1$, alors :

$$\varphi'(\gamma_{i+1}) = \varphi'(\gamma'_{i+1}) = g_i.$$

— Enfin, considérons le cas $j = i$:

$$\begin{aligned}
\varphi'(\gamma_i) &= \varphi'\left((\gamma'_i)^{\gamma'_{i+1}}\right) \\
&= \varphi'\left(\gamma'_{i+1}\right)\varphi'\left(\gamma'_i\right)\varphi'\left((\gamma'_{i+1})^{-1}\right) \\
&= g_i g_{i+1} g_i^{-1} \\
&= (g_{i+1})^{g_i}.
\end{aligned}$$

Ceci conclut la preuve. □

Proposition: *Action du groupe des tresses sur les n-uplets*

Proposition 3.3.6. *La formule suivante induit une action du groupe des tresses d'Artin B_n sur les n-uplets d'éléments de G :*

$$\sigma_i.(g_1, \dots, g_n) = \left(g_1, \dots, g_{i-1}, (g_{i+1})^{g_i}, g_i, g_{i+2}, \dots, g_n\right).$$

La preuve de la proposition 3.3.6 consiste à vérifier que cette définition est compatible avec les relations qui définissent le groupe des tresses d'Artin (Définition 2.4.1). On désigne par $\sim$ la relation d'équivalence entre uplets de même taille n (sans préciser la taille) correspondant aux orbites sous l'action de B_n de la proposition 3.3.6.

3.3.2. **Description combinatoire des composantes des espaces de Hurwitz**

De la sous-section 3.3.1, et notamment de la proposition 3.3.5, on déduit que deux G-revêtements marqués ramifiés en $\underline{t} \in \mathrm{Conf}_{n,X}$ sont reliés par un chemin dans $\mathrm{Hur}^*_X(G,n)$ si et seulement si leurs descriptions des cycles de branchement pour un même bouquet $\underline{\gamma}$ sont dans une même orbite pour l'action du groupe des tresses d'Artin B_n de la proposition 3.3.6. Puisque $\mathrm{Conf}_{n,X}$ est connexe (voir la proposition 2.3.5), toute composante connexe de $\mathrm{Hur}^*_X(G,n)$ contient un G-revêtement de la forme $(\underline{t},\varphi)$. On en déduit le résultat suivant :

Théorème: *Description combinatoire des composantes connexes de l'espace de Hurwitz* $\mathrm{Hur}^*_X(G,n)$

Théorème 3.3.7. *Les composantes connexes de* $\mathrm{Hur}^*_X(G,n)$ *admettent la description combinatoire suivante :*

(i) Les composantes connexes de l'espace de Hurwitz $\mathrm{Hur}^*_{\mathbb{A}^1(\mathbb{C})}(G,n)$ *sont en bijection avec les orbites des n-uplets de G sous l'action du groupe des tresses d'Artin* B_n.

(ii) Les composantes connexes de l'espace de Hurwitz $\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(G,n)$ *sont en bijection avec les orbites des n-uplets $\underline{g} \in G^n$ dont le produit $\pi\underline{g}$ vaut 1 sous l'action du groupe des tresses d'Artin* B_n.

Proposition: *Invariants principaux (taille, produit, groupe, multidiscriminant) sous l'action des tresses*

Proposition 3.3.8. *Soit un n-uplet $\underline{g} \in G^n$. Les objets suivants, associés à $\underline{g}$, sont invariants sous l'action des tresses :*

(i) La taille $\left|\underline{g}\right| = n$ *du n-uplet.*

(ii) Le produit $\pi\underline{g} = g_1 g_2 \dots g_n$ *du n-uplet.*

(iii) Le groupe $H = \left\langle \underline{g} \right\rangle = \langle g_1, g_2, \dots, g_n \rangle$ *du n-uplet.*

(iv) Le (H',c)-multidiscriminant du uplet, pour tout sous-groupe H' de G contenant H et tout sous-ensemble c de H', invariant par conjugaison et contenant les g_i.

De plus, toute permutation des classes de conjugaison de H' figurant parmi les éléments de $\underline{g}$ est réalisable par une tresse.

Démonstration. L'invariance de la taille va de soi. L'invariance du produit découle de l'observation suivante :

$$g_i g_{i+1} = \left(g_{i+1}^{g_i}\right) g_i.$$

De même, l'invariance du groupe engendré résulte de :

$$\langle g_i, g_{i+1} \rangle = \left\langle g_{i+1}^{g_i}, g_i \right\rangle.$$

Au niveau des classes de conjugaison de H', remplacer (g_i, g_{i+1}) par $\left(g_{i+1}^{g_i}, g_i\right)$ a pour seul effet de permuter deux classes de conjugaison adjacentes, ce qui est sans effet sur le (H',c)-multidiscriminant. Puisque les transpositions de classes adjacentes sont réalisables et que les transpositions de la forme $(i, i+1)$ engendrent $\mathfrak{S}_n$, toute permutation des classes de conjugaison est réalisable par une tresse. □

La proposition 3.3.8 a pour conséquence que la taille, le produit, le groupe de monodromie et le H-multidiscriminant d'une composante connexe des espaces de Hurwitz $\mathrm{Hur}^*_X(G,n)$ sont des notions bien définies. On étend l'utilisation des symboles $|x|$, $\pi(x)$, $\langle x \rangle$ et $\mu_{H,c}(x)$ lorsque x est une B_n-orbite de n-uplets d'éléments de G ou une composante d'un espace de Hurwitz de G-revêtements marqués.

Remarque 3.3.9. On donne quelques variantes du théorème 3.3.7 pour d'autres espaces de Hurwitz :

— Les composantes connexes de $\mathrm{PHur}^*_X(G,n)$ sont en bijection avec les orbites des n-uplets de G (de produit 1 dans le cas $X=\mathbb{P}^1(\mathbb{C})$) sous l'action du groupe des tresses pures d'Artin PB_n.

— Les composantes connexes de $\mathrm{CHur}^*_X(G,n)$ sont en bijection avec les orbites des n-uplets de G (de produit 1 dans le cas $X=\mathbb{P}^1(\mathbb{C})$) qui engendrent G, sous l'action du groupe des tresses d'Artin B_n.

— Les composantes connexes de $\mathrm{Hur}_X(G,n)$ sont en bijection avec les orbites des n-uplets de G (de produit 1 dans le cas $X=\mathbb{P}^1(\mathbb{C})$) sous l'action du produit direct $G\times \mathrm{B}_n$, définie de la façon suivante :

$$(g,\sigma).\underline{g}=\sigma.(\underline{g}^g)=(\sigma.\underline{g})^g.$$

Autrement dit, ce sont des n-uplets d'éléments de G considérés à la fois modulo l'action des tresses et modulo l'action de conjugaison de G.

— Les composantes connexes de $\mathrm{Hur}^*_X(G,D,\xi)$ sont en bijection avec les orbites des n-uplets de G (de produit 1 dans le cas $X=\mathbb{P}^1(\mathbb{C})$) contenant $\xi(c)$ éléments de chaque $c\in D$, sous l'action du groupe des tresses pures d'Artin PB_n.

Dans le cas des composantes connexes de $\mathrm{Hur}_X(G,n)$, le produit et le groupe de monodromie ne sont définis qu'à conjugaison près ; parmi les multidiscriminants, seul le G-multidiscriminant est toujours bien défini.

Remarque 3.3.10. L'action du groupe des tresses sur les bouquets est transitive (voir [DE06]). Ainsi, alors que la description des cycles de branchement $\underline{g}$ d'un G-revêtement marqué dépend du choix d'un bouquet, l'orbite du uplet $\underline{g}$ sous l'action du groupe des tresses (qui représente une composante connexe d'un espace de Hurwitz) est la même quel que soit le bouquet. Cela entraîne qu'il existe une bijection *canonique* entre les B_n-orbites de n-uplets d'éléments de G (de produit 1 dans le cas $X=\mathbb{P}^1(\mathbb{C})$) et les composantes connexes de l'espace de Hurwitz $\mathrm{Hur}^*_X(G,n)$.

3.3.3. **Quelques propriétés de l'action du groupe des tresses**

Nous énonçons et démontrons ici quelques propriétés de l'action du groupe des tresses d'Artin B_n sur les n-uplets d'éléments de G, et de la relation d'équivalence $\sim$ qui correspond aux orbites (voir la proposition 3.3.6). Ces propriétés nous seront fréquemment utiles tout au long de ce travail.

Proposition: *Propriétés de l'action du groupe des tresses sur les uplets*

Proposition 3.3.11. *La relation d'équivalence $\sim$ vérifie les propriétés suivantes :*

(i) Si $\underline{g}_1\sim\underline{g}_2$ et $\underline{g}'_1\sim\underline{g}'_2$, alors :

$$\underline{g}_1\underline{g}'_1\sim\underline{g}_2\underline{g}'_2.$$

Ainsi, la concaténation des uplets est compatible avec la relation d'équivalence $\sim$.

(ii) Soit deux uplets $\underline{g}$ et $\underline{g}'$ d'éléments de G. On a les équivalences suivantes :

$$\underline{g}\underline{g}'\sim\left(\underline{g}'\right)^{\pi_{\underline{g}}}\underline{g}\sim\underline{g}'\underline{g}^{(\pi_{\underline{g}'})^{-1}}.$$

(iii) Soit deux uplets $\underline{g}, \underline{g}'$ d'éléments de G. Si $\pi\underline{g} = 1$, alors :

$$\underline{g}\underline{g}' \sim \underline{g}'\underline{g}.$$

On peut déplacer les sous-uplets de produit 1 librement en utilisant des tresses.

(iv) Soit $\underline{g}$ un uplet d'éléments de G satisfaisant $\pi\underline{g} = 1$. Alors :

$$(g_1, g_2, \dots, g_n) \sim (g_2, g_3, \dots, g_n, g_1).$$

On peut permuter circulairement les éléments d'un uplet de produit 1 en utilisant des tresses.

(v) Soit $\underline{g}$ un uplet d'éléments de G satisfaisant $\pi\underline{g} = 1$, et soit h un élément de $\left\langle \underline{g} \right\rangle$. Alors :

$$\underline{g} \sim \underline{g}^h.$$

On peut conjuguer les uplets de produit 1 par des éléments de leur groupe en utilisant des tresses.

(vi) Soit trois uplets $\underline{g}, \underline{g}', \underline{g}''$ d'éléments de G avec $\pi\underline{g}' = 1$. Soit $H_1 = \left\langle \underline{g}, \underline{g}'' \right\rangle$ et $H_2 = \left\langle \underline{g}' \right\rangle$. Alors, pour tout γ qui se trouve soit dans H_1 soit dans H_2, on a :

$$\underline{g}\underline{g}'\underline{g}'' \sim \underline{g}(\underline{g}')^\gamma \underline{g}''.$$

La proposition 3.3.11 (iv) est démontrée dans [Cau12, Lemme 2.8, p.564], et la proposition 3.3.11 (vi) dans [Cau12, Lemme 2.11, p.567].

Démonstration. (i) Soit $n = \left|\underline{g}_1\right| = \left|\underline{g}_2\right|$ et $n' = \left|\underline{g}'_1\right| = \left|\underline{g}'_2\right|$. Soit $\sigma_{a(1)} \cdots \sigma_{a(N_1)} \in \mathrm{B}_n$ une tresse envoyant $\underline{g}_1$ sur $\underline{g}_2$ et $\sigma_{b(1)} \cdots \sigma_{b(N_2)} \in \mathrm{B}_{n'}$ une tresse envoyant $\underline{g}'_1$ sur $\underline{g}'_2$. Alors la tresse suivante envoie $\underline{g}_1\underline{g}'_1$ sur $\underline{g}_2\underline{g}'_2$:

$$\left(\sigma_{b(1)+n} \cdots \sigma_{b(N_2)+n}\right)\left(\sigma_{a(1)} \cdots \sigma_{a(N_1)}\right).$$

(ii) La première équivalence découle du calcul suivant :

$$\begin{aligned}
\underline{g}\underline{g}' &= (g_1, \dots, g_n, g'_1, g'_2, \dots, g'_{n'}) \\
&\sim (g_1, \dots, g_{n-1}, (g'_1)^{g_n}, (g'_2)^{g_n}, \dots, (g'_{n'})^{g_n}, g_n) \\
&\sim (g_1, \dots, g_{n-2}, (g'_1)^{g_{n-1}g_n}, (g'_2)^{g_{n-1}g_n}, \dots, (g'_{n'})^{g_{n-1}g_n}, g_{n-1}, g_n) \\
&\sim \dots \\
&\sim ((g'_1)^{g_1 g_2 \cdots g_n}, (g'_2)^{g_1 g_2 \cdots g_n}, \dots, (g'_{n'})^{g_1 g_2 \cdots g_n}, g_1, g_2, \dots, g_n) \\
&= \left(\underline{g}'\right)^{\pi\underline{g}} \underline{g}.
\end{aligned}$$

La seconde équivalence découle de la première de la façon suivante :

$$\underline{g}'\underline{g}^{(\pi\underline{g}')^{-1}} \sim \left(\underline{g}^{(\pi\underline{g}')^{-1}}\right)^{(\pi\underline{g}')} \underline{g}' = \underline{g}^{(\pi\underline{g})(\pi\underline{g}')^{-1}}\underline{g}' = \underline{g}\underline{g}'.$$

(iii) Découle directement du point (ii).

(iv) Puisque $g_1 g_2 \dots g_n = 1$, nous avons $g_2 g_3 \dots g_n = g_1^{-1}$. Ainsi :

$$\begin{aligned}
(g_1, g_2, \dots, g_n) &\sim \left(g_2, g_3, \dots, g_n, g_1^{(g_2 g_3 \cdots g_n)^{-1}}\right) \\
&= \left(g_2, g_3, \dots, g_n, g_1^{g_1}\right) \\
&= (g_2, g_3, \dots, g_n, g_1).
\end{aligned}$$

(v) Puisque les éléments g_i engendrent H et que $H^{g_i} = H$, il suffit de montrer le résultat lorsque h est un des générateurs g_i. On a :

$$\underline{g} = (g_1, \dots, g_{i-1}, g_i, g_{i+1}, \dots, g_n) \sim (g_1, \dots, g_{i-1}, g_{i+1}^{g_i}, g_{i+2}^{g_i}, \dots, g_n^{g_i}, g_i).$$

Puisque le uplet est de produit 1, on applique le point (iv) pour le permuter circulairement :

$$\begin{aligned}\underline{g} &\sim (g_i, g_1, \dots, g_{i-1}, g_{i+1}^{g_i}, g_{i+2}^{g_i}, \dots, g_n^{g_i}) \\ &\sim (g_1^{g_i}, \dots, g_{i-1}^{g_i}, g_i, g_{i+1}^{g_i}, g_{i+2}^{g_i}, \dots, g_n^{g_i}) \\ &= (g_1^{g_i}, \dots, g_{i-1}^{g_i}, g_i^{g_i}, g_{i+1}^{g_i}, g_{i+2}^{g_i}, \dots, g_n^{g_i}) \\ &= \underline{g}^{g_i}.\end{aligned}$$

Ceci conclut la preuve.

(vi) Si γ est dans H_2, cela suit directement des points (i) et (v). On traite donc le cas $\gamma \in H_1$. Il suffit de traiter le cas des générateurs g_i et g_i''. Les deux cas étant identiques, on fait le calcul dans le cas $\gamma = g_i$:

$$\begin{aligned}\underline{g}\underline{g}'\underline{g}'' &= (g_1, \dots, g_{i-1}, g_i, g_{i+1}, \dots g_n, \underline{g}', \underline{g}'') \\ &\sim (g_1, \dots, g_{i-1}, g_i, \underline{g}', g_{i+1}, \dots, g_n, \underline{g}'') \\ &\sim (g_1, \dots, g_{i-1}, (\underline{g}')^{g_i}, g_i, g_{i+1}, \dots, g_n, \underline{g}'') \\ &\sim (g_1, \dots, g_{i-1}, g_i, g_{i+1}, \dots g_n, (\underline{g}')^{g_i}, \underline{g}'') \\ &= \underline{g}(\underline{g}')^{g_i}\underline{g}''.\end{aligned}$$

On a utilisé le fait que $\pi(\underline{g}') = \pi\left((\underline{g}')^{g_i}\right) = 1$ pour déplacer ces sous-uplets librement, en vertu du point (iii).

□

Remarque 3.3.12. Le proposition 3.3.11 (v) a la conséquence suivante : lorsqu'on regarde des composantes de G-revêtements connexes, la distinction entre composantes de G-revêtements marqués et G-revêtements non-marqués est inutile. En effet, l'action de conjugaison de $\mathrm{Inn}(G)$ est déjà « comprise » dans l'action des tresses sur les composantes de groupe G : deux marquages différents d'un même G-revêtement connexe sont toujours dans la même composante connexe de $\mathrm{Hur}_X^*(G, n)$.

3.4. Monoïdes et anneaux des composantes

3.4.1. **Le monoïde des composantes**

Il résulte de la proposition 3.3.11 (i) que l'opération de recollement définie dans la sous-section 2.4.2 induit une opération au niveau des composantes des espaces de Hurwitz : on peut donc « recoller » une composante connexe de $\mathrm{Hur}_X^*(G, n)$ afin d'obtenir une composante connexe de $\mathrm{Hur}_X^*(G, n')$ en une composante de $\mathrm{Hur}_X^*(G, n + n')$ lorsque $X = \mathbb{A}^1(\mathbb{C})$ ou $X = \mathbb{P}^1(\mathbb{C})$. Cela permet de définir une structure de monoïde gradué sur l'ensemble gradué suivant :

$$\bigsqcup_{n \geq 0} \pi_0 \mathrm{Hur}_X^*(G, n).$$

On en donne plutôt une définition combinatoire :

Définition 3.4.1. Le *monoïde des composantes* $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$ est le monoïde gradué dont les éléments de degré n sont les B_n-orbites de n-uplets d'éléments de G, et dont la loi de composition est induite par la concaténation.

Définition:
Monoïde des composantes de G-revêtements (marqués, ramifiés) de $\mathbb{A}^1(\mathbb{C})$

L'élément neutre de ce monoïde est l'orbite du 0-uplet, qui correspond à la composante du revêtement trivial (non-ramifié) $|G| \times \mathbb{A}^1(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C})$.

D'après le théorème 3.3.7 (i), les éléments de degré n de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$ sont en bijection avec les composantes connexes de $\mathrm{Hur}^*_{\mathbb{A}^1(\mathbb{C})}(G,n)$. Pour cette raison, nous appellerons ces éléments des *composantes*.

Remarque 3.4.2. On donne une présentation différente de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$: il s'agit du monoïde engendré par les 1-uplets (g) pour chaque élément $g \in G$, soumis aux relations correspondant aux tresses élémentaires :

$$(g)(h) = (h^g)(g) \text{ pour tous } g,h \in G.$$

Remarque 3.4.3. Le *degré* d'une composante est son degré comme élément du monoïde gradué des composantes. Dans le cas de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$, il s'agit du nombre de points de branchement des G-revêtements que la composante contient, c'est-à-dire la taille des uplets la représentant. C'est aussi sa dimension complexe (ou la moitié de la dimension réelle) puisque $\mathrm{Hur}^*_X(G,n)$ est un revêtement fini de l'espace de configurations $\mathrm{Conf}_{n,\mathbb{A}^1(\mathbb{C})}$ (voir la remarque 3.2.6). On n'utilisera jamais le mot « degré » pour parler du degré des revêtements contenus dans la composante (qui est toujours $|G|$) ou du degré de la composante vue comme sous-variété.

D'après la proposition 3.3.8 (ii), le produit $\pi(x)$ d'un élément $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$ est un élément de G bien défini. Puisqu'on a de plus l'égalité $\pi(\underline{gg'}) = (\pi\underline{g})(\pi\underline{g'})$, le produit définit un morphisme de monoïdes :

$$\pi : \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G) \to G.$$

Définition 3.4.4. Le *monoïde des composantes* $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$ est le noyau du morphisme π. C'est le sous-monoïde gradué de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$ dont les éléments de degré n sont les B_n-orbites de n-uplets $\underline{g} \in G^n$ satisfaisant $\pi\underline{g} = 1$, avec le produit induit par la concaténation.

Définition:
Monoïde des composantes de G-revêtements (marqués, ramifiés) de $\mathbb{P}^1(\mathbb{C})$

Le théorème 3.3.7 (ii) entraîne que les éléments de degré n de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$ sont en bijection avec les composantes connexes de l'espace de Hurwitz $\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(G,n)$, ce qui justifie la notation.

Remarque 3.4.5. On ne peut pas définir de la même manière un monoïde des composantes de G-revêtements non-marqués. Il manque en effet un équivalent de la proposition 3.3.11 (i) pour l'action de conjugaison par G. Donnons un exemple : si $G = \mathfrak{S}_3$, alors les uplets $\underline{g} = ((12),(12))$ et $\underline{g'} = ((13),(13))$ sont conjugués par l'élément $(23) \in G$ et représentent donc la même composante de $\mathrm{Hur}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_3,2)$, mais les concaténations $\underline{gg'} = ((12),(12),(13),(13))$ et $\underline{g'}\underline{g'} = ((13),(13),(13),(13))$ ne sont pas équivalentes puisque leurs groupes ne sont pas identiques. Un ersatz sera présenté dans la sous-section 3.4.5 : on définit un *anneau* des composantes de G-revêtements non-marqués.

De la proposition 3.3.11 (iii), on déduit directement la proposition suivante :

Proposition 3.4.6. *Le monoïde des composantes* $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$ *est un sous-monoïde central de* $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$*. En particulier, c'est un monoïde commutatif.*

Proposition: *Commutativité de* $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$

Remarque 3.4.7. En termes de G-revêtements (et non de composantes d'espaces de Hurwitz), la proposition 3.4.6 est un résultat de commutativité *à homotopie près* (pour l'opération de recollement), où les homotopies sont les chemins dans les espaces de Hurwitz. Voir les choses de cette manière au lieu de quotienter par l'action des tresses permet d'étudier l'homologie supérieure des espaces de Hurwitz[4]. Une forme plus concrète de cette remarque est l'utilisation des *quantum shuffle algebras* dans l'article [ETW17].

Remarque: *Pour les G-revêtements de $\mathbb{P}^1(\mathbb{C})$, l'opération de recollement est commutative à homotopie près*

[4] En 2007, Ellenberg utilisait l'expression « moralement incorrect » (*morally wrong*) dans son article de blog *Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and Malle's conjecture for function fields*, pour désigner cette opération de quotientage.

Fait 3.4.8. Les monoïdes des composantes $\mathrm{Comp}_X(G)$ ne sont en général pas simplifiables. Donnons un exemple. On prend $G = \mathfrak{S}_3$ et on considère les deux uplets $\underline{g} = ((12),(12))$ et $\underline{g}' = ((13),(13))$. Ils ne sont pas équivalents sous l'action des tresses puisque leurs groupes sont différents. On pose $\underline{g}'' = ((23),(23))$. En appliquant le proposition 3.3.11 (vi), on obtient :

$$\underline{g}\underline{g}'' \sim \underline{g}^{(23)}\underline{g}'' = \underline{g}'\underline{g}''.$$

Le monoïde des composantes $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_3)$ n'est donc pas simplifiable. Cependant, on énonce une forme faible de simplifiabilité dans le théorème 3.4.39 : lorsque les classes de conjugaison qui apparaissent dans les uplets y apparaissent assez souvent, le monoïde des composantes se comporte « comme un groupe ».

Soit H un sous-groupe de G et c un sous-ensemble de H invariant par conjugaison. On note D^* l'ensemble des classes de conjugaison de H contenues dans c.

Définition 3.4.9. On définit les sous-monoïdes suivants de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$:

Définition: *Monoïde des composantes à monodromie dans c*

— $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(H,c)$ est le sous-monoïde de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$ constitué des B_n-orbites de uplets d'éléments de c.[5]

— $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(H,c)$ est l'intersection de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(H,c)$ et de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$.

[5] Cela est bien défini car les tresses élémentaires ne font que permuter les éléments du uplet et les conjuguer par des éléments de H, ce qui conserve la propriété d'appartenir ou non à c.

Il découle de la proposition 3.3.8 (iv) que le (H,c)-multidiscriminant des uplets, au sens de la définition 1.4.6, induit un morphisme de monoïdes, pour $X \in \{\mathbb{A}^1(\mathbb{C}), \mathbb{P}^1(\mathbb{C})\}$:

$$\mu_{H,c} : \mathrm{Comp}_X(H,c) \to \mathbb{Z}^{D^*}. \tag{3.4.1}$$

On donne encore une autre variante de la définition du monoïde des composantes, qui généralise les cas précédents :

Définition 3.4.10. Soit D un ensemble de sous-ensembles de G deux à deux disjoints et invariants par conjugaison, et soit ξ une application $D \to \{1,2,\dots\}$. Le *monoïde des composantes* $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,D,\xi)$ est le monoïde gradué dont les éléments de degré n sont les $\mathrm{B}_{n|\xi|}$-orbites de $n\,|\xi|$-uplets d'éléments de G tels que $n\xi(\gamma)$ de ces éléments appartiennent à γ pour chaque $\gamma \in D$, et dont la multiplication provient de la concaténation. En tant qu'ensemble, $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,D,\xi)$ est donc :

Définition: *Monoïde des composantes avec des contraintes sur les classes de monodromie*

$$\bigsqcup_{n\geq 0} \left\{ (g_1,\dots,g_{n|\xi|}) \;\middle|\; |\{i \in \{1,\dots,n\,|\xi|\} \mid g_i \in \gamma\}| = n\xi(\gamma) \text{ pour tout } \gamma \in D \right\} \Big/ \mathrm{B}_{n|\xi|}.$$

Le *monoïde des composantes* $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G,D,\xi)$ est défini de la même façon en ne considérant que les uplets dont le produit vaut 1.

Les éléments de degré n de $\mathrm{Comp}_X(G, D, \xi)$ sont en bijection avec les composantes connexes de $\mathrm{Hur}^*_X(G, D, n\xi)$. On insiste sur le fait que le degré d'un élément de $\mathrm{Comp}_X(G, D, \xi)$ ne correspond au nombre de points de branchement des G-revêtements de la composante correspondante qu'à un facteur $|\xi|$ près.

On retrouve les constructions précédentes comme cas particuliers. En effet, pour $X = \mathbb{A}^1(\mathbb{C})$ ou $X = \mathbb{P}^1(\mathbb{C})$:

— $\mathrm{Comp}_X(G)$ correspond au cas $D = \{G\}$, $\xi(G) = 1$.

— $\mathrm{Comp}_X(H, c)$ correspond au cas $D = \{c\}$, $\xi(c) = 1$.

Remarque: *Fonctorialité du monoïde des composantes*

Remarque 3.4.11. Dans l'esprit de la sous-section 3.2.5, on remarque que $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}$ et $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}$ définissent des foncteurs de la catégorie **ConjInv** dans la catégorie des monoïdes (commutatifs dans le second cas).

3.4.2. L'anneau des composantes

On fixe un corps k de caractéristique première à l'ordre $|G|$ du groupe G. On définit désormais l'anneau des composantes, introduit par Ellenberg, Venkatesh et Westerland dans [EVW16] :

Définition: *Anneau des composantes*

Définition 3.4.12. L'*anneau des composantes* $R_{\mathbb{A}^1(\mathbb{C})}(G)$ est la k-algèbre graduée du monoïde $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$:

$$k[\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)].$$

Comme k-espace vectoriel, il s'agit de :

$$\bigoplus_{n\geq 0} H_0(\mathrm{Hur}^*_{\mathbb{A}^1(\mathbb{C})}(G, n), k)$$

dont les éléments sont des sommes formelles (à coefficients dans k) de composantes connexes d'espaces de Hurwitz de G-revêtements marqués ramifiés de $\mathbb{A}^1(\mathbb{C})$. La multiplication de cette algèbre est induite par l'opération de recollement. On définit de même les anneaux de composantes $R_{\mathbb{P}^1(\mathbb{C})}(G)$, $R_{\mathbb{A}^1(\mathbb{C})}(H, c)$, $R_{\mathbb{P}^1(\mathbb{C})}(H, c)$, $R_{\mathbb{A}^1(\mathbb{C})}(G, D, \xi)$ et $R_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$, comme étant les k-algèbres des monoïdes gradués correspondants.

Tous les anneaux des composantes de la forme $R_{\mathbb{P}^1(\mathbb{C})}(\cdots)$ sont des k-algèbres commutatives, en conséquence de la proposition 3.4.6. Cette propriété rend possible de considérer leur spectre du point de vue de la géométrie algébrique, ce qu'on fera dans le chapitre 5.

Fait: *Fonctorialité de l'anneau des composantes*

Fait 3.4.13. Là encore, $R_{\mathbb{A}^1(\mathbb{C})}$ et $R_{\mathbb{P}^1(\mathbb{C})}$ définissent des foncteurs de la catégorie **ConjInv** (voir la sous-section 3.2.5) dans la catégorie des k-algèbres (commutatives dans le second cas).

3.4.3. Les monoïdes et anneaux des composantes sont finiment engendrés

Définition: *Composante non-factorisable*

Définition 3.4.14. Une composante non-triviale $x \in \mathrm{Comp}_X(G, D, \xi)$ est *non-factorisable* elle n'est pas égale au produit de deux éléments non-triviaux de $\mathrm{Comp}_X(G, D, \xi)$.

La notion définie dans la définition 3.4.14 coïncide avec la notion usuelle d'élément irréductible d'un monoïde, mais nous évitons le terme ambigu « composante irréductible ». Une récurrence immédiate sur le degré des éléments de $\mathrm{Comp}_X(G, D, \xi)$ montre le fait suivant :

Lemme 3.4.15. *Tout élément de* $\mathrm{Comp}_X(G, D, \xi)$ *s'écrit comme un produit de composantes non-factorisables.*

Lemme: *Les composantes non-factorisables engendrent le monoïde des composantes*

Remarque 3.4.16. Si c est un sous-ensemble de G invariant par conjugaison et $g \in c$, l'élément de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$ représenté par le uplet suivant est non-factorisable :

$$(\underbrace{g, \dots, g}_{\mathrm{ord}(g)}).$$

Remarque: *Exemples de composantes non-factorisables*

En effet, l'action des tresses sur ce uplet est triviale[6]. Il suffit alors d'observer qu'aucun $(\underbrace{g, \dots, g}_{k})$ n'est de produit 1 pour $1 \leq k < \mathrm{ord}(g)$. En particulier, il y a toujours au moins $|c|$ éléments non-factorisables de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$. De plus, il y a équivalence entre les deux faits suivants :

[6] Ainsi, la composante correspondante est un revêtement de degré 1 de $\mathrm{Conf}_{n,\mathbb{P}^1(\mathbb{C})}$ – elle est donc homéomorphe à $\mathrm{Conf}_{n,\mathbb{P}^1(\mathbb{C})}$.

— Toutes les composantes non-factorisables de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$ ont même degré.

— Tous les éléments de c ont même ordre, qu'on note $\mathrm{ord}(c)$, et $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$ est engendré par les composantes de degré $\mathrm{ord}(c)$.

Quand $X = \mathbb{A}^1(\mathbb{C})$, les composantes non-factorisables se décrivent simplement : ce sont les éléments de degré 1 de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, D, \xi)$, dont le nombre est majoré par :

$$\prod_{c \in D} |c|^{\xi(c)}.$$

En particulier, ces composantes sont en nombre fini. Dans le cas $X = \mathbb{P}^1(\mathbb{C})$, un résultat analogue est donné par le lemme suivant :

Lemme 3.4.17. *Les composantes non-factorisables de* $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ *sont en nombre fini.*

Lemme: *Il y a un nombre fini de composantes non-factorisables*

Démonstration. On désigne par $c_1, \dots, c_r$ les éléments de D, qui sont des sous-ensembles disjoints de G invariants par conjugaison.

Soit $\underline{g}$ un uplet représentant un élément de degré n de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$. En utilisant des tresses pour permuter les classes de conjugaison, on se ramène à la situation où $\underline{g}$ est la concaténation de n « blocs » de la forme :

$$\left(g_{1,1}\,,\ \cdots\ ,\, g_{\xi(c_1),1}\,,\ \cdots\ ,\, g_{1,r}\,,\ \cdots\ ,\, g_{\xi(c_r),r}\right)$$

où $g_{i,j} \in c_j$. Bien sûr, ces blocs n'ont aucune raison d'être de produit 1 : on vient de décomposer $\underline{g}$ comme un produit d'éléments de degré 1 de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, D, \xi)$.

Soit A l'entier $\prod_{c \in D} |c|^{\xi(c)}$, qui majore le nombre de blocs de la forme ci-dessus. Supposons $n > \exp(G)A$. D'après le principe des tiroirs, l'un des blocs $\underline{h}$ apparaissant dans $\underline{g}$ apparaît au moins $\exp(G) + 1$ fois. En utilisant des tresses pour déplacer ces copies de $\underline{h}$ une à une vers la gauche du uplet, on montre que $\underline{g}$ est équivalent à un uplet de la forme :

$$\underline{h}^{\exp(G)} \left(\underline{h}\, \underline{g}'\right).$$

Le uplet $\underline{h}^{\exp(G)}$ est de produit $(\pi\underline{h})^{\exp(G)} = 1$ et de degré $\exp(G) > 0$. Le uplet $\underline{h}\, \underline{g}'$ est de degré ≥ 1, et il est aussi de produit 1 puisque :

$$\pi\left(\underline{h}\, \underline{g}'\right) = (\pi\underline{g}) \left(\pi\underline{h}^{\exp(G)}\right)^{-1} = 1.$$

Ainsi, l'élément de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ représenté par $\underline{g}$ est factorisable. On déduit de ce qui précède que les composantes non-factorisables sont de degré au plus $\exp(G)A$. Puisqu'il y a un nombre fini de composantes de chaque degré, il y a bien un nombre fini de composantes non-factorisables. □

Le lemme 3.4.15 et le lemme 3.4.17, ainsi que les remarques concernant le cas $X = \mathbb{A}^1(\mathbb{C})$, entraînent l'énoncé général :

Corollaire: *Les monoïdes et anneaux des composantes sont finiment engendrés*

Corollaire 3.4.18. *Les monoïdes des composantes sont finiment engendrés, et les anneaux des composantes sont des k-algèbres de type fini.*

Remarque: *Les monoïdes et anneaux des composantes pour $X = \mathbb{P}^1(\mathbb{C})$ sont finiment présentés*

Remarque 3.4.19. Un monoïde commutatif finiment engendré est nécessairement de présentation finie, ce qu'on montre en utilisant le lemme de Dickson. Cela entraîne qu'il existe une liste finie d'égalités entre éléments du monoïde $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$, envisagés comme mots sur l'alphabet des éléments non-factorisables, qui engendrent toutes les relations. Il suit aussi que $R_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ admet une présentation finie comme k-algèbre, ce qui découle aussi de la nœthérianité de $k[X_1, \ldots, X_N]$ où N est le nombre de composantes non-factorisables.

Remarque: *Les composantes non-factorisables n'ont pas nécessairement même degré*

Remarque 3.4.20. En général, les éléments non-factorisables du monoïde gradué $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ n'ont pas tous le même degré. Par exemple, si $G = \mathfrak{S}_4$ et si c est la classe de conjugaison des 3-cycles, alors les uplets suivants définissent des éléments non-factorisables de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$, de degrés 2 et 3 respectivement :

$$((123), (321)) \quad \text{et} \quad ((123), (123), (123)).$$

3.4.4. Idéaux et sous-anneaux remarquables dans les anneaux des composantes

Dans cette sous-section, on décrit quelques familles d'idéaux homogènes bilatères et de sous-anneaux de l'anneau des composantes $R_X(G, D, \xi)$. Les pendants géométriques de ces objets, dans le cas $X = \mathbb{P}^1(\mathbb{C})$, servent à la description du spectre de l'anneau des composantes qu'on entreprend dans le chapitre 5.

On suppose qu'aucun $\gamma \in D$ ne contient 1, de sorte qu'une composante de degré non nul ait toujours un groupe de monodromie non trivial.

Définition: *Idéal irrelevant*

Définition 3.4.21. L'*idéal irrelevant* ϖ est le sous-k-espace vectoriel gradué de $R_X(G, D, \xi)$ engendré par les composantes de degré non nul.

Proposition: *L'idéal irrelevant est maximal*

Proposition 3.4.22. *L'idéal ϖ est un idéal bilatère maximal de $R_X(G, D, \xi)$, dont le corps résiduel est k.*

Démonstration. Le sous-espace ϖ est bien un idéal bilatère. Tout élément de $R_X(G, D, \xi)$ peut se décomposer sous la forme $\lambda + x'$ pour une constante $\lambda \in k$ et un élément $x' \in \varpi$. Cette décomposition montre que $R_X(G, D, \xi)/\varpi$ est isomorphe au corps k. On en conclut que ϖ est un idéal maximal de corps résiduel k. □

Définition: *Familles remarquables d'idéaux bilatères et de sous-anneaux de l'anneau des composantes*

Définition 3.4.23. Soit H un sous-groupe de G. On définit les k-sous-espaces vectoriels gradués suivants de $R_X(G, D, \xi)$:

— I_H est engendré par les composantes dont le groupe de monodromie contient H.

— I_H^* est engendré par les composantes dont le groupe de monodromie contient H strictement.

— J_H est engendré par les composantes dont le groupe de monodromie n'est pas strictement contenu dans H.

— J_H^* est engendré par les composantes dont le groupe de monodromie n'est pas inclus dans H.

— R^H est engendré par les composantes dont le groupe de monodromie est inclus dans H.

Pour tout sous-groupe H et G, les sous-espaces I_H, I_H^*, J_H et J_H^* sont des idéaux bilatères homogènes de $R_X(G, D, \xi)$, et R^H est une sous-k-algèbre graduée de $R_X(G, D, \xi)$. Lorsque H a une intersection non-triviale avec chaque $\gamma \in D$, le sous-anneau R^H est lui-même un anneau des composantes : en effet, il est isomorphe à l'anneau des composantes $R_X(H, D_H, \xi_H)$ où $D_H = \{\gamma \cap H \mid \gamma \in D\}$ et $\xi_H : D_H \to \mathbb{Z}$ envoie $\gamma \cap H$ sur $\xi(\gamma)$ (ceci est bien défini).

Des sous-espaces similaires sont considérés dans [ETW17, subsection 6.5] : Les idéaux I_H et I_H^* apparaissent en tant que $F^{\geq H}R$ et $(\sum_{K>H} F^{\geq K}R)$ respectivement. Le sous-anneau R^H est également défini, et l'idéal J_H^* apparaît implicitement comme noyau de la surjection $\rho_H : R \to R^H$ (voir la proposition 3.4.26).

On rappelle que $\mathrm{Sub}_{G,D}$ est l'ensemble des sous-groupes D-engendrés de G, défini dans la définition 3.2.20.

Proposition: *Propriétés des espaces R^H, $I_H^{(*)}$ et $J_H^{(*)}$*

Proposition 3.4.24. *Les espaces définis dans la définition 3.4.23 satisfont les propriétés suivantes :*

(i) Pour tout sous-groupe H de G, on a les inclusions :

$$I_H^* \subseteq I_H \qquad I_H^* \subseteq J_H^*$$
$$I_H \subseteq J_H \qquad J_H^* \subseteq J_H.$$

Ces inclusions sont strictes si et seulement si $H \in \mathrm{Sub}_{G,D}$.

(ii) Une inclusion $H \subseteq H'$ entre sous-groupes de G donne lieu à une inclusion dans le même sens entre les sous-algèbres associées :

$$R^H \subseteq R^{H'},$$

et des inclusions dans le sens opposé entre les idéaux associés :

$$I_{H'} \subseteq I_H \qquad I_{H'}^* \subseteq I_H^*$$
$$J_{H'} \subseteq J_H \qquad J_{H'}^* \subseteq J_H^*.$$

(iii) Les idéaux I_1 et J_1, ainsi que le sous-anneau R^G, sont égaux à l'anneau des composantes $R_X(G, D, \xi)$ tout entier.
Les idéaux I_1^* et J_1^* sont égaux à l'idéal irrelevant ϖ.
Le sous-anneau R^1 est égal au corps k.
Les idéaux I_G^* et J_G^* sont égaux à l'idéal nul.

(iv) Pour tout sous-groupe H de G, on a les égalités :

$$I_H^* = I_H \cap J_H^* \qquad\qquad J_H = I_H + J_H^*.$$

(v) Pour tout sous-groupe H de G, on a les égalités :

$$I_H^* = \sum_{\substack{H' \supsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} I_{H'} \qquad\qquad J_H = \bigcap_{\substack{H' \subsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} J_{H'}^*.$$

(vi) Pour tous sous-groupes H_1 et H_2 de G, on a les égalités :

$$I_{\langle H_1, H_2 \rangle} = I_{H_1} \cap I_{H_2} \qquad\qquad J_{H_1 \cap H_2}^* = J_{H_1}^* + J_{H_2}^*.$$

Démonstration. Les preuves de ces propriétés étant des vérifications directes, on passe rapidement dessus.

(i) Les inclusions résultent de la définition. Le fait que les inclusions soient strictes si et seulement $H \in \mathrm{Sub}_{G,D}$ résulte de la proposition 3.2.22.

(ii) et (iii) Résultent de la définition.

(iv)(a) Les éléments de $I_H \cap J_H^*$ sont les combinaisons linéaires de composantes dont le groupe est plus grand que H et n'est pas contenu dans H – c'est-à-dire que leur groupe est strictement plus grand que H. On retrouve la définition de I_H^*.

(b) Les éléments de $I_H + J_H^*$ sont les combinaisons linéaires de composantes dont le groupe est soit non inclus dans H (donc, strictement plus grand que H ou non-comparable avec H), soit plus grand que H (ce qui ne rajoute que H). On retrouve exactement les éléments de J_H.

(v)(a) Les éléments de I_H^* sont les combinaisons linéaires de composantes dont le groupe H'' contient strictement H. Il est équivalent de demander que H'' contienne un sous-groupe H' qui contienne strictement H : cela démontre l'égalité.

(b) Pour J_H: Les éléments de J_H sont les combinaisons linéaires de composantes dont le groupe H'' n'est pas strictement inclus H. Il est équivalent de demander que H'' ne soit pas inclus dans un sous-groupe H' qui soit strictement inclus dans H : cela démontre l'égalité.

(vi) Les égalités proviennent respectivement des faits suivants :

(a) un sous-groupe de G contient $\langle H_1, H_2 \rangle$ si et seulement s'il contient à la fois H_1 et H_2,

(b) un sous-groupe de G est inclus dans $H_1 \cap H_2$ si et seulement s'il est inclus à la fois dans H_1 et dans H_2.

□

Proposition: *Générateurs de J_H^**

Proposition 3.4.25. *L'idéal bilatère J_H^* est égal à l'idéal bilatère engendré par les composantes non-factorisables dont le groupe n'est pas inclus dans H.*

Démonstration. L'idéal J_H^* est engendré par les composantes dont le groupe n'est pas inclus dans H. Soit x une telle composante. En la décomposant comme un produit de composantes non-factorisables $x_1 \cdots x_r$, il apparaît qu'au moins un des sous-groupes $\langle x_i \rangle$ doit ne pas être inclus dans H, sans quoi $\langle x \rangle = \langle x_1, \ldots, x_r \rangle$ serait inclus dans H.

□

Proposition: *Le sous-anneau R^H est aussi un quotient*

Proposition 3.4.26. *Le sous-anneau R^H de $R_X(G,D,\xi)$ est isomorphe au quotient $R_X(G,D,\xi)/J_H^*$.*

Démonstration. Cela découle du fait qu'un élément $x \in R_X(G,D,\xi)$ se décompose de manière unique comme somme d'un élément de R^H et d'un élément de J_H^* : pour le premier élément, on ne garde que les termes correspondant à des composantes dont le groupe est inclus dans H, et on met les autres termes dans le second élément. □

3.4.5. Un anneau des composantes de G-revêtements non-marqués

Cette sous-section est une ouverture, et ne sert pas dans le reste du texte. On explore brièvement l'idée de la définition d'un anneau des composantes des espaces de Hurwitz de G-revêtements non-marqués. Il résulte des observations de la remarque 3.4.5 qu'on ne peut pas définir « naïvement » un anneau des composantes dont les éléments seraient des sommes à coefficients dans k de composantes connexes de $\bigsqcup_n \mathrm{Hur}_X(G,D,n\xi)$. En effet, l'opération de recollement est mal définie. Une manière de contourner cette difficulté est de ne pas considérer le H_0 de l'espace topologique quotient :

$$\mathrm{Hur}_X(G,D,n\xi) = \mathrm{Hur}_X^*(G,D,n\xi)/\mathrm{Inn}(G),$$

mais de considérer l'homologie (en degré 0) de l'orbifold correspondant, en d'autres mots l'homologie $\mathrm{Inn}(G)$-équivariante de $\bigsqcup_n \mathrm{Hur}_X^*(G,D,n\xi)$. Cela motive la définition suivante :

Définition: *Anneau des composantes de revêtements non-marqués*

Définition 3.4.27. L'*anneau des composantes de G-revêtements non-marqués*, qu'on note $R_X(G,D,\xi)^{\mathrm{Inn}(G)}$, est le sous-anneau de $R_X(G,D,\xi)$ formé des éléments invariants sous l'action de conjugaison de $\mathrm{Inn}(G)$.

Considérons une composante connexe de $\mathrm{Hur}_X(G,D,n\xi)$. Elle correspond à l'orbite, sous les actions simultanées du groupe des tresses et de $\mathrm{Inn}(G)$, d'un uplet $\underline{g}$. L'élément suivant, qui est $\mathrm{Inn}(G)$-équivariant, ne dépend pas du choix de $\underline{g}$:

$$\underline{g}^+ \stackrel{\mathrm{def}}{=} \sum_{h\in G} (g_1,\dots,g_n)^h.$$

Fait: *Base de $R_X(G,D,\xi)^{\mathrm{Inn}(G)}$*

Fait 3.4.28. Le k-espace vectoriel $R_X(G,D,\xi)^{\mathrm{Inn}(G)}$ admet comme base l'ensemble des éléments de la forme $\underline{g}^+$ pour des uplets $\underline{g}$ d'éléments de G (de produit 1 si $X = \mathbb{P}^1(\mathbb{C})$, et contenant $n\xi(\gamma)$ éléments de chaque $\gamma \in D$ pour un certain n). En effet, si un terme λm pour $m \in \mathrm{Comp}_X(G,D,\xi)$ apparaît dans un élément de $R_X(G,D,\xi)^{\mathrm{Inn}(G)}$, alors tous les λm^h pour $h \in G$ doivent apparaître dans la somme. En notant G_m le sous-groupe des éléments $h \in G$ tels que $m^h = m$, la somme doit donc contenir le terme $\sum_{h\in G/G_m} m^h$, qui est aussi :

$$\frac{1}{|G_m|}\sum_{h\in G} m^h = \frac{1}{|G_m|} m^+.$$

Notons qu'il est crucial à cet endroit que $|G|$ soit premier avec la caractéristique de k pour pouvoir effectuer la division par $|G_m|$.

La dimension du k-espace vectoriel des éléments de degré n de l'anneau gradué $R_X(G,D,\xi)^{\mathrm{Inn}(G)}$ est égale au nombre de composantes connexes de l'espace de

Hurwitz $\mathrm{Hur}_X(G, D, n\xi)$. En ce sens, $R_X(G, D, \xi)^{\mathrm{Inn}(G)}$ est bien un anneau des composantes de G-revêtements non-marqués.

La proposition 3.4.29 ci-dessous (qui n'a d'intérêt que si $X = \mathbb{P}^1(\mathbb{C})$) est généralisée par [Bia22, Lemma 4.31], où la conjugaison dans le groupe G est remplacée par un *quandle* quelconque :

Proposition: *Les éléments G-invariants de l'anneau des composantes sont centraux*

Proposition 3.4.29. *L'anneau $R_X(G, D, \xi)^{\mathrm{Inn}(G)}$ est un sous-anneau central de $R_X(G, D, \xi)$.*

Démonstration. Il suffit de démontrer que les éléments de la forme $\underline{g}^+$ commutent avec les éléments de la forme $\underline{g}'$.

$$\begin{aligned}
\underline{g}^+\underline{g}' &= \sum_{h\in G} \underline{g}^h\underline{g}' \\
&= \sum_{h\in G} \underline{g}' \left(\underline{g}^h\right)^{\left(\pi\underline{g}'\right)^{-1}} && \text{par la proposition 3.3.11 (ii)} \\
&= \underline{g}' \left(\sum_{h\in G} \underline{g}^{\left(\pi\underline{g}'\right)^{-1}h}\right) \\
&= \underline{g}' \left(\sum_{h'\in G} \underline{g}^{h'}\right) \\
&= \underline{g}'\underline{g}^+.
\end{aligned}$$

□

Il faut faire attention au fait que cet « anneau des composantes » n'est pas finiment engendré en général.

Remarque 3.4.30. La définition 3.4.27 est un exemple de situation dans laquelle le fait d'avoir à disposition un *anneau* des composantes est crucial : la définition n'a aucun équivalent dans le monoïde $\mathrm{Comp}_X(G, D, \xi)$. C'est aussi une illustration de l'importance de l'hypothèse sur la caractéristique de k. En effet, si $\underline{g}$ est un uplet de groupe G, alors la proposition 3.3.11 (v) entraîne :

$$\underline{g}^+ = \sum_{h\in G} \underline{g}^h = \sum_{h\in G} \underline{g} = |G|\,\underline{g}$$

ce qui est de peu d'intérêt lorsque $|G| = 0$ dans k.

3.4.6. **Quelques propriétés additionnelles du multidiscriminant**

Soit c un sous-ensemble de G invariant par conjugaison et D^* l'ensemble des classes de conjugaison de G incluses dans c.

Fait 3.4.31. Si on connaît le (G, c)-multidiscriminant $\psi \in \mathbb{Z}^{D^*}$ d'un uplet $\underline{g}$ dont les éléments appartiennent à c, on peut retrouver la taille du uplet en utilisant la formule :

$$\left|\underline{g}\right| = \sum_{\gamma\in D^*} \psi(\gamma).$$

On peut également retrouver, à partir du (G, c)-multidiscriminant ψ d'un uplet $\underline{g}$, la projection dans l'abélianisé G^{ab} du produit $\pi\underline{g} \in G$. Pour cela, on définit un morphisme de groupes $\widetilde{\pi} : \mathbb{Z}^{D^*} \to G^{\mathrm{ab}}$:

Définition: *Le morphisme $\widetilde{\pi}$*

Définition 3.4.32. Si $\psi \in \mathbb{Z}^{D^*}$, on définit l'élément $\widetilde{\pi}(\psi) \in G^{\mathrm{ab}}$ de la façon suivante :

$$\widetilde{\pi}(\psi) \stackrel{\text{def}}{=} \prod_{\gamma \in D^*} (\widetilde{\gamma})^{\psi(\gamma)}$$

où $\widetilde{\gamma}$ désigne l'image commune dans G^{ab} de tous les éléments d'une même classe de conjugaison $\gamma \in D^*$. L'application $\widetilde{\pi}$ définit un morphisme de groupes :

$$\widetilde{\pi} : \mathbb{Z}^{D^*} \to G^{\mathrm{ab}}.$$

On a alors la propriété suivante :

Proposition: *Calcul de l'image de $\pi\underline{g}$ dans G^{ab} à partir du multidiscriminant*

Proposition 3.4.33. *Si ψ est le (G,c)-multidiscriminant d'un uplet $\underline{g}$ d'éléments de c, alors $\widetilde{\pi}(\psi)$ est la projection dans G^{ab} de $\pi\underline{g}$.*

3.4.6.1. Lien entre les différents multidiscriminants. Soit H un sous-groupe de G. On note $c_H = c \cap H$ et D_H^* l'ensemble des classes de conjugaison de H contenues dans l'ensemble c_H, qui est invariant par conjugaison.

Puisque deux éléments conjugués dans H sont aussi conjugués dans G, il existe une unique application $\xi_{H\to G} : D_H^* \to D^*$ telle que pour tout $\gamma \in D_H^*$, la classe $\gamma \in D_H^*$ soit incluse dans la classe $\xi_{H\to G}(\gamma) \in D^*$.

Définition: *Le morphisme $\iota_{H'}^{H}$*

Définition 3.4.34. On définit un morphisme de groupes :

$$\iota_G^H : \mathbb{Z}^{D_H^*} \to \mathbb{Z}^{D^*}$$

par la formule suivante, pour une application $\psi : D_H^* \to \mathbb{Z}$ et une classe de conjugaison $\gamma \in D^*$:

$$\iota_G^H(\psi)(\gamma) = \sum_{\gamma' \in \xi_{H\to G}^{-1}(\gamma)} \psi(\gamma').$$

Fait 3.4.35. Si H, H' sont deux sous-groupes de G tels que $H \subseteq H'$, alors $\iota_G^{H'} \circ \iota_{H'}^{H} = \iota_G^H$.

Proposition: *Le morphisme ι_G^H fait le lien entre les différents multidiscriminants*

Proposition 3.4.36. *Pour tout n-uplet $\underline{g}$ d'éléments de c_H, nous avons l'égalité:*

$$\mu_{G,c}(\underline{g}) = \left(\iota_G^H \circ \mu_{H,c_H}\right)(\underline{g}).$$

Démonstration. Soit $\gamma \in D^*$ une classe de conjugaison de G. Alors $\gamma \cap H$ est un sous-ensemble de H invariant par conjugaison. Notons $d_1, \ldots, d_\sigma$ les classes de conjugaison de H qui constituent $\gamma \cap H$. Ainsi, l'ensemble $\xi_{H\to G}^{-1}(\gamma)$ est égal à $\{d_1, \ldots, d_\sigma\}$.

Considérons un uplet $\underline{g}$ d'éléments de c_H. On a :

$$\iota_G^H\left(\mu_{H,c_H}(\underline{g})\right)(\gamma) = \sum_{i=1}^{\sigma} \mu_{H,c_H}(\underline{g})(d_i).$$

Le membre de droite est le nombre d'éléments du uplet $\underline{g}$ qui appartiennent à $\bigsqcup d_i$, c'est-à-dire à $\gamma \cap H$. Puisque les éléments du uplet $\underline{g}$ sont dans H, c'est aussi le nombre d'éléments du uplet $\underline{g}$ qui se trouvent dans γ, et ce nombre est $\mu_{G,c}(\underline{g})(\gamma)$ par définition. On obtient ainsi l'égalité souhaitée :

$$\iota_G^H(\mu_{H,c_H}(\underline{g}))(\gamma) = \mu_{G,c}(\underline{g})(\gamma).$$

□

La proposition 3.4.36 peut se réécrire sous forme d'un diagramme commutatif de monoïdes :

$$\begin{array}{ccc} \mathrm{Comp}(G,c) & \xrightarrow{\mu_{G,c}} & \mathbb{Z}^{D^*} \\ \subseteq\uparrow & & \uparrow \iota_G^H \\ \mathrm{Comp}(H,c_H) & \xrightarrow[\mu_{H,c_H}]{} & \mathbb{Z}^{D_H^*} \end{array}$$

Ainsi, le (G,c)-multidiscriminant d'une composante se déduit de son (H,c_H)-multidiscriminant lorsque tous deux sont définis. Cela entraîne que, parmi les multidiscriminants, l'invariant le plus fin est le $\left\langle \underline{g} \right\rangle$-multidiscriminant.

Le fait que le G-multidiscriminant soit d'autant moins précis que les groupes de monodromie des composantes sont petits est une manifestation du phénomène de *délitement* des classes de conjugaison (*splitting* en anglais), dont nous parlons dans la section 4.2 et qui sera au centre du chapitre 4 : si l'on ne contraint que le G-multidiscriminant d'un uplet de groupe H (comme on le fait dans la définition 3.2.15) nous perdons le contrôle des classes de conjugaison de H qui apparaissent lorsque les classes de conjugaison de G se délitent en plusieurs classes de conjugaison dans le sous-groupe H.

3.4.7. Le *lifting invariant* d'Ellenberg, Venkatesh et Westerland

Dans cette section, nous donnons une définition du lifting invariant des composantes des espaces de Hurwitz, introduit dans [EVW12] suivant des idées de [Fri95], et nous citons certaines de ses propriétés. On suit essentiellement l'article [Woo21], qui est une présentation claire et concise de cet invariant, et qui contient les preuves des faits énoncés ici.

3.4.7.1. Présentation de l'invariant. Soit c un sous-ensemble invariant par conjugaison du groupe G, qui engendre G. Soit D^* l'ensemble des classes de conjugaison de G qui sont incluses dans c. On trouve dans [EVW12 ; Woo21] la définition du groupe suivant :

Définition 3.4.37. Le groupe $U(G,c)$ est engendré par des générateurs $[g]$ pour chaque élément $g \in c$, sujets aux relations $[h^g][g] = [g][h]$ pour tous $g,h \in c$.

Une comparaison avec la remarque 3.4.2 montre que $U(G,c)$ est le groupe de Grothendieck du monoïde des composantes $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c)$. Autrement dit, on peut voir ses éléments comme des uplets d'éléments de c, modulo l'action des tresses, mais auxquels on rajoute des « inverses formels » (on peut même n'ajouter l'inverse que d'une composante particulière, voir [EVW12, Theorem 7.5.1]). Notamment, la formule $(g_1,\dots,g_n) \mapsto [g_1]\cdots[g_n]$ définit un morphisme de monoïdes :

$$\Pi_{G,c} : \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c) \to U(G,c).$$

Définition:
Le lifting invariant

Définition 3.4.38. Le (G,c)-*lifting invariant* de la composante $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c)$ est son image par le morphisme $\Pi_{G,c}$, qui est un élément du groupe $U(G,c)$. Si on ne précise pas G et c dans la notation, le *lifting invariant* $\Pi(x)$ d'une composante $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$ est son (H,c)-lifting invariant où $H = \langle x \rangle$, et c est l'union des classes de conjugaison de H représentées dans x.

On a défini un invariant des uplets modulo l'action des tresses, qui prend ses valeurs dans un groupe. D'après la propriété universelle du groupe de Grothendieck, tout morphisme de monoïdes de $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c)$ dans un groupe doit se factoriser par $U(G,c)$: le lifting invariant est le plus fin parmi les invariants multiplicatifs des composantes à valeurs dans un groupe. Les deux exemples suivants sont notables :

— Le morphisme « produit » $\pi : \mathrm{Comp}(G,c) \to G$ (voir la sous-section 3.4.1) se factorise par un morphisme de groupes, qu'on note aussi π, de $U(G,c)$ dans G. En termes de générateurs, ce morphisme $\pi : U(G,c) \to G$ est induit par la formule $\pi([g]) = g$. On a, pour tout $x \in \mathrm{Comp}(G,c)$:

$$\pi(x) = \pi(\Pi_{G,c}(x)).$$

— Le (G,c)-multidiscriminant $\mu_{G,c} : \mathrm{Comp}(G,c) \to \mathbb{Z}^{D^*}$ (voir l'équation (3.4.1)) se factorise par un morphisme de groupes, qu'on note aussi $\mu_{G,c}$, de $U(G,c)$ dans $\mathbb{Z}^{D^*}$. En termes de générateurs, ce morphisme est induit par la formule :

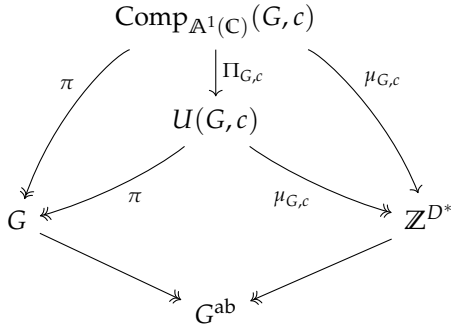
$$\mu_{G,c}([g])(\gamma) = \begin{cases} 1 & \text{si } g \in \gamma \\ 0 & \text{sinon} \end{cases}.$$

On a, pour tout $x \in \mathrm{Comp}(G,c)$:

$$\mu_{G,c}(x) = \mu_{G,c}(\Pi_{G,c}(x)).$$

Ainsi, le (G,c)-lifting invariant est un invariant plus fin que le (G,c)-multidiscriminant.

On peut résumer les liens existant entre les différents morphismes, de groupes ou de monoïdes, par le diagramme suivant :



où le morphisme $\widetilde{\pi} : \mathbb{Z}^{D^*} \to G^{\mathrm{ab}}$ est celui de la définition 3.4.32.

Le monoïde des composantes $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c)$ n'étant pas simplifiable en général (voir le fait 3.4.8), le morphisme $\Pi_{G,c}$ n'est généralement pas injectif. Nous énonçons désormais le théorème 3.4.39. Ce théorème offre une solution partielle au problème de la simplifiabilité : quand on le restreint aux orbites de uplets de groupe G dans lesquels toutes les classes de conjugaison $\gamma \in D^*$ apparaissent suffisamment souvent, le morphisme $\Pi_{G,c}$ est injectif. Il s'agit d'une forme plus générale d'un résultat dû à Conway et Parker : ce résultat, qui est présenté dans [FV91, Appendix], est le théorème 3.4.39 dans le cas particulier où le groupe $H_2(G,c)$ (défini dans la définition 3.4.44) est trivial. La preuve de ce théorème est donnée dans [Woo21] et dans [EVW12], ce théorème est nommé *Geometric Branch-Generation Theorem* (ou théorème de Conway-Fried-Parker-Völklein) par Fried[7]. On introduit d'abord quelques notations : pour tout élément $\psi \in \mathbb{Z}^{D^*}$, on pose $|\psi| = \sum_{\gamma \in D^*} \psi(\gamma)$ et $\min(\psi) = \min_{\gamma \in D^*}(\psi(\gamma))$.

[7] Pour la présentation qu'en fait Fried, on peut consulter son site : `https://www.math.uci.edu/~mfried/deflist-cov/CFPV-Thm.html#BG-Thm:`

Théorème 3.4.39. *Il existe un entier $M_{G,c}$ tel que pour toute application $\psi : D^* \to \mathbb{Z}$ satisfaisant $\min(\psi) \geq M_{G,c}$, le morphisme $\Pi_{G,c}$ induise une bijection entre les deux ensembles suivants :*

— *D'une part, l'ensemble des éléments $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c)$ satisfaisant $\mu_{G,c}(x) = \psi$ et $\langle x \rangle = G$.*

— *D'autre part, l'ensemble des éléments $x \in U(G,c)$ satisfaisant $\mu_{G,c}(x) = \psi$.*

On peut écrire cette bijection un peu différemment :

$$\left\{ \underline{g} \in G^{|\psi|} \;\middle|\; \begin{array}{c} \left\langle \underline{g} \right\rangle = G \\ \forall i,\, g_i \in c \\ \mu_{G,c}(\underline{g}) = \psi \end{array} \right\} \Big/ \mathrm{B}_{|\psi|} \xrightarrow{\sim} \{ x \in U(G,c) \mid \mu_{G,c}(x) = \psi \}.$$

Théorème:
Le (G,c)-lifting invariant caractérise uniquement les composantes avec un « gros » multidiscriminant. [Woo21, Theorem 3.1], [EVW12, Theorem 7.6.1]

Définition 3.4.40. Soit $M \in \mathbb{N}$ un entier. Une composante $x \in \mathrm{Comp}(G)$ est *M-vaste* si toutes les classes de conjugaison de $\langle x \rangle$ qui apparaissent dans x apparaissent au moins M fois.

Définition:
Composante M-vaste

Remarque 3.4.41. En prenant la valeur maximale de l'entier $M_{H,c}$ du théorème 3.4.39, prise sur les couples (H,c) où H est un sous-groupe de G et c est un sous-ensemble de H invariant par conjugaison qui engendre H, on obtient une unique constante M, qui ne dépend que du groupe G, telle que toute composante M-vaste (au sens de la définition 3.4.40) est déterminée par son lifting invariant (au sens de la définition 3.4.38).

3.4.7.2. Lifting invariant des composantes de produit 1. On note $U_1(G,c)$ le noyau du morphisme $\pi : U(G,c) \to G$.

Proposition 3.4.42. *Le sous-groupe normal $U_1(G,c) = \ker(\pi)$ est central dans $U(G,c)$. En particulier, c'est un groupe abélien.*

Proposition:
Centralité de $U_1(G,c)$

Démonstration. Soit x un élément du groupe $U_1(G,c)$. On le décompose comme $[g_1]^{\varepsilon_1} \cdots [g_n]^{\varepsilon_n}$ avec $g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n} = 1$ et $\varepsilon_i \in \{-1,1\}$. Soit alors $[h]$ un des générateurs de $U(G,c)$. On a :

$$\begin{aligned} x[h] &= [g_1]^{\varepsilon_1} \cdots [g_{n-1}]^{\varepsilon_{n-1}} [g_n]^{\varepsilon_n} [h] \\ &= [g_1]^{\varepsilon_1} \cdots [g_{n-1}]^{\varepsilon_{n-1}} [h^{g_n^{\varepsilon_n}}] [g_n]^{\varepsilon_n} \\ &= [h^{g_1^{\varepsilon_1} \cdots g_n^{\varepsilon_n}}] [g_1]^{\varepsilon_1} \cdots [g_{n-1}]^{\varepsilon_{n-1}} [g_n]^{\varepsilon_n} \\ &= [h] x. \end{aligned}$$

Ainsi, x commute avec les générateurs de $U(G,c)$. Cela montre que $U_1(G,c)$ est un sous-groupe central de $U(G,c)$. □

Par restriction et corestriction, le (G,c)-lifting invariant induit un morphisme de monoïdes commutatifs, qu'on note toujours $\Pi_{G,c}$, de $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G,c)$ dans $U_1(G,c)$. Le groupe abélien $U_1(G,c)$ est le groupe de Grothendieck du monoïde commutatif $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G,c)$.

Le (G,c)-lifting invariant d'une composante $x \in \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G,c)$ ne dépend que de la composante de G-revêtements *non-marqués* obtenue en oubliant les points marqués des revêtements appartenant à x. C'est une conséquence de la proposition suivante :

Proposition: *Le* lifting invariant *est invariant sur les* $\mathrm{Inn}(G)$*-orbites*

Proposition 3.4.43. *Si* $\gamma \in G$ *et* $x \in \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G,c)$*, alors* $\Pi_{G,c}(x) = \Pi_{G,c}(x^\gamma)$.

Démonstration. Puisque c engendre G, on choisit des éléments $\gamma_1, \dots, \gamma_n \in c$ tels que $\gamma_1 \cdots \gamma_n = \gamma$. Dans $U(G,c)$, on a alors les égalités :

$$\begin{aligned}[\gamma_1]\cdots[\gamma_n]\Pi_{G,c}(x) &= [\gamma_1]\cdots[\gamma_{n-1}]\Pi_{G,c}(x^{\gamma_n})[\gamma_n] \\ &= \Pi_{G,c}(x^{\gamma_1\cdots\gamma_n})[\gamma_1]\cdots[\gamma_n] \\ &= \Pi_{G,c}(x^{\gamma})[\gamma_1]\cdots[\gamma_n].\end{aligned}$$

D'après la proposition 3.4.42, l'élément $\Pi_{G,c}(x^\gamma) \in U_1(G,c)$ est central, et on peut donc annuler les facteurs $[\gamma_1]\cdots[\gamma_n]$ dans cette égalité. Ceci conclut la preuve. □

3.4.7.3. La description des groupes $U(G,c)$ et $U_1(G,c)$. Nous donnons à présent une description rapide du groupe $U(G,c)$. Les faits énoncés dans ce paragraphe sont démontrés dans [Woo21, Sous-section 2.1].

On commence par fixer une extension de Schur S de G, choisie arbitrairement (voir [Woo21] pour la définition). Il y a alors une suite exacte :

$$1 \to H_2(G,\mathbb{Z}) \to S \xrightarrow{p} G \to 1.$$

Notons $\pi(S)$ l'isomorphisme $H_2(G,\mathbb{Z}) \xrightarrow{\sim} \ker(S \to G)$ qui s'en déduit. Soit Q_c le sous-groupe normal de $H_2(G,\mathbb{Z})$ engendré par les antécédents, pour l'isomorphisme $\pi(S)$, des commutateurs $[\widehat{x},\widehat{y}]$ entre éléments de S dont les images dans G sont des éléments de c qui commutent l'un avec l'autre :

$$Q_c \overset{\text{def}}{=} \left\langle \Big(\pi(S)\Big)^{-1}\big([\widehat{x},\widehat{y}]\big) \;\middle|\; \begin{array}{c} p(\widehat{x}) \in c \\ p(\widehat{y}) \in c \\ p(\widehat{x})p(\widehat{y}) = p(\widehat{y})p(\widehat{x}) \end{array} \right\rangle.$$

Définition: *Le groupe* $H_2(G,c)$

Définition 3.4.44. Le groupe $H_2(G,c)$ est le quotient de $H_2(G,\mathbb{Z})$ par le sous-groupe normal Q_c.

Notons S_c le quotient de S par $\pi(S)(Q_c)$, que Wood nomme *extension de Schur réduite*. Nous avons la suite exacte :

$$1 \to H_2(G,c) \to S_c \to G \to 1.$$

Le résultat principal est [Woo21, Theorem 2.5] :

Théorème: *Description de* $U(G,c)$

Théorème 3.4.45. *Le groupe* $U(G,c)$ *est isomorphe au produit fibré suivant :*

$$U(G,c) \simeq S_c \underset{G^{ab}}{\times} \mathbb{Z}^{D^*}.$$

Le morphisme $U(G,c) \to \mathbb{Z}^{D^*}$ *correspond au* (G,c)*-multidiscriminant* $\mu_{G,c}$.

On en déduit le corollaire suivant :

Corollaire: *Description de* $U_1(G,c)$

Corollaire 3.4.46. *Le groupe* $U_1(G,c)$ *est isomorphe au produit direct de* $H_2(G,c)$ *et du noyau de* $\widetilde{\pi} : \mathbb{Z}^{D^*} \to G$ *:*

$$U_1(G,c) \simeq H_2(G,c) \times \ker(\widetilde{\pi}).$$

En particulier, le groupe $H_2(G,c) \simeq \ker\big(U_1(G,c) \to \ker(\widetilde{\pi})\big)$ ne dépend pas (à isomorphisme près) du choix de l'extension de Schur S.

3.5. Summary of the chapter in English

In this section, we summarize some of the content of Chapter 3 in English. The focus is on stating only key definitions and results which are used later in the text.

3.5.1. **Topological Hurwitz spaces, components and combinatorial description (Sections 3.2 and 3.3)**

We denote by $\mathrm{Hur}^*_X(G,n)$ the topological Hurwitz space of marked G-covers of (X,t_0), branched at a configuration $\underline{t} \in \mathrm{Conf}_{n,X}$ (Definition 3.2.4). The points of this space are isomorphism classes of branched marked G-covers of (X,t_0), unramified at t_0. The topology (Definition 3.2.2) is defined so that the map that takes a marked G-cover branched at $\underline{t}$ to the configuration $\underline{t}$ is a covering map $\mathrm{Hur}^*_X(G,n) \to \mathrm{Conf}_{n,X}$, whose fiber above some configuration $\underline{t} \in \mathrm{Conf}_{n,X}$ consists of isomorphism classes of marked G-covers of X branched at $\underline{t}$.

We introduce other Hurwitz spaces:

— $\mathrm{CHur}^*_X(G,n)$ is the Hurwitz space of *connected* G-covers of X (Definition 3.2.11). It is a subspace of $\mathrm{Hur}^*(G,n)$.

— $\mathrm{Hur}_X(G,n)$ (resp. $\mathrm{CHur}_X(G,n)$) is the Hurwitz space of unmarked (resp. unmarked and connected) G-covers of X (Definition 3.2.12). They are obtained as quotients of Hurwitz spaces of marked G-covers by the conjugation action of G.

— Let D be a set of disjoint conjugation-invariant non-empty subsets of G and ξ be a map $D \to \{0,1,\ldots\}$. The Hurwitz space $\mathrm{Hur}^*_X(G,D,\xi)$ is the Hurwitz space of marked G-covers of X such that each monodromy class γ belongs to some element of D, and such that for each element $\gamma \in D$, the conjugacy classes of G contained in γ are the monodromy classes at exactly $\xi(\gamma)$ branch points, collectively (Definition 3.2.15).

  We define similarly Hurwitz spaces $\mathrm{CHur}^*_X(G,D,\xi)$, $\mathrm{Hur}_X(G,D,\xi)$ and $\mathrm{CHur}_X(G,D,\xi)$.

Hurwitz spaces are generally not connected. One can determine whether two marked G-covers branched at a same configuration $\underline{t} \in \mathrm{Conf}_{n,X}$ are in the same connected component by looking at their branch cycle descriptions, which are n-tuples $\underline{g}, \underline{g}'$ of elements of G. Indeed, there is an action of the Artin braid group B_n on n-tuples of elements of G (Proposition 3.3.6) induced by the formula:

$$\sigma_i.(g_1,\ldots,g_n) \overset{\text{def}}{=} (g_1,\ldots,g_{i-1},(g_{i+1})^{g_i},g_i,g_{i+2},\ldots,g_n).$$

And the connected components of $\mathrm{Hur}^*_X(G,n)$ are in one-to-one correspondance with orbits, for this action, of n-tuples $\underline{g} \in G^n$, with the additional condition that $\pi\underline{g} = 1$ if $X = \mathbb{P}^1(\mathbb{C})$ (Theorem 3.3.7). We have analogous descriptions for connected components of other Hurwitz spaces (we do not include every situation):

— Connected components of $\mathrm{CHur}^*_X(G,n)$ correspond to braid group orbits of n-tuples $\underline{g} \in G^n$ such that $\left\langle \underline{g} \right\rangle = G$ (and $\pi\underline{g} = 1$ if $X = \mathbb{P}^1(\mathbb{C})$).

— Connected components of $\mathrm{Hur}_X(G,n)$ correspond to orbits of n-tuples $\underline{g} \in G^n$ (such that $\pi\underline{g} = 1$ if $X = \mathbb{P}^1(\mathbb{C})$) under the action of the direct product $\mathrm{Inn}(G) \times \mathrm{B}_n$.

— Connected components of $\mathrm{Hur}^*_X(G, D, \xi)$ correspond to braid group orbits of n-tuples $\underline{g} \in G^n$ (with $\pi\underline{g} = 1$ if $X = \mathbb{P}^1(\mathbb{C})$) such that every g_i belongs to some element of D, and each element $\gamma \in D$ contains exactly $\xi(\gamma)$ elements of the tuple $\underline{g}$.

The size (Definition 1.4.3), product (Definition 1.4.4), group (Definition 1.4.5) and multidiscriminant (Definition 1.4.6) of a tuple are invariant under the action of the braid group (Proposition 3.3.8). This means that these are well-defined invariants for components of Hurwitz spaces too: we extend the use of the notations $|x|$, $\pi(x)$ and $\langle x \rangle$ and $\mu_{H,c}(x)$.

Whereas the branch cycle description $\underline{g}$ of a cover depends on the choice of a bouquet, the braid group orbit of $\underline{g}$ does not: this is due to the fact that B_n acts transitively on topological bouquets up to conjugacy (Remark 3.3.10). Hence, the combinatorial description of connected components of Hurwitz spaces is a *canonical* bijection.

3.5.2. **Monoids and rings of components**

3.5.2.1. Monoids of components. Via the description of connected components of $\mathrm{Hur}^*_X(G, n)$ as B_n-orbits of n-tuples of elements of G, the concatenation of tuples induces a well-defined product operation on components of Hurwitz spaces:

$$(g_1, \dots, g_n)(g'_1, \dots, g'_{n'}) = (g_1, \dots, g_n, g'_1, \dots, g'_{n'}).$$

The *monoids of components* $\mathrm{Comp}_X(G)$ are defined in the following way:

$$\begin{aligned} \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G) &= \bigsqcup_{n\geq 0} G^n \,/_{\mathrm{B}_n}, \\ \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G) &= \bigsqcup_{n\geq 0} \left\{ \underline{g} \in G^n \;\middle|\; \pi\underline{g} = 1 \right\} /_{\mathrm{B}_n}, \end{aligned}$$

graded by the size n of a tuple, and equipped with the well-defined product operation induced by concatenation. Elements of degree n of $\mathrm{Comp}_X(G)$ are in bijection with connected components of $\mathrm{Hur}^*_X(G, n)$. The identity element of $\mathrm{Comp}_X(G)$ is the braid orbit of the empty tuple, i.e. the connected component of the trivial G-cover. The monoid $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$ is commutative and finitely generated. (Proposition 3.4.6 and Corollary 3.4.18)

We define similarly the following monoid of components:

— If H is a subgroup of G and c is a conjugation-invariant subset of H, then $\mathrm{Comp}_X(H, c)$ is the graded monoid of tuples of elements of c (of product 1 if $X = \mathbb{P}^1(\mathbb{C})$), with the product induced by concatenation (Definition 3.4.9).

— If D is a set of disjoint conjugation-invariant non-empty subsets of G, and ξ is a map $D \to \{1, 2, \dots\}$, then $\mathrm{Comp}_X(G, D, \xi)$ is the graded monoid whose elements of degree n are braid orbits of tuples of elements of $\left(\bigsqcup_{\gamma\in D} \gamma\right)$, such that $n\xi(\gamma)$ elements belong to each set $\gamma \in D$, with the product induced by concatenation (Definition 3.4.10).

We translate some of the properties of Proposition 3.3.11 (restated in terms of the monoids of components) in English, as they are used frequently:

Proposition 3.3.11 (iii) (translated). *The submonoid* $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$ *is central in*

Proposition 3.3.11 (iii) (translated)

$\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$. *Hence, one can move subtuples whose product is* 1 *freely using braids.*

Proposition 3.3.11 (v) (translated). *Let $x \in \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$ and $g \in \langle x \rangle$. Then $x = x^g$. Hence, one can conjugate tuples of product* 1 *by elements of their group using braids.*

Proposition 3.3.11 (v) (translated)

Proposition 3.3.11 (vi) (translated). *Let $x, y, z \in \mathrm{Comp}_{AC}(G)$ with $\pi(y) = 1$. For each g which belongs either to $\langle x, z \rangle$ or to $\langle y \rangle$, one has $xyz = xy^g z$.*

Proposition 3.3.11 (vi) (translated)

3.5.2.2. Rings of components. Let k be a field whose characteristic does not divide $|G|$. Following [EVW16], we define the rings of components $R_X(G)$, $R_X(H, c)$ and $R_X(G, D, \xi)$ as the monoid rings over k of the corresponding monoids of components (Definition 3.4.12) These rings of components are graded k-algebras of finite type, commutative when $X = \mathbb{P}^1(\mathbb{C})$. We define ideals and subrings of the ring $R_X(G, D, \xi)$, which are used in Chapter 5:

Definition 3.4.23 (translated). *Let H be a subgroup of G.*

Definition 3.4.23 (translated)

— *I_H is the two-sided homogeneous ideal of $R_X(G, D, \xi)$ generated by components whose monodromy group contains H.*

— *I_H^* is the two-sided homogeneous ideal of $R_X(G, D, \xi)$ generated by components whose monodromy group contains H strictly.*

— *J_H is the two-sided homogeneous ideal of $R_X(G, D, \xi)$ generated by components whose monodromy group is not strictly contained in H.*

— *J_H^* is the two-sided homogeneous ideal of $R_X(G, D, \xi)$ generated by components whose monodromy group is not contained in H.*

— *R^H is the subalgebra of $R_X(G, D, \xi)$ generated by components whose monodromy group is contained in H. This subalgebra is itself a ring of components, and it is isomorphic to the quotient algebra $R_X(G, D, \xi)/J_H^*$ (Proposition 3.4.26).*

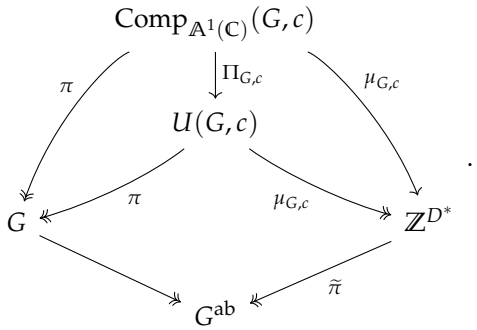
Properties of these subspaces are given in Proposition 3.4.24.

3.5.2.3. Lifting invariant. We review a lifting invariant introduced in [EVW12] based on ideas of [Fri95]. A clear and concise presentation of this invariant, which includes proofs for the facts stated here, may be found in [Woo21]. Let c be a conjugation-invariant subset of G that generates G, and let D^* be the set of all conjugacy classes of G which are contained in c. We let $U(G, c)$ be the Grothendieck group of $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, c)$, i.e. the group generated by generators $[g]$ for each $g \in c$, satisfying $[g][h] = [h^g][g]$ (Definition 3.4.37).

There is a morphism of monoids:

$$\Pi_{G,c} : \begin{cases} \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c) & \to & U(G,c) \\ (g_1,\dots,g_n) & \mapsto & [g_1]\cdots[g_n]. \end{cases}$$

The (G,c)-*lifting invariant* of a component $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c)$ is its image $\Pi_{G,c}(x) \in U(G,c)$. When (G,c) is not specified, the *lifting invariant* of a component $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G)$ is its (H,c)-lifting invariant where $H = \langle x \rangle$ and c is the smallest conjugation-invariant subset of H such that $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(H,c)$ (Definition 3.4.38). There are group morphisms $\pi : U(G,c) \to G$ (induced by $[g] \mapsto g$) and $\mu_{G,c} : U(G,c) \to \mathbb{Z}^{D^*}$ which let one recover the product and (G,c)-multidiscriminant of a component $x \in \mathrm{Comp}(G,c)$ based on its (G,c)-lifting invariant:



Here, $\widetilde{\pi} : \mathbb{Z}^{D^*} \to G^{\mathrm{ab}}$ is the group morphism defined on generators in the following way: the basis element of $\mathbb{Z}^{D^*}$ corresponding to a conjugacy class $\gamma \subseteq c$ is mapped to the well-defined image in G^{ab} of the elements of γ (Definition 3.4.32).

We denote by $U_1(G,c)$ the kernel of the product morphism $\pi : U(G,c) \to G$. The subgroup $U_1(G,c)$ is central in $U(G,c)$ (Proposition 3.4.42). The group $U_1(G,c)$ is the Grothendieck group of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G,c)$, and the lifting invariant defines a morphism of monoids:

$$\Pi_{G,c} : \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G,c) \to U_1(G,c).$$

The monoid of components $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c)$ is not cancellative in general (Fact 3.4.8), and thus $\Pi_{G,c}$ is generally not injective. The following theorem, which is [Woo21, Theorem 3.1] or [EVW12, Theorem 7.6.1], offers a partial solution.

Theorem 3.4.39 (translated). *There exists an integer $M_{G,c}$ such that for every map $\psi : D^* \to \mathbb{Z}$ satisfying $\min(\psi) \geq M_{G,c}$, the morphism $\Pi_{G,c}$ induces a bijection between the two following sets:*

Theorem 3.4.39 (translated)

— *On the one hand, the set of elements $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G,c)$ such that $\mu_{G,c}(x) = \psi$ and $\langle x \rangle = G$.*

— *On the other hand, the set of elements $x \in U(G,c)$ such that $\mu_{G,c}(x) = \psi$.*

A component $x \in \mathrm{Comp}(G)$ is *M-big* if it is represented by a tuple $\underline{g}$ such that every conjugacy class of $\left\langle \underline{g} \right\rangle$ which appears in the tuple appears at least M times (Definition 3.4.40). By taking the maximal value of $M_{H,c}$ over couples (H,c) where H

is a subgroup of G and c is a conjugation-invariant subset of H, one can choose an integer M depending only of the group G, such that the lifting invariant of an M-big component determines this component. (Remark 3.4.41)

Finally, we quickly describe the groups $U(G,c)$ and $U_1(G,c)$. Fix a Schur extension $S \twoheadrightarrow G$ (cf. [Woo21] for a definition). It fits in an exact sequence:

$$1 \to H_2(G,\mathbb{Z}) \to S \xrightarrow{p} G \to 1.$$

Let $\pi(S)$ be the isomorphism $H_2(G,\mathbb{Z}) \simeq \ker(S \to G)$. Let Q_c be the normal subgroup of $H_2(G,\mathbb{Z})$ generated by preimages under $\pi(S)$ of commutators $[\widehat{x},\widehat{y}]$ between elements of S whose images in G are commuting elements of c:

$$Q_c \overset{\text{def}}{=} \left\langle \Big(\pi(S)\Big)^{-1}\big([\widehat{x},\widehat{y}]\big) \;\middle|\; \begin{array}{c} p(\widehat{x}) \in c \\ p(\widehat{y}) \in c \\ p(\widehat{x})p(\widehat{y}) = p(\widehat{y})p(\widehat{x}) \end{array} \right\rangle.$$

Definition 3.4.44 (translated). *The group $H_2(G,c)$ is the quotient group $H_2(G,\mathbb{Z})/Q_c$.*

Definition 3.4.44 (translated)

Let S_c be the quotient group $S/\pi(S)(Q_c)$ (a *reduced Schur extension* in Wood's terminology). It fits in the exact sequence:

$$1 \to H_2(G,c) \to S_c \to G \to 1.$$

We can now state [Woo21, Theorem 2.5] and its corollary:

Theorem 3.4.45 (translated). *The group $U(G,c)$ is isomorphic to the following fibered product:*

$$U(G,c) \simeq S_c \underset{G^{ab}}{\times} \mathbb{Z}^{D^*}.$$

Theorem 3.4.45 (translated)

Corollary 3.4.46 (translated). *The group $U_1(G,c)$ is isomorphic to the following direct product:*

$$U_1(G,c) \simeq H_2(G,c) \times \ker(\widetilde{\pi}).$$

Corollary 3.4.46 (translated)

Chapitre 4

Counting Components of Hurwitz Spaces

Summary of the chapter

In this chapter, we estimate the number of connected components of the Hurwitz space $\mathrm{Hur}_X^*(G, D, n\zeta)$ (Definition 3.2.15) with a given monodromy group as $n \to \infty$ (Theorem 4.3.1).

The content of this chapter is largely taken from the preprint [Seg22].

Outline of the chapter

Une triste lumière arrose
Brusquement les cieux assombris :
Des oiseaux noirs, à larges cris,
Brisent du bec, dans la nuit close,
Le soleil, comme un grand œuf rose.

— A. Giraud,
Décor, in *Pierrot Lunaire*, 1898.

4.1. Introduction

4.1.1. Motivation and previous work

Let G be a finite group. An important question in number theory is to count Galois extensions of a field K whose Galois group is G, with additional conditions, e.g. on the discriminant or conductor. Several conjectures are of this type: the inverse Galois problem, the van der Waerden conjecture, the Cohen-Lenstra conjecture, the Malle conjecture, etc.

When $K = F(t)$ is a function field over a field F and the focus is on regular extensions of K, this question concerns geometrical objects: we are counting connected branched G-covers[1] of the projective line which are defined over the field F. Counting G-covers defined over F is related to counting F-points on *Hurwitz schemes*[2]: these moduli spaces classify G-covers of $\mathbb{P}^1$ with a fixed number of branch points and fixed ramification type. These ideas are detailed in [Fri77; FV91].

[1] i.e. Galois covers whose automorphism group is G, cf. Subsection 2.2.2 for a definition in the non-connected case.
[2] cf. Section 7.2

In [EVW16], Ellenberg, Venkatesh and Westerland introduce new techniques to count the $\mathbb{F}_q$-points of Hurwitz schemes, and apply these results to the Cohen-Lenstra conjecture over function fields over finite fields. Their techniques involve a graded algebra: the *ring of components*. Elements of this ring are formal sums of connected components of Hurwitz spaces, graded by the number of branch points of the covers they contain. The product is induced by the gluing operation of Definition 2.4.18: one may glue two covers with n (resp. n') branch points into a cover with $n + n'$ branch points. For more details about the monoids and rings of components, see Section 3.4.

Under some hypotheses, they construct a central homogeneous element U of the ring of components whose degree is positive, and such that multiplication by U has

finite-dimensional kernel and cokernel. It follows that the zeroth homology of certain Hurwitz spaces becomes $\deg(U)$-periodic for large numbers of branch points [EVW16, Lemma 3.5]. Using a variant of the Koszul complex, the authors then show that higher homology has a similar form of stability [EVW16, Theorem 6.1]. They then apply the Grothendieck-Lefschetz fixed-point theorem to count $\mathbb{F}_q$-points using topological data [EVW16, Theorem 8.8]. This lets them prove the validity of the Cohen-Lenstra heuristics for function fields [EVW16, Theorem 1.2].

Their work has been extended in various ways. For instance, in [Tie16], a *colored* version of Hurwitz spaces is defined and studied.

4.1.2. **Approach of this work**

The work of Ellenberg, Tran, Venkatesh and Westerland [EVW16; EVW12; ETW17] has made clear that the asymptotics of extensions of function fields were related to the asymptotics of the homology of Hurwitz spaces with large numbers of branch points. We study this question by obtaining asymptotical estimates of their zeroth homology.

The main differences between the approach of [EVW16] and ours are the following:

— In [EVW16], the ring of components is generated by components of Hurwitz moduli spaces of marked branched G-covers of the affine line, whereas we consider both marked branched G-covers of both the affine and projective lines. In the projective setting, the ring of components is a commutative k-algebra of finite type (Proposition 3.4.6, Corollary 3.4.18). In Chapter 5, we introduce and study the *spectrum of the ring of components* and relate its geometry to the results of this chapter.

— Let c be a conjugacy class of G which generates G. The results of [EVW16] depend on an assumption, the *non-splitting property*: the couple (G, c) is *non-splitting* if for every subgroup $H \subseteq G$ which intersects c, the subset $c \cap H$ consists of a single conjugacy class of H. In the situation of [EVW16], this hypothesis is satisfied.

  We are mostly interested in situations where this assumption does not hold. In Section 4.2, we introduce a quantitative version of that property, the *splitting number* (Definition 4.2.3), which vanishes exactly when the non-splitting property holds. We prove quantitative versions of some of the stabilization results of [EVW16] (see Theorem 4.3.1). We also systematically consider the case of multiple conjugacy classes.

4.1.3. **Outline of the chapter**

We briefly outline the contents of this chapter:

— In Section 4.2, we take a look at splitting phenomena and introduce the splitting number.

— In Section 4.3, we state our key results – notably Theorem 4.3.1, which sums up the results of later sections.

— In Section 4.4, we prove that the splitting number $\Omega(D_H)$ is the smallest exponent of a monomial which dominates the function of n which counts the components of $\mathrm{Hur}^*_X(G, D, n\xi)$ with monodromy group H (Theorem 4.4.2).

— In Section 4.5, we focus on the coefficient of the leading monomial of the same counting function. In particular situations, we are able to compute this leading coefficient using group-theoretical information (Proposition 4.5.2, Proposition 4.5.6 and Corollary 4.5.9).

Of course, counting connected components is not the whole story: one should also study higher homology.[3] Nevertheless, we feel like the phenomena which arise and the group-theoretic invariants which play a role in our count of connected components shed some light on the question. For example, the results of Section 4.4 compute the degree d in [ETW17, Theorem 7.7], and the results of Section 4.5 give information about the function $r(n)$ in the same article.

Disclaimer: Some of the results of this chapter, which have been made public in [Seg22], have since been rediscovered and/or improved in [ETW23] and [BM23].

[3] Each connected component, represented by a tuple $\underline{g}$, is weakly homotopy equivalent to the Eilenberg-Maclane space $K(\pi, 1)$ where π is the subgroup of the Artin braid group B_n which stabilizes $\underline{g}$. This means that the higher homology is given by group homology of subgroups of braid groups.

4.2. Splitting phenomena and the splitting number

In this section, we take a look at splitting phenomena and at their role in our counting problem. We introduce some terminology which helps describing these phenomena, notably the splitting number.

Let D be a set of disjoint conjugation-invariant subsets of G and ξ be a map $D \to \{1, 2, \dots\}$. The notation that follows is used frequently:

Definition 4.2.1. If H is a group that intersects all elements $\gamma \in D$ nontrivially, then we let:

$$D_H \stackrel{\text{def}}{=} \{\gamma \cap H \,|\, \gamma \in D\}.$$

The map that takes an element $\gamma \cap H \in D_H$ to the unique $\gamma \in D$ which contains it defines a bijection $\beta_H : D_H \xrightarrow{\sim} D$. We let $\xi_H \stackrel{\text{def}}{=} \xi \circ \beta_H$.

4.2.1. Non-connected covers and the non-splitting property

One can see a morphism $\pi_1(X \setminus \underline{t}) \to G$ as a surjective morphism into its image $H \subseteq G$. This leads to the useful homeomorphism:

$$\mathrm{Hur}^*_X(G, D, n\xi) = \bigsqcup_{H \subseteq G} \mathrm{CHur}^*_X(G, D_H, n\xi_H). \tag{4.2.1}$$

When $X = \mathbb{A}^1(\mathbb{C})$ or $X = \mathbb{P}^1(\mathbb{C})$, the union can be taken over all $H \in \mathrm{Sub}_{G,D}$ (cf. Definition 3.2.20) instead, as a consequence of Proposition 3.2.22. Assume D consists of conjugacy classes of G. If H is a subgroup of G, then the conjugation-invariant subset D_H does not necessarily consist of conjugacy classes. Hence, the multidiscriminant of G-covers in $\mathrm{Hur}^*_X(G, D, n\xi)$ is generally more constrained for connected G-covers than for G-covers of monodromy group H. This is due to the fact that a conjugacy class may split into multiple classes when intersected with H. In [EVW16], this issue is addressed by assuming the *non-splitting property* ([EVW16, Definition 3.1]). We give a slightly generalized version of this property (the original statement concerns a single conjugacy class):

Definition: *Non-splitting property*

Definition 4.2.2. Assume D consists of conjugacy classes of G. The couple (G, D) is *non-splitting* if the conjugacy classes $\gamma \in D$ generate G (collectively), and if for every D-generated subgroup $H \subseteq G$, the set D_H consists of conjugacy classes of H.

If (G, D) is non-splitting, points of $\mathrm{Hur}_X^*(G, D, n)$ with monodromy group H correspond to points of $\mathrm{CHur}_X^*(H, D_H, n)$; thus, their monodromy classes are completely determined. This fact is used crucially in [EVW16] to prove results concerning all G-covers by proving them for connected G-covers.

We introduce a quantitative version of the non-splitting property:

Definition: *Splitting number*

Definition 4.2.3. Let D be a set of disjoint non-empty conjugation-invariant subsets of G. Let c be the union of the subsets $\gamma \in D$ and $H = \langle c \rangle$ be the subgroup of G generated by the elements of c. Let D^* be the set of conjugacy classes of H contained in c. The *splitting number* $\Omega(D)$ is the nonnegative integer $|D^*| - |D|$.

When D consists of conjugacy classes of G which together generate G, the non-splitting property for (G, D) is equivalent to requiring $\Omega(D_H) = 0$ for all D-generated subgroups H, where D_H is defined as in Definition 4.2.1.

Finally, we introduce some terminology to speak about splitting phenomena:

Definition: *Terminology for splitting*

Definition 4.2.4.— If γ is a conjugacy class of G and H is a subgroup of G, we say that H *splits* γ if $\gamma \cap H$ is not a conjugacy class in H.

— Let D be a set of conjugacy classes of G. A subgroup H of G is a *splitter* (where D is clear from the context) if it splits some class $\gamma \in D$. Otherwise, H is a *non-splitter*.

The non-splitting property for the couple (G, D) (Definition 4.2.2) asks that all D-generated subgroups be non-splitters. This can also be understood using the morphism ι_G^H from Definition 3.4.34:

Proposition 4.2.5. *Let H be a D-generated subgroup of G. The morphism ι_G^H from Definition 3.4.34 is an isomorphism if and only if H is a non-splitter.*

4.2.2. Examples of non-splitters

In this subsection, we describe situations where the non-splitting property holds. The following lemma gives a condition under which we can ensure that a subgroup splits no conjugacy class:

Lemma 4.2.6. *If N is a normal subgroup of G with no outer automorphisms and γ is a conjugacy class of G which intersects N nontrivially, then N does not split γ.*

Proof. Consider elements $g, g' \in \gamma \cap N$. There exists $h \in G$ such that $g' = g^h$. Conjugation by h defines an automorphism of N since N is normal, and this automorphism is inner because N has no outer automorphisms. Thus there exists $h' \in N$ such that $n^h = n^{h'}$ for all $n \in N$. In particular, we have $g' = g^{h'}$ and thus g and g' are conjugate in N. This shows that $\gamma \cap N$ is a conjugacy class in N. □

The hypothesis of Lemma 4.2.6 is very strong. We give another instance where the non-splitting property is satisfied. It relies on the following definition:

Definition: *Antirational element*

Definition 4.2.7. An element $g \in G$ of order n is *antirational* if g is not conjugate to any g^k for $k \in \{2, \dots, n-1\}$.

Note that any involution is antirational. The existence of antirational elements is related to the non-splitting property by the following lemma, which generalizes [EVW16, Lemma 3.2]:

Lemma: *A situation where the non-splitting property holds*

Lemma 4.2.8. *Assume that $|G| = ps$ for some prime p not dividing s, and that there is an antirational element $g \in G$ of order p. Then, elements of order p form exactly $p-1$ conjugacy classes of G which we denote by $c_1, \dots, c_{p-1}$. If moreover G is generated by its elements of order p, then the couple $(G, \{c_1, \dots, c_{p-1}\})$ is non-splitting.*

Proof. For $i \in \{1, \dots, p-1\}$, let c_i be the conjugacy class of g^i. We show that these are $p-1$ distinct conjugacy classes. If $g^i = (g^j)^\gamma$, let k be an inverse of i modulo p; then:

$$g = (g^i)^k = \left((g^j)^\gamma\right)^k = \left(g^{jk}\right)^\gamma.$$

By antirationality of g, this implies $jk = 1 \mod p$ and thus $i = j$. So the conjugacy classes $c_1, \dots, c_{p-1}$ are distinct.

By the second Sylow theorem, any two p-subgroups of G are conjugate. Since $|G| = ps$ with p not dividing s, these are the subgroups of G isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Let $g' \in G$ be an element of order p, then $\langle g' \rangle \simeq \mathbb{Z}/p\mathbb{Z}$ and thus there exists $h \in G$ such that $\langle g' \rangle = \langle g \rangle^h$, i.e. there is a $k \in \{1, \dots, p-1\}$ such that $g' = \left(g^k\right)^h$, i.e. $g' \in c_k$. Therefore, $D = \{c_1, \dots, c_{p-1}\}$ is the set of all conjugacy classes of elements of order p. This proves the first claim.

Consider a D-generated subgroup H of G. By definition, it contains some element g^h of c_1. The element g^h is an antirational element of H. Indeed, if for some $k \in \{2, \dots, p-1\}$ and $h' \in H$ we have:

$$g^h = \left(\left(g^h\right)^k\right)^{h'} = (g^k)^{h'h}$$

then the antirationality of g (as an element of G) is contradicted by the equality $g = (g^k)^{h^{-1}h'h}$.

Since H contains the subgroup $\left\langle g^h \right\rangle \simeq \mathbb{Z}/p\mathbb{Z}$, we know that p divides $|H|$. Let $|H| = ps'$. Since H is a subgroup of G we know that p does not divide s'. Apply the first claim – which we have already proved – to H: the elements of order p of H form exactly $p-1$ conjugacy classes $d_1, \dots, d_{p-1}$ which are the conjugacy classes of $g^h, (g^h)^2, \dots, (g^h)^{p-1}$. Hence, $c_i \cap H = d_i$ is a single conjugacy class of H for any D-generated subgroup H; therefore, the couple (G, D) is non-splitting when G is generated by its elements of order p. □

Example: *Example of couple (G, c) satisfying the non-splitting property*

Let us give an application of Lemma 4.2.8:

Example 4.2.9. Consider $G = \mathfrak{A}_4$, which is of order $12 = 3 \times 4$. Its elements of order 3 are the 3-cycles, which generate G. The 3-cycle (123) is antirational in $\mathfrak{A}_4$. By Lemma 4.2.8, there are exactly two conjugacy classes of elements of order 3 in $\mathfrak{A}_4$:

$$\begin{aligned} c_1 &= \{(123), (142), (134), (243)\} \\ c_2 &= \{(132), (124), (143), (234)\} \end{aligned}.$$

and the couple $(G, \{c_1, c_2\})$ is non-splitting.

4.3. Main results

In this section, X is either $\mathbb{A}^1(\mathbb{C})$ or $\mathbb{P}^1(\mathbb{C})$, G is a finite group, D is a set of nontrivial conjugacy classes of G which together generate G, and ξ is a map $D \to \{1, 2, \dots\}$. We let $c = \bigsqcup_{\gamma \in D} \gamma$.

Before we state our main results, we introduce or recall some notation. If H is a D-generated subgroup of G (cf. Definition 3.2.20), then:

— We let $D_H \overset{\text{def}}{=} \{\gamma \cap H \,|\, \gamma \in D\}$ as in Definition 4.2.1. The map that takes an element $\gamma \cap H \in D_H$ to the unique $\gamma \in D$ which contains it defines a bijection $\beta_H : D_H \simeq D$. We let $\xi_H \overset{\text{def}}{=} \xi \circ \beta_H$ as in Definition 4.2.1.

— We let $c_H = c \cap H$, and we denote by D_H^* the set of all conjugacy classes of H which are contained in the conjugation-invariant set c_H.

— We denote by $\tau_H : D_H^* \to D$ the surjection which maps a conjugacy class of H which belongs to D_H^* to the unique conjugacy class of G which contains it.

— Finally, we define the splitting number:

$$\Omega(D_H) \overset{\text{def}}{=} |D_H^*| - |D_H| = |D_H^*| - |D|\,.$$

The splitting number is nonnegative. It vanishes if and only if τ_H is a bijection, i.e. D_H consists of conjugacy classes of H, i.e. H is a non-splitter (cf. Definition 4.2.4).

We look for information concerning the asymptotical count of connected components of $\mathrm{Hur}_X^*(G, D, n\xi)$ as $n \to \infty$. Note that this is also the Hilbert function of the ring of components $R_X(G, D, \xi)$ (cf. Definition 3.4.12). The homeomorphism:

$$\mathrm{Hur}_X^*(G, D, n\xi) = \bigsqcup_{H \in \mathrm{Sub}_{G,D}} \mathrm{CHur}_X^*(H, D_H, n\xi_H) \tag{4.3.1}$$

relates the counts of connected components of the Hurwitz spaces $\mathrm{Hur}_X^*(G, D, n\xi)$ and $\mathrm{CHur}_X^*(H, D_H, n\xi_H)$. Therefore, it suffices to estimate the number of connected components of $\mathrm{CHur}^*(H, D_H, n\xi_H)$ for all subgroups $H \in \mathrm{Sub}_{G,D}$. This is done in the following theorem:

Theorem: *Asymptotics for the count of connected components of Hurwitz spaces*

Theorem 4.3.1. *Let H be a nontrivial D-generated subgroup of G. We denote by $\mathrm{HF}_H(n)$ the number of connected components of $\mathrm{CHur}^*(H, D_H, n\xi_H)$.*

(i) If $X = \mathbb{A}^1(\mathbb{C})$, then:

$$\mathrm{HF}_H(n) \underset{n\to\infty}{\sim} \left(\frac{|H|\,|H_2(H, c_H)|}{\left|H^{ab}\right|} \prod_{\gamma \in D} \frac{\xi(\gamma)^{\left|\tau_H^{-1}(\gamma)\right|-1}}{\left(\left|\tau_H^{-1}(\gamma)\right| - 1\right)!} \right) n^{\Omega(D_H)}.$$

This is Theorem 4.5.3.

(ii) If $X = \mathbb{P}^1(\mathbb{C})$, if H is a non-splitter, and if k is the order of the element $\widetilde{\pi}(\xi_H)$ in H^{ab} (cf. Definition 3.4.32), then:

$$\mathrm{HF}_H(n) = \begin{cases} 0 & \text{if } n \notin k\mathbb{N} \\ |H_2(H, c_H)| & \text{otherwise, for } n \text{ large enough} \end{cases}.$$

This is Proposition 4.5.6.

(iii) If $X = \mathbb{P}^1(\mathbb{C})$, if $D = \{c\}$ is a singleton, and if $\xi(c) = 1$, then an average order[4] of $\mathrm{HF}_H(n)$ is given by:

$$\frac{|H_2(H, c_H)|\, n^{\Omega(D_H)}}{\left|H^{ab}\right|\,(\Omega(D_H))!}.$$

This is Corollary 4.5.9.

[4] A function g is an *average order* of a function f if:

$$\sum_{k=0}^{n} f(k) \underset{n\to\infty}{\sim} \sum_{k=0}^{n} g(k).$$

(iv) If $X = \mathbb{P}^1(\mathbb{C})$, we have:

$$\mathrm{HF}_H(n) = O^\sharp\left(n^{\Omega(D_H)}\right).$$

This is Theorem 4.4.2 (ii). (cf. Definition 1.4.1 for the definition of $O^\sharp$)

Here is an example of how one can use Theorem 4.3.1: to estimate the growth of the Hilbert function $\mathrm{HF}(n)$ of the ring of components $R_X(G, D, \xi)$, one should determine for which subgroups $H \in \mathrm{Sub}_{G,D}$ the maximal value of the splitting number $\Omega(D_H)$ is reached. The degree of the leading monomial of $\mathrm{HF}(n)$ is this maximal splitting number, and the leading coefficient (which has a clear definition if $X = \mathbb{A}^1(\mathbb{C})$, and can be given a meaning when $X = \mathbb{P}^1(\mathbb{C})$ by looking at average orders) is the sum of the leading coefficients for subgroups with maximal splitting numbers.

If H is a nontrivial non-splitter, then Theorem 4.3.1 tells us that the number of elements of $\mathrm{Comp}_X(G, D, \xi)$ of group H and degree n is a bounded function of n. This is a form of the homological stability for the 0-th homology of Hurwitz spaces shown in [EVW16].

In the next two sections, we prove the various parts of Theorem 4.3.1. In Theorem 4.3.1, we have stated the results in terms of a subgroup H of G. However, in Sections 4.4 and 4.5, we do all computations "intrinsically": we count the connected components of $\mathrm{CHur}^*_X(G, D, n\xi)$ for a general triple $(G, D, \xi) \in \mathbf{ConjInv}$ (cf. Definition 3.2.18). This can be used to deduce Theorem 4.3.1 as stated above, using the equality:

$$\mathrm{HF}_H(n) = \left|\pi_0 \mathrm{CHur}^*_X(H, D_H, n\xi_H)\right|.$$

In this new setting, we "forget" about the fact that the disjoint conjugation-invariant subsets $\gamma \in D$ come from the splitting of conjugacy classes in a bigger group. Instead, elements of D are not assumed to be conjugacy classes, and the splitting number may be recovered intrinsically by defining D^* as the set of conjugacy classes of G which are contained in $c = \bigsqcup_{\gamma \in D} \gamma$, and considering $\Omega(D) \overset{\text{def}}{=} |D^*| - |D|$, cf. Definition 4.2.3.

4.4. Asymptotics of the count of components of $\mathrm{CHur}^*_X(G, D, n\xi)$. Part 1: the exponent

The setting for this section is the following: G is a finite group, D is a set of non-empty disjoint conjugation-invariant subsets of G which together generate G, and ξ is a map $D \to \{1, 2, \ldots\}$. We denote by $|\xi|$ the positive integer $\sum_{\gamma \in D} \xi(\gamma)$.

Definition 4.4.1. For $X = \mathbb{A}^1(\mathbb{C})$ or $X = \mathbb{P}^1(\mathbb{C})$, denote by $\pi_0\mathrm{CHur}^*_X(G, D, n\xi)$ the set of braid orbits of $n\,|\xi|$-tuples $\underline{g}$ of elements of G such that:

Definition: *The set* $\pi_0\mathrm{CHur}^*_X(G, D, n\xi)$

— The elements of $\underline{g}$ generate G, i.e. $\left\langle \underline{g} \right\rangle = G$.

— For each $\gamma \in D$, exactly $\xi(\gamma)$ elements of the tuple $\underline{g}$ belong to γ.

— If $X = \mathbb{P}^1(\mathbb{C})$, then $\pi\underline{g} = 1$.

By Theorem 3.3.7 and Remark 3.3.9, the set $\pi_0\mathrm{CHur}^*_X(G, D, n\xi)$ is in bijection with the connected components of the Hurwitz space $\mathrm{CHur}^*_X(G, D, n\xi)$ (hence the notation). Our goal, in both this section and Section 4.5, is to estimate how the cardinality of this set grows as $n \to \infty$.

We let $c = \bigsqcup_{\gamma \in D} \gamma$, and let D^* be the set of conjugacy classes of G which are contained in c. Each $\gamma \in D^*$ is contained in a unique element of D, which we denote by $\tau(\gamma)$. This defines a surjective map $\tau : D^* \to D$. We let $\Omega(D)$ be the "intrinsic" splitting number $\Omega(D) \overset{\text{def}}{=} |D^*| - |D|$, cf. Definition 4.2.3. Note that $\Omega(D) = 0$ if and only if $D = D^*$, i.e. D consists of conjugacy classes of G.

In this section, we prove the following result:

Theorem: *Growth of* $|\pi_0 \mathrm{CHur}^*_X(G, D, n\xi)|$

Theorem 4.4.2. *We have the following asymptotical estimates for* $|\pi_0 \mathrm{CHur}^*_X(G, D, n\xi)|$*:*

(i)

$$\left|\pi_0 \mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G, D, n\xi)\right| = \Theta\left(n^{\Omega(D)}\right).$$

(ii)

$$\left|\pi_0 \mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi)\right| = O^\sharp\left(n^{\Omega(D)}\right).$$

The proof of Theorem 4.4.2 is in four steps:

— In Subsection 4.4.1, we prove that the number of maps $D^* \to \{0, 1, \ldots\}$ which are "likely" to be (G, c)-multidiscriminants of components of group G and of degree n (cf. Definition 4.4.3) grows like $n^{\Omega(D)}$ (Proposition 4.4.6).

— In Subsection 4.4.2, we prove the lower bounds in Theorem 4.4.2 (Proposition 4.4.7). To do so, we associate to every likely map ψ a component of group G whose multidiscriminant is closely related to ψ.

— In Subsection 4.4.3, we prove that one can factor a given component from any component whose multidiscriminant is "big enough" (Lemma 4.4.8).

— In Subsection 4.4.4, we prove the upper bounds in Theorem 4.4.2 (Proposition 4.4.11). For this, we use the factorization lemma Lemma 4.4.8 to establish that the number of components with a given multidiscriminant is bounded above by a constant independent of the multidiscriminant (Lemma 4.4.10).

4.4.1. Counting likely maps

If $\underline{g}$ is a tuple of elements of c, the number of elements of $\underline{g}$ which belong to a certain $\gamma \in D$ is:

$$\sum_{\gamma' \in \tau^{-1}(\gamma)} \mu_{G,c}(\underline{g})(\gamma').$$

In particular, a tuple $\underline{g}$ represents an orbit which belongs to $\pi_0 \mathrm{CHur}^*_X(G, D, n\xi)$ if and only if:

— The size of $\underline{g}$ is $n\,|\xi|$.

— $\left\langle \underline{g} \right\rangle = G$.

— $\pi(\underline{g}) = 1$ if $X = \mathbb{P}^1(\mathbb{C})$.

— The (G, c)-multidiscriminant ψ of $\underline{g}$ satisfies:

$$\sum_{\gamma' \in \tau^{-1}(\gamma)} \mu_{G,c}(\underline{g})(\gamma') = n\xi(\gamma)$$

for all $\gamma \in D$.

This suggests defining *likely maps*, i.e. maps $D^* \to \{0, 1, \ldots\}$ which are likely to be the (G, c)-multidiscriminant of an element of $\pi_0 \mathrm{CHur}^*_X(G, D, n\xi)$:

Definition: *Likely map*

Definition 4.4.3. Let $n \in \mathbb{N}$. A map $\psi : D^* \to \{0, 1, \ldots\}$ is a *likely map of degree n* if:

$$\sum_{\gamma' \in \tau^{-1}(\gamma)} \psi(\gamma') = n\xi(\gamma).$$

for all $\gamma \in D$. We denote by $\mathcal{L}_n(G, D, \xi)$ the set of all likely maps of degree n.

In this way, we can describe $\pi_0 \mathrm{CHur}^*_X(G, D, n\xi)$:

Proposition: *Multidiscriminants are likely maps*

Proposition 4.4.4. *The set $\pi_0 \mathrm{CHur}^*_X(G, D, n\xi)$ is the set of elements $x \in \mathrm{Comp}_X(G, c)$ such that $\langle x \rangle = G$, $\deg(x) = n\,|\xi|$ and $\mu_{G,c}(x) \in \mathcal{L}_n(G, D, \xi)$.*

Remark: *The monoid of likely maps*

Remark 4.4.5. Likely maps form a submonoid of $\mathbb{Z}^{D^*}$:

$$\mathcal{L}(G, D, \xi) = \bigoplus_{n \geq 0} \mathcal{L}_n(G, D, \xi).$$

Another way to state Proposition 4.4.4 is the following: $\mathrm{Comp}_X(G, D, \xi)$ is the preimage of $\mathcal{L}(G, D, \xi)$ by the morphism of monoids $\mu_{G,c} : \mathrm{Comp}_X(G, c) \to \mathbb{Z}^{D^*}$ (though one has to be aware that the degrees are divided by $|\xi|$):

$$\begin{array}{ccc} \mathrm{Comp}_X(G, D, \xi) & \longrightarrow & \mathcal{L}(G, D, \xi) \\ \big\downarrow & \lrcorner & \big\downarrow \subseteq \\ \mathrm{Comp}_X(G, c) & \xrightarrow[\mu_{G,c}]{} & \mathbb{Z}^{D^*} \end{array}$$

We now count likely maps:

Proposition: *The count of likely maps*

Proposition 4.4.6. *We have the following asymptotical equivalence:*

$$|\mathcal{L}_n(G, D, \xi)| \underset{n \to \infty}{\sim} \left(\prod_{\gamma \in D} \frac{\xi(\gamma)^{|\tau^{-1}(\gamma)|-1}}{(|\tau^{-1}(\gamma)| - 1)!} \right) n^{\Omega(D)}.$$

Proof. To determine a likely map of degree n, one must choose for every conjugation-invariant subset $\gamma \in D$ a way to divide $n\xi(\gamma)$ into the $\left|\tau^{-1}(\gamma)\right|$ conjugacy classes that make up γ. Therefore, $|\mathcal{L}_n(G, D, \xi)|$ is equal to the number of such possibilities, which is given by:

$$\prod_{\gamma \in D} \binom{n\xi(\gamma) + \left|\tau^{-1}(\gamma)\right| - 1}{\left|\tau^{-1}(\gamma)\right| - 1}$$

When n is large enough, this expression is equal to a polynomial in n of degree:

$$\sum_{\gamma \in D} \left(\left|\tau^{-1}(\gamma)\right| - 1 \right) = \left| \bigsqcup_{\gamma \in D} \tau^{-1}(\gamma) \right| - |D| = |D^*| - |D| = \Omega(D),$$

and of leading coefficient:

$$\prod_{\gamma \in D} \frac{\xi(\gamma)^{|\tau^{-1}(\gamma)|-1}}{(|\tau^{-1}(\gamma)| - 1)!}.$$

This concludes the proof. □

4.4.2. Proof of the lower bound on $|\pi_0\mathrm{CHur}^*_X(G,D,n\xi)|$

To obtain the desired lower bound on $|\pi_0\mathrm{CHur}^*_X(G,D,n\xi)|$, we show that likely maps are not much more numerous than components by associating to every likely map a component.

Proposition: *Lower bounds in Theorem 4.4.2*

Proposition 4.4.7. *We have the following lower bounds for $|\pi_0\mathrm{CHur}^*_X(G,D,n\xi)|$:*

(i) If $X=\mathbb{A}^1(\mathbb{C})$, then $n^{\Omega(D)}=O\Big(|\pi_0\mathrm{CHur}^*_X(G,D,n\xi)|\Big)$.

(ii) If $X=\mathbb{P}^1(\mathbb{C})$, then $n^{\Omega(D)}=O\Big(|\pi_0\mathrm{CHur}^*_X(G,D,\exp(G)\,n\,\xi)|\Big)$.

Proof. First fix a tuple $\underline{h}$ representing an element of $\mathrm{Comp}_X(G,D,\xi)$ of group G, which is possible by Proposition 3.2.22. Denote by r the degree of this element.

For each conjugacy class $\gamma\in D^*$, choose an arbitrary element $\widetilde{\gamma}\in\gamma$. If $\psi\in\mathcal{L}_n(G,D,\xi)$ is a likely map of degree n, define the following tuple, where the concatenation happens in an arbitrary order:

$$\underline{g}_\psi=\prod_{\gamma\in D^*}(\underbrace{\widetilde{\gamma},\widetilde{\gamma},\dots,\widetilde{\gamma}}_{\psi(c)}).$$

The (G,c)-multidiscriminant of y_ψ is ψ. So $\underline{h}\underline{g}_\psi$ is a tuple of group G and of (G,c)-multidiscriminant $\psi+\mu_{G,c}(\underline{h})\in\mathcal{L}_{n+r}(G,D,\xi)$.

For each $\psi\in\mathcal{L}_n(G,D,\xi)$, the tuple $\underline{h}\underline{g}_\psi$ represents an element of $\pi_0\mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G,D,(n+r)\xi)$, and these tuples are pairwise nonequivalent for various maps ψ since they have distinct multidiscriminants (cf. Proposition 3.3.8 (iv)). This proves the lower bound:

$$\left|\pi_0\mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G,D,(n+r)\xi)\right|\geq|\mathcal{L}_n(G,D,\xi)|\,.$$

Coupled with Proposition 4.4.6, this implies point (i).

Now consider the tuple $\left(\underline{h}\underline{g}_\psi\right)^{\exp(G)}$, whose product is one. For each ψ, this defines an element of $\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,D,\exp(G)(n+r)\xi)$ with (G,c)-multidiscriminant $\exp(G)\,(\psi+\mu_{G,c}(\underline{h}))$. Similarly, we obtain the lower bound:

$$\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,D,\exp(G)(n+r)\xi)\right|\geq|\mathcal{L}_n(G,D,\xi)|\,,$$

which implies point (ii) when coupled with Proposition 4.4.6. □

4.4.3. The factorization lemma

We prove the factorization result Lemma 4.4.8, which is a generalized version of [EVW16, Proposition 3.4]. This will come in handy to minimize redundancy when counting components.

Lemma: *The factorization lemma Generalization of [EVW16, Proposition 3.4]*

Lemma 4.4.8. *Let $\underline{g}\in G^r$ and $\underline{g}'\in G^n$ be tuples of elements of G. Assume:*

— $\left\langle\underline{g}'\right\rangle=G$.

— *If γ is a conjugacy class of G and $n(\gamma)$ is the number of elements of $\underline{g}$ which belong to γ, then either $n(\gamma)=0$, or there are at least $|\gamma|\,\mathrm{ord}(\gamma)+n(\gamma)$ elements of $\underline{g}'$ which belong to γ.*

Then there exists a tuple $\underline{g}'' \in G^{n-r}$ satisfying $\left\langle \underline{g}'' \right\rangle = G$ such that $\underline{g}'$ is equivalent to the product $\underline{g} \cdot \underline{g}''$.

Note that if $\underline{g}$ and $\underline{g}'$ are tuples or product 1, then any $\underline{g}''$ such that $\underline{g}' = \underline{g}\underline{g}''$ is also a tuple of product 1.

Proof. We start by factoring the first element g_1 of the tuple $\underline{g}$. Let γ be the conjugacy class of g_1 in G. By hypothesis, there are at least $|\gamma| \operatorname{ord}(\gamma) + 1$ elements of $\underline{g}'$ which belong to γ. So some $h_1 \in \gamma$ appears at least $\operatorname{ord}(\gamma) + 1$ times in $\underline{g}'$. Using braids, move $\operatorname{ord}(\gamma) + 1$ copies of h_1 in front:

$$\underline{g}' \sim (\underbrace{h_1, \ldots, h_1}_{\operatorname{ord}(\gamma)}, h_1, k_1, \ldots, k_w).$$

The tuple $(h_1, k_1, \ldots, k_w)$ still generates G. Now use Proposition 3.3.11 (vi) to conjugate the block $(\underbrace{h_1, \ldots, h_1}_{\operatorname{ord}(\gamma)})$, whose product is 1, by an element $\gamma \in G$ such that $h_1^\gamma = g_1$. This yields:

$$\underline{g}' \sim (\underbrace{g_1, \ldots, g_1}_{\operatorname{ord}(\gamma)}, h_1, k_1, \ldots, k_w).$$

We have factored g_1 from $\underline{g}'$. Now, we have to factor g_2 from the tuple:

$$(\underbrace{g_1, \ldots, g_1}_{\operatorname{ord}(\gamma)-1}, h_1, k_1, \ldots, k_w).$$

This tuple satisfies the same hypotheses as $\underline{g}'$, except that it has one less element from the class γ. Since there is also one less element of γ to factor, we may factor g_2, and similarly for $g_3, g_4, \ldots, g_r$. □

Let κ be the maximum value of $|\gamma| \operatorname{ord}(\gamma)$ over classes $\gamma \in D^*$. We have $\kappa \leq |G| \exp(G)$. For $\psi \in \mathbb{Z}^{D^*}$ and $\gamma \in D^*$, let:

$$\mathcal{N}(\psi)(\gamma) = \begin{cases} 1 & \text{if } \psi(\gamma) \geq 1 \\ 0 & \text{otherwise} \end{cases}.$$

This notation lets us rewrite (a slightly weaker version of) Lemma 4.4.8 using (G, c)-multidiscriminants:

Corollary 4.4.9. *Let $x, y \in \operatorname{Comp}_X(G, D, \xi)$, with $\langle y \rangle = G$. If $\mu_{G,c}(y) \geq \mu_{G,c}(x) + \kappa \mathcal{N}(\mu_{G,c}(x))$, then there exists a component $z \in \operatorname{Comp}_X(G, D, \xi)$ such that $y = zx$ and $\langle z \rangle = G$.*

Corollary: *The factorization lemma in terms of multidiscriminants*

4.4.4. Proof of the upper bound on $|\pi_0 \mathrm{CHur}^*_X(G, D, n\xi)|$

In this subsection, we prove Proposition 4.4.11, which is the upper bound in Theorem 4.4.2:

If ψ is a map $D^* \to \{0, 1, \ldots\}$, we denote by F_ψ the set of elements of $\operatorname{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, c)$ of group G whose (G, c)-multidiscriminant is ψ. This is a finite set.

Lemma 4.4.10. *There is a constant K such that for every map $\psi : D^* \to \{0,1,\dots\}$, the cardinality of F_ψ is at most K.*

Proof. Let κ be as in Corollary 4.4.9, and define:

$$K \stackrel{\text{def}}{=} \max_{\substack{\psi: D^* \to \{0,1,\dots\} \\ \text{s.t. } \max(\psi) \leq \kappa}} \left|F_\psi\right|.$$

This number is finite since there are finitely many maps $\psi : D^* \to \{0,1,\dots\}$ for which $\max(\psi) \leq \kappa$, and for every such ψ there are finitely many components whose (G,c)-multidiscriminant is ψ.

We prove that $\left|F_\psi\right| \leq K$ for all maps $\psi : D^* \to \{0,1,\dots\}$, by induction on $\max(\psi)$:

— If $\max(\psi) \leq \kappa$, then $K \geq \left|F_\psi\right|$ by definition.

— Let ψ be a map $D^* \to \{0,1,\dots\}$ such that $\max(\psi) > \kappa$, and assume $\left|F_{\psi'}\right| \leq K$ for every map $\psi' : D^* \to \{0,1,\dots\}$ such that $\max(\psi') < \max(\psi)$.

Let $c_1, \dots, c_r$ be the elements of D^* at which ψ takes its maximal value. For each $i \in \{1,\dots,r\}$, let g_i be an element of c_i. This defines an r-tuple $\underline{g} = (g_1, \dots, g_r)$.

Notice that $\mu_{G,c}(\underline{g})$ takes the value 1 exactly where ψ is maximal, and takes the value 0 otherwise. Therefore:

$$\begin{aligned}\psi &\geq \max(\psi)\mu_{G,c}(\underline{g}) \\ &\geq (1+\kappa)\mu_{G,c}(\underline{g}) \\ &= \mu_{G,c}(\underline{g}) + \kappa\mathcal{N}\left(\mu_{G,c}(\underline{g})\right).\end{aligned}$$

By Corollary 4.4.9, we can factor the component represented by $\underline{g}$ from any component of group G whose multidiscriminant is ψ. This means that concatenation with $\underline{g}$ induces a surjection:

$$F_{\psi - \mu_{G,c}(\underline{g})} \twoheadrightarrow F_\psi.$$

Note that $\psi - \mu_{G,c}(\underline{g})$ is a map $D^* \to \{0,1,\dots\}$ whose maximum is $\max(\psi) - 1$. Finally, using the induction hypothesis:

$$\left|F_\psi\right| \leq \left|F_{\psi - \mu_{G,c}(\underline{g})}\right| \leq K.$$

□

Proposition: *Upper bound in Theorem 4.4.2*

Proposition 4.4.11. *We have $\left|\pi_0\mathrm{CHur}^*_X(G,D,n\xi)\right| = O\left(n^{\Omega(D)}\right)$.*

Proof. Since $\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,D,n\xi)\right| \leq \left|\pi_0\mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G,D,n\xi)\right|$, it is enough to prove the result when $X = \mathbb{A}^1(\mathbb{C})$. It follows from Proposition 4.4.4 that:

$$\pi_0\mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G,D,n\xi) = \bigsqcup_{\psi \in \mathcal{L}_n(G,D,\xi)} F_\psi.$$

Finally:

$$\begin{aligned}\left|\pi_0\mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G,D,n\xi)\right| &= \sum_{\psi \in \mathcal{L}_n(G,D,\xi)} \left|F_\psi\right| \\ &\leq \left|\mathcal{L}_n(G,D,\xi)\right| \times K \qquad \text{by Lemma 4.4.10} \\ &= \Theta\left(n^{\Omega(D)}\right) \qquad \text{by Proposition 4.4.6.}\end{aligned}$$

This concludes the proof. □

4.5. Asymptotics of the count of components of $\mathrm{CHur}^*_X(G, D, n\xi)$. Part 2: the leading coefficient

The setting is the same as in the previous section (Section 4.4): we choose G, D, c, ξ and define $D^*, \tau, \Omega(D)$ in the same way.

In this section, we obtain additional information on the leading term of the count of connected components of $\mathrm{CHur}^*_X(G, D, n\xi)$ as n grows, in two situations. In Subsection 4.5.1, we prove Lemma 4.5.1, which implies that the bijection of Theorem 3.4.39 concerns "most" elements of the ring of components. In Subsection 4.5.2, we prove Theorem 4.5.3, which is the case $X = \mathbb{A}^1(\mathbb{C})$. For the case $X = \mathbb{P}^1(\mathbb{C})$, Subsection 4.5.3 contains general results, Subsection 4.5.4 addresses the situation where H is a non-splitter, and Subsection 4.5.5 focuses on the case $\xi = 1$.

4.5.1. Most components are M-big

Let M be a constant as in Theorem 3.4.39, i.e. such that M-big components (Definition 3.4.40) of group G are characterized by their (G, c)-lifting invariant.

Lemma: *Most components are M-big*

Lemma 4.5.1. *For $n \in \mathbb{N}$, denote by $F_X^{M\text{-small}}(G, D, n\xi)$ the set of components $x \in \mathrm{Comp}_X(G, D, \xi)$ of group G and degree n such that $\min(\mu_{G,c}(x)) < M$. Then:*

$$\left|F_X^{M\text{-small}}(G, D, n\xi)\right| = O\left(n^{\Omega(D)-1}\right).$$

This should be compared with the result of Proposition 4.4.6: as n grows, an arbitrarily high proportion of all components are M-big.

Proof. Let us count the number of likely maps ψ of degree n such that $\min(\psi) \geq M$. To fix such a likely map, for each $\gamma \in D$, we first put aside M occurrences for each of the $\left|\tau^{-1}(\gamma)\right|$ conjugacy class which γ consists of. Then, for each $\gamma \in D$, we have to choose how to split the $n\xi(\gamma) - M\left|\tau^{-1}(\gamma)\right|$ remaining occurrences between the $\left|\tau^{-1}(\gamma)\right|$ conjugacy classes that γ consists of. The number of ways to do so is:

$$\prod_{\gamma \in D} \binom{\left(n\xi(\gamma) - M\left|\tau^{-1}(\gamma)\right|\right) + \left|\tau^{-1}(\gamma)\right| - 1}{\left|\tau^{-1}(\gamma)\right| - 1},$$

which we rewrite as:

$$\prod_{c \in D} \binom{n\xi(\gamma) + (1-M)\left|\tau^{-1}(\gamma)\right| - 1}{\left|\tau^{-1}(\gamma)\right| - 1}.$$

For n large enough, this is equal to a polynomial of same degree and same leading coefficient as $|\mathcal{L}_n(G, D, \xi)|$ (cf. Proposition 4.4.6). So the number of likely maps ψ satisfying $\min(\psi) < M$ is a $O\left(n^{\Omega(D)-1}\right)$. It now follows from Lemma 4.4.10 that:

$$\left|F_X^{M\text{-small}}(G, D, n\xi)\right| = O\left(n^{\Omega(D)-1}\right).$$

□

4.5.2. The case $X = \mathbb{A}^1(\mathbb{C})$

Proposition 4.5.2. *Let $\psi \in \mathbb{Z}^{D^*}$ be a likely map such that $\min(\psi) \geq M$. The number of elements of $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, D, \xi)$ of group G whose (G, c)-multidiscriminant is ψ is given by:*

$$\frac{|G|\,|H_2(G,c)|}{\left|G^{ab}\right|}.$$

Proof. By Theorem 3.4.39, the components of group G and multidiscriminant ψ are in bijection with the elements of $U(G, c)$ whose image in $\mathbb{Z}^{D^*}$ is ψ. Recall from Theorem 3.4.45 that $U(G, c)$ is isomorphic to the group $S_c \underset{G^{\mathrm{ab}}}{\times} \mathbb{Z}^{D^*}$. Therefore the elements of $U(G, c)$ whose image in $\mathbb{Z}^{D^*}$ is ψ are in bijection with the elements of S_c whose image in G^{ab} is $\widetilde{\pi}(\psi)$. Recall that S_c fits in an exact sequence:

$$1 \to H_2(G, c) \to S_c \to G \to 1.$$

In particular, each lift of $\widetilde{\pi}(\psi)$ in G, of which there are $|G| \,/\, \left|G^{\mathrm{ab}}\right|$, is the image of exactly $|H_2(G, c)|$ elements of S_c. We can conclude: the number of components of group G and multidiscriminant ψ is:

$$\frac{|G|\,|H_2(G,c)|}{\left|G^{\mathrm{ab}}\right|}.$$

□

Theorem: *Asymptotics of the count of components of* $\mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G, D, n\xi)$

Theorem 4.5.3. *We have the following asymptotical equivalence:*

$$\left|\pi_0 \mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G, D, n\xi)\right| \underset{n\to\infty}{\sim} \left(\frac{|G|\,|H_2(G,c)|}{\left|G^{ab}\right|} \prod_{\gamma \in D} \frac{\xi(\gamma)^{|\tau^{-1}(\gamma)|-1}}{(|\tau^{-1}(\gamma)|-1)!}\right) n^{\Omega(D)}.$$

Proof. By Proposition 4.4.4, we have:

$$\pi_0 \mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G, D, n\xi) = \bigsqcup_{\psi \in \mathcal{L}_n(G,D,\xi)} F_\psi.$$

So:

$$\left|\pi_0 \mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G, D, n\xi)\right| = \sum_{\min(\psi) > M} \left|F_\psi\right| + F_X^{M\text{-small}}(G, D, n\xi).$$

Apply Proposition 4.5.2 and Lemma 4.5.1 to obtain:

$$\left|\pi_0 \mathrm{CHur}^*_{\mathbb{A}^1(\mathbb{C})}(G, D, n\xi)\right| = |\mathcal{L}_n(G, D, \xi)|\, \frac{|G|\,|H_2(G,c)|}{\left|G^{\mathrm{ab}}\right|} + O\left(n^{\Omega(D)-1}\right).$$

We conclude using Proposition 4.4.6. □

4.5.3. Really-likely maps

Let us observe an obstruction for a given likely map to be the (G, c)-multidiscriminant of a component of $\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi)$. Recall from Definition 3.4.32 that there is a morphism $\widetilde{\pi} : Z^{D^*} \to G^{\mathrm{ab}}$ such that $\widetilde{\pi}(\mu_{G,c}(x))$ is the image in G^{ab} of $\pi(x)$, for each $x \in \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, D, \xi)$. Hence if $x \in \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi) = \ker(\pi)$, it is necessary that $\mu_{G,c}(x) \in \ker(\widetilde{\pi})$. This motivates the following definition:

Definition 4.5.4. A *really-likely map* is a likely map $\psi \in \mathcal{L}(G, D, \xi)$ such that $\widetilde{\pi}(\psi) = 1$.

Once again, fix a value of M as in Theorem 3.4.39. We show that the obstruction observed above is the only obstruction as soon as $\min(\psi) \geq M$, and we determine the exact number of components whose (G, c)-multidiscriminant is ψ:

Proposition 4.5.5. *Let $\psi \in \mathbb{Z}^{D^*}$ be a really-likely map satisfying $\min(\psi) \geq M$. Then ψ is the (G, c)-multidiscriminant of exactly $|H_2(G, c)|$ elements of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ of group G.*

Proof. By Theorem 3.4.39, the elements of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ of group G with multidiscriminant ψ are in bijection with the elements of $U_1(G, c)$ whose image in $\mathbb{Z}^{D^*}$ is ψ. Recall from Corollary 3.4.46 that $U_1(G, c)$ is isomorphic to the direct product of $H_2(G, c)$ and of the subgroup $\ker(\widetilde{\pi})$ of $\mathbb{Z}^{D^*}$ consisting of elements whose image in G^{ab} is 1, which is the case of really-likely maps. It follows that the elements of $U_1(G, c)$ whose image in $\mathbb{Z}^{D^*}$ is ψ are in bijection with the elements of $H_2(G, c)$. This concludes the proof. □

The main remaining task, in order to count components of group G and of degree n precisely, is to count really-likely maps of degree n.

4.5.4. Situation 1: The non-splitting case

In this subsection, we focus on the case $\Omega(D) = 0$. In this case, the elements of D are conjugacy classes, i.e. $D = D^*$, and τ is the identity map. For every $n \in \mathbb{N}$ there is exactly one likely map of degree n, namely $n\xi$. Whether it is a really-likely map depends only on the order k of the element $\widetilde{\pi}(\xi) \in G^{\mathrm{ab}}$:

$$k \overset{\mathrm{def}}{=} \mathrm{ord}\left(\widetilde{\pi}(\xi)\right).$$

This integer can be computed explicitly in concrete situations. For every n, either n is not a multiple of k and then there is no component of $\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi)$, or n is a multiple of k and then there is exactly one really-likely map of degree n. As soon as $n \geq M$, this map takes only values $\geq M$, thus Proposition 4.5.5 implies the following result, which gives the exact value of the count of components of $\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi)$ for n large enough:

Proposition: *Exact formula for the count of components of high degree in the non-splitting case*

Proposition 4.5.6. *For $n \in \mathbb{N}$, we have:*

$$\left|\pi_0 \mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi)\right| = \begin{cases} 0 & \text{if } n \notin k\mathbb{N} \\ |H_2(G, c)| & \text{otherwise, provided } n \geq M \end{cases}.$$

In particular, an average order of $\left|\pi_0 \mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G, D, n\xi)\right|$ is given by the following constant:

$$\frac{1}{k}\left|H_2(G, c)\right|.$$

4.5.5. Situation 2: When $|\xi| = 1$

In this subsection, we discuss the case where D is a singleton $\{c\}$, and $\xi(c) = 1$, i.e. we are counting elements of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$ of group G and degree n.

Let $c_1, \dots, c_s$ be the elements of D^*, with $s = \Omega(D) + 1$. In this situation, multidiscriminants and likely maps are s-tuples of elements of $\mathbb{Z}$. If $\psi \in \mathbb{Z}^s$, we let as above:

$$\widetilde{\pi}(\psi) = \prod_{i=1}^{s} (\widetilde{c_i})^{\psi(i)}.$$

Lemma 4.5.7. *The morphism $\widetilde{\pi} : \mathbb{Z}^s \to G^{ab}$ is surjective.*

Proof. Consider an element $\widetilde{g} \in G^{\mathrm{ab}}$ and fix an arbitrary lift $g \in G$. Since c generates G, g factors as a product $g_1 \cdots g_r$ of elements of c. Let $\psi \in \mathbb{Z}^s$ be the map that counts for each $i = 1, \dots, s$ the number of elements of c_i in this factorization. In G^{ab}, we have $\widetilde{g} = \widetilde{\pi}(\psi)$. □

Proposition: *Estimate of the count of really-likely maps*

Proposition 4.5.8. *As $n \to \infty$, the number of really-likely maps of degree $\leq n$ is equivalent to:*

$$\frac{n^s}{\left|G^{ab}\right| s!}.$$

Proof. Let $\Delta = \exp(G^{\mathrm{ab}})$. For any $\psi \in \mathbb{Z}^s$, the value of $\widetilde{\pi}(\psi)$ depends only on the class of ψ in $(\mathbb{Z}/\Delta\mathbb{Z})^s$. Since $\widetilde{\pi}$ is surjective by Lemma 4.5.7, the induced morphism $\widetilde{\pi} : (\mathbb{Z}/\Delta\mathbb{Z})^s \to G^{\mathrm{ab}}$ is surjective too; hence, its kernel is of cardinality:

$$\frac{\Delta^s}{\left|G^{\mathrm{ab}}\right|}.$$

Let X_n be the subset of $\{0, 1, \dots\}^s$ defined by the condition $x_1 + x_2 + \cdots + x_s \leq n$. This is the set of likely maps of degree $\leq n$. Consider some $\underline{a} = (a_1, \dots, a_s) \in (\mathbb{Z}/\Delta\mathbb{Z})^s$. For each $i = 1, \dots, s$, denote by b_i the element of $\{0, \dots, \Delta - 1\}$ whose class modulo Δ is a_i. Then:

$$\sum_{i=1}^{s} b_i + k_i\Delta = \left(\sum_{i=1}^{s} b_i\right) + \left(\sum_{i=1}^{s} k_i\right)\Delta.$$

Let $S(\underline{a}) = \sum_{i=1}^{s} b_i$. The number of elements of X_n whose projection in $(\mathbb{Z}/\Delta\mathbb{Z})^s$ is $\underline{a}$ is given by the number of nonnegative integers $k_1, \dots, k_s$ whose sum is smaller than $\left\lceil \frac{n - S(\underline{a})}{\Delta} \right\rceil$, i.e.:

$$\binom{s + \left\lceil \frac{n-S(\underline{a})}{\Delta} \right\rceil}{s}.$$

For n large enough, this expression is equal to a polynomial of leading term $\frac{1}{s!}\left(\frac{n}{\Delta}\right)^s$.

Putting everything together, the number of really-likely maps of degree $\leq n$, i.e. the number of elements $\psi \in X_n$ such that $\widetilde{\pi}(\psi) = 1$, is asymptotically equivalent as $n \to \infty$ to:

$$\frac{\Delta^s}{\left|G^{\mathrm{ab}}\right|} \times \frac{1}{s!}\left(\frac{n}{\Delta}\right)^s = \frac{n^s}{\left|G^{\mathrm{ab}}\right| s!}.$$

□

Corollary: *Asymptotics of the count of components of group G and degree $\leq n$*

Corollary 4.5.9. *We have:*

$$\sum_{k=0}^{n} \left|\pi_0 \mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G, \{c\}, k)\right| \underset{n\to\infty}{\sim} \frac{|H_2(G, c)|\, n^s}{\left|G^{ab}\right| s!}$$

In particular, an average order of $\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},n)\right|$ is given by:

$$\frac{|H_2(G,c)|\, n^{s-1}}{\left|G^{\mathrm{ab}}\right|(s-1)!}$$

Proof. Start by separating components according to their multidiscriminants:

$$\sum_{k=0}^{n}\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},k)\right| = \sum_{\substack{\psi \text{ really-likely}\\ \text{of degree } \leq n\\ \min(\psi)\geq M}}\left|F_\psi\right| + \sum_{\substack{\psi \text{ really-likely}\\ \text{of degree } \leq n\\ \min(\psi)< M}}\left|F_\psi\right|.$$

Now, apply Proposition 4.5.5 and Lemma 4.5.1 to obtain:

$$\sum_{k=0}^{n}\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},k)\right| = \sum_{\substack{\psi \text{ really-likely}\\ \text{of degree } \leq n}}|H_2(G,c)| + O\left(n^{s-1}\right).$$

Finally, using Proposition 4.5.8:

$$\begin{aligned}\sum_{k=0}^{n}\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},k)\right| &= \left(\frac{n^s}{\left|G^{\mathrm{ab}}\right|s!} + o\left(n^s\right)\right)|H_2(G,c)| + O\left(n^{s-1}\right)\\ &\sim \frac{|H_2(G,c)|\, n^s}{\left|G^{\mathrm{ab}}\right|s!}.\end{aligned}$$

□

Remark 4.5.10. It follows from Lemma 5.4.4 (applied to the subalgebra $k + I_G$ of $R_{\mathbb{P}^1(\mathbb{C})}(G,c)$) that there is a finite list of polynomials $Q_0,\ldots,Q_{W-1}$ such that, for $m \in \{0,\ldots,W-1\}$ and n big enough, we have $\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},Wn+m)\right| = Q_m(n)$. For $m = 0,\ldots,W-1$, define the polynomial:

$$\widetilde{Q}_m(n) = Q_m\left(\frac{n-m}{W}\right)$$

so that $\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},n)\right| = \widetilde{Q}_m(n)$ if n is big enough and congruent to m modulo W. We show in Lemmas 5.4.5 and 5.4.6 that the polynomials $\widetilde{Q}_m$ have degree $\leq s-1$. Let q_m be the coefficient in front of n^{s-1} in $\widetilde{Q}_m$. This coefficient may be zero, but it is always nonnegative, and it is nonzero for $m = 0$. A Cesàro-like argument shows that:

$$\sum_{i=0}^{n}\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},i)\right| \underset{n\to\infty}{\sim} \left(\frac{1}{W}\sum_{m=0}^{W-1} q_m\right)\frac{n^s}{s}.$$

This equivalence, together with Corollary 4.5.9, gives the "average leading coefficient" in terms of group-theoretical data:

$$\frac{1}{W}\sum_{m=0}^{W-1} q_m = \frac{|H_2(G,c)|}{\left|G^{\mathrm{ab}}\right|(s-1)!}.$$

A noteworthy particular case is when all non-factorizable elements of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G,c)$ have the same degree d. We can then take $W = d$ and we have $q_0 \neq 0$, $q_1 = q_2 = \ldots = q_{d-1} = 0$. Then:

$$q_0 = \frac{d\,|H_2(G,c)|}{\left|G^{\mathrm{ab}}\right|(s-1)!}.$$

In this case, $\left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},n)\right|$ is accurately described by:

$$\begin{cases} \left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},n)\right| & = & 0 \text{ if } n \notin d\mathbb{N} \\ \left|\pi_0\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,\{c\},dn)\right| & \underset{n\to\infty}{\sim} & \dfrac{d^s\left|H_2(G,c)\right|}{\left|G^{\mathrm{ab}}\right|(s-1)!}n^{s-1} \end{cases}.$$

Chapitre 5

The Geometry of Rings of Components of Hurwitz Spaces

Summary of the chapter

In this chapter, we study various aspects of the set of geometric points of the spectrum of the ring of components. The main results are a partition of the spectrum (Proposition 5.1.3), a computation of the dimension of the subsets in that partition (Theorem 5.1.4), and a complete description of the spectrum under specific hypotheses (Theorem 5.5.13).

The content of this chapter is largely taken from the preprint [Seg22].

Outline of the chapter

> Au début, on crut que Tlön était un pur chaos, une irresponsable licence de l'imagination ; on sait maintenant que c'est un cosmos, et les lois intimes qui le régissent ont été formulées, du moins provisoirement.
>
> — J. L. Borges (trad. P. Verdevoye),
> *Tlön, Uqbar, Orbis Tertius*, in *Fictions*, 1944.

5.1. Introduction and main results

For the whole chapter, G is a finite group, D is a set of nontrivial conjugacy classes of G, and ξ is a map $D \to \{1, 2, \ldots\}$. We fix an algebraically closed field k of characteristic relatively prime to $|G|$.

We denote by R the ring of components $R_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ (Definition 3.4.12), which is a commutative graded k-algebra of finite type (Proposition 3.4.6, Corollary 3.4.18).

5.1.1. Introduction

Since R is a commutative k-algebra, we can consider its spectrum $\mathrm{Spec}(R)$, which is a k-scheme. The growth of the number of components of Hurwitz spaces corresponds to the Hilbert function of the graded ring R. Hence, this combinatorial information is related to geometric properties of the spectrum, such as dimensions and degrees of subschemes. This was our initial motivation for the geometric study of this spectrum; along the way, we discovered various phenomena which this chapter attempts to describe. The goal is to better understand rings of components – and, ultimately, Hurwitz spaces.

The geometric study of rings of components of Hurwitz spaces has been a source of fruitful interrogations concerning components themselves: for example, the proof of Theorem 5.1.4 has led us to study nilpotent elements of the ring of components (Section 5.3) and consequently torsion in the monoid of components. The study of torsion in the monoid of components is the analog of the following question when one focuses on components instead of covers: how often does it happen that polynomials $P_1(x, t)$ and $P_2(x, t)$ define non-isomorphic covers, but the polynomials $P_1(x, t^n)$ and $P_2(x, t^n)$ define isomorphic covers? This is a question which we would not have considered were it not for its geometric relevance for the spectrum.

Remark 5.1.1. The ring R is a graded k-algebra, and thus it may seem curious to look at $\mathrm{Spec}(R)$ instead of $\mathrm{Proj}(R)$. As we have discussed in Remark 3.4.20, non-factorizable components need not all have the same degree. Therefore, the ring of components may be a non-standard graded algebra. This means that its Proj lies in a "weighted" projective space, whose k-points form the quotient of $k^N \setminus \{0\}$ by the following action of $k^\times$:

$$\lambda.(z_1, \dots, z_N) = (\lambda^{d_1} z_1, \dots, \lambda^{d_N} z_N)$$

where N is the number of non-factorizable components and the integers d_i are their respective degrees. Weighted projective spaces may be embedded in usual projective spaces of higher dimension [Hos20, Theorem 3.4.9], but we work with $\mathrm{Spec}(R)$ instead of $\mathrm{Proj}(R)$ to avoid dealing with these issues.

We abusively use the word "spectrum" to refer to the set $\mathrm{Spec}(R)(k)$ of the k-points of the spectrum of R, i.e. the set of morphisms of k-algebras from R to k, equipped with the Zariski topology. This choice is in part justified by the fact that the ring of components is « not far from being reduced », as we shall see in Section 5.3.

5.1.2. Main results

We denote by Z the order-reversing map which takes an ideal I of R to the corresponding closed subset $Z(I)$ of $\mathrm{Spec}(R)(k)$.

We use 0 to denote the single point of $Z(\mathfrak{w})$ (the irrelevant ideal $\mathfrak{w}$ is maximal, cf. Proposition 3.4.22). We also introduce the subset $\gamma_\xi(H)$ of $\mathrm{Spec}(R)(k)$, whose definition uses the ideals from Definition 3.4.23:

Definition: *The subset $\gamma_\xi(H)$*

Definition 5.1.2. For every subgroup H of G, the set $\gamma_\xi(H)$ is the following subset of $\mathrm{Spec}(R)(k)$:

$$\gamma_\xi(H) \stackrel{\text{def}}{=} Z(I_H^*) \setminus Z(I_H).$$

The sets $\gamma_\xi(H)$ are neither open nor closed in general, and so they do not correspond to obvious algebraic objects. The following proposition is a first indication of their relevance:

Proposition: *A partition of the spectrum*

Proposition 5.1.3. *The sets $\gamma_\xi(H)$ form a partition of* $\mathrm{Spec}(R)(k)$*:*

$$\mathrm{Spec}(R)(k) = \bigsqcup_{H \in \mathrm{Sub}_{G,D}} \gamma_\xi(H).$$

Proposition 5.1.3 follows from the more general Theorem 5.2.3 by setting $H = G$ in the equality concerning $Z(I_H^*)$. This proposition implies that it suffices to describe all the subsets $\gamma_\xi(H)$ to describe the whole spectrum.

Let H be a nontrivial D-generated subgroup[1] of G. The integer $\dim\big(\gamma_\xi(H)\big)$ is the topological Krull dimension[2] of the set $\gamma_\xi(H)$, equipped with the subspace topology inherited from the Zariski topology on $\mathrm{Spec}(R)(k)$. We relate this Krull dimension to the splitting number $\Omega(D_H)$ from Definition 4.2.3:

[1] cf. Subsection 3.2.6

[2] [Stacks, Definition 0055]

Theorem: *The dimension of $\gamma_\xi(H)$ in terms of the splitting number*

Theorem 5.1.4. *The dimension* $\dim\big(\gamma_\xi(H)\big)$ *is equal to* $\Omega(D_H) + 1$.

The proof of Theorem 5.1.4 is the focus of Section 5.4. Note that the dimension of $\gamma_\xi(H)$ does not actually depend on ξ, but only on D.

In Subsection 5.4.5, we discuss further connections between group-theoretic, combinatorial and algebrogeometric quantities: the second group homology of H, which

we have related to the growth of the number of components of group H in Section 4.5, is connected with the *degree* of the subset $\gamma_{\xi}(H)$ seen as embedded in projective space, when all non-factorizable components have the same degree.

In Section 5.5, we approach the spectrum of the rings of components more "directly": we make strong assumptions on the ring of components and describe parts of its spectrum explicitly. The main theorem of that section is Theorem 5.5.13, which describes the k-points of the spectrum of the ring of components under constraining hypotheses. We do not reproduce the statement of this theorem here since it relies on a lot of terminology.

5.1.3. **Outline of the chapter**

This chapter is organized as follows:

— In Section 5.2, we prove Theorem 5.2.3, from which the partition of the spectrum into parts associated to subgroups to G follows (Proposition 5.1.3).

— In Section 5.3, we show that the ring of components satisfies a weak asymptotic form of reducedness (Theorem 5.3.1): most elements of high degree are not nilpotent. The proof relies on the lifting invariant presented in Subsection 3.4.7. We also make use of standard results from model theory, namely Łos's theorem and the completeness of the theory of algebraically closed fields of characteristic 0.

— In Section 5.4, we prove that the Krull dimension of the subset $\gamma_{\xi}(H)$ of $\mathrm{Spec}(R)(k)$ is one more than the splitting number (Theorem 5.1.4). In Subsection 5.4.5, we discuss the degree of $\gamma_{\xi}(H)$. The proofs use the results from Chapter 4.

— In Section 5.5, we describe the points of the spectrum of the ring of components seen as embedded in an affine space under specific hypotheses (Theorem 5.5.13). These results are applied in Chapter 6 to the case where G is a symmetric group.

5.2. A partition of the spectrum

In this section, we prove the partition of the spectrum proposed in Proposition 5.1.3. More precisely, we prove Theorem 5.2.3, which is more general. We first restate some of the properties from Proposition 3.4.24 geometrically:

Proposition: *Properties of the closed subsets $Z(I_H)$, $Z(I_H^*)$, $Z(J_H)$ and $Z(J_H^*)$*

Proposition 5.2.1. *The closed subsets $Z(I_H)$, $Z(I_H^*)$, $Z(J_H)$ and $Z(J_H^*)$ (defined using the ideals from Definition 3.4.23) satisfy the following properties:*

(i) For every subgroup H of G, we have the inclusions:

$$\begin{array}{ll} Z(I_H) \subseteq Z(I_H^*) & Z(J_H^*) \subseteq Z(I_H^*) \\ Z(J_H) \subseteq Z(I_H) & Z(J_H) \subseteq Z(J_H^*) \end{array}.$$

These inclusions are strict if and only if $H \in \mathrm{Sub}_{G,D}$ (cf. Definition 3.2.20).

(ii) An inclusion $H \subseteq H'$ between two subgroups of G induces inclusions between the corresponding closed subsets:

$$\begin{array}{ll} Z(I_H) \subseteq Z(I_{H'}) & Z(I_H^*) \subseteq Z(I_{H'}^*) \\ Z(J_H) \subseteq Z(J_{H'}) & Z(J_H^*) \subseteq Z(J_{H'}^*) \end{array}$$

i.e. the maps $H \mapsto Z(I_H)$, $Z(I_H^*)$, $Z(J_H)$, $Z(J_H^*)$ are all order-preserving.

(iii) We have

$$Z(I_1) = Z(J_1) = \varnothing$$
$$Z(I_1^*) = Z(J_1^*) = \{0\}$$
$$Z(I_G^*) = Z(J_G^*) = \mathrm{Spec}(R)(k).$$

(iv) For every subgroup H of G:

$$Z(I_H^*) = Z(I_H) \cup Z(J_H^*) \qquad Z(J_H) = Z(I_H) \cap Z(J_H^*).$$

(v) For every subgroup H of G:

$$Z(I_H^*) = \bigcap_{\substack{H' \supsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} Z(I_{H'}) \qquad Z(J_H) = \bigcup_{\substack{H' \subsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} Z(J_{H'}^*).$$

(vi) For every subgroups $H_1, H_2 \subseteq G$:

$$Z(I_{\langle H_1, H_2 \rangle}) = Z(I_{H_1}) \cup Z(I_{H_2}) \qquad Z(J_{H_1 \cap H_2}^*) = Z(J_{H_1}^*) \cap Z(J_{H_2}^*).$$

Proof. Follows directly from Proposition 3.4.24. The strict inclusions in point (i) deserve a careful look. For example, to prove that the inclusion $Z(I_H) \subseteq Z(I_H^*)$ is strict, we need $\sqrt{I_H^*} \subsetneq \sqrt{I_H}$. Let $H \in \mathrm{Sub}_{G,D}$. Any component of group H (which exists by Proposition 3.2.22) is in $\sqrt{I_H}$, and its powers are components of group H and thus are never in I_H^*. Hence $\sqrt{I_H} \neq \sqrt{I_H^*}$. □

We recall Definition 5.1.2:

Definition 5.1.2 (recalled). *For every subgroup H of G, the set $\gamma_\xi(H)$ is the following subset of* $\mathrm{Spec}(R)(k)$*:*

$$\gamma_\xi(H) \stackrel{def}{=} Z(I_H^*) \setminus Z(I_H).$$

Definition 5.1.2 (recalled)

For example, $\gamma_\xi(1) = \{0\}$. It follows from Proposition 5.2.1 (i) that $\gamma_\xi(H)$ is nonempty if and only if $H \in \mathrm{Sub}_{G,D}$. Moreover:

Proposition 5.2.2. *For every subgroup H of G, the set $\gamma_\xi(H)$ is equal to $Z(J_H^*) \setminus Z(J_H)$.*

Proposition: *Another description of $\gamma_\xi(H)$*

Proof.

$$\begin{aligned}
\gamma_\xi(H) &= Z(I_H^*) \setminus Z(I_H) && \text{by Definition 5.1.2} \\
&= (Z(I_H) \cup Z(J_H^*)) \setminus Z(I_H) && \text{by Proposition 5.2.1 (iv)} \\
&= Z(J_H^*) \setminus (Z(I_H) \cap Z(J_H^*)) \\
&= Z(J_H^*) \setminus Z(J_H) && \text{by Proposition 5.2.1 (iv).}
\end{aligned}$$

□

We finally prove Theorem 5.2.3:

Theorem:
Various closed subsets of the spectrum are made of sets $\gamma_\xi(H)$

Theorem 5.2.3. *For every subgroup H of G, we have the following equalities:*

$$Z(I_H) = \bigsqcup_{\substack{H' \in \mathrm{Sub}_{G,D} \\ H \text{ not contained in } H'}} \gamma_\xi(H') \qquad Z(I_H^*) = \bigsqcup_{\substack{H' \in \mathrm{Sub}_{G,D} \\ H \text{ not strictly contained in } H'}} \gamma_\xi(H')$$

$$Z(J_H) = \bigsqcup_{H' \subsetneq H} \gamma_\xi(H') \qquad Z(J_H^*) = \bigsqcup_{H' \subseteq H} \gamma_\xi(H').$$

Proof.

— We first prove that the sets $\gamma_\xi(H)$ are disjoint. Consider two distinct subgroups $H, H' \in \mathrm{Sub}_{G,D}$.

- Assume first that neither of H and H' is a subset of the other, and let $J = \gamma_\xi(H) \cap \gamma_\xi(H')$. Then $\widetilde{H} = \langle H, H' \rangle$ is strictly larger than both H and H'. Since $Z(I_H^*) \subseteq Z(I_{\widetilde{H}})$, we have $\gamma_\xi(H) \subseteq Z(I_{\widetilde{H}})$. The same holds for H' and thus $J \subseteq Z(I_{\widetilde{H}})$. But then $Z(I_{\widetilde{H}}) \setminus J$ is a subset of $Z(I_{\widetilde{H}})$ containing both $Z(I_H)$ and $Z(I_{H'})$. Since $Z(I_{\widetilde{H}}) = Z(I_H) \cup Z(I_{H'})$, this implies $J = 0$.
- Now assume instead that $H \subsetneq H'$. The set $\gamma_\xi(H)$ is contained in $Z(I_H^*)$ and therefore in $Z(I_{H'})$. Thus $\gamma_\xi(H') = Z(I_{H'}^*) \setminus Z(I_{H'})$ has an empty intersection with $\gamma_\xi(H)$.

— Let us prove, by decreasing induction on the size of a subgroup $H \in \mathrm{Sub}_{G,D}$, that:

$$Z(I_H)^c = \bigcup_{\substack{H' \in \mathrm{Sub}_{G,D} \\ H' \supseteq H}} \gamma_\xi(H')$$

Let $H \in \mathrm{Sub}_{G,D}$ and assume every $H' \in \mathrm{Sub}_{G,D}$ of bigger cardinality satisfies the equality above. Then:

$$\begin{aligned}
Z(I_H)^c &= \left(Z(I_H^*) \setminus \gamma_\xi(H)\right)^c && \text{by definition of } \gamma_\xi(H) \\
&= \left(\bigcap_{\substack{H' \supsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} Z(I_{H'}) \right)^c \cup \gamma_\xi(H) && \text{by Proposition 5.2.1 (ii)} \\
&= \left(\bigcup_{\substack{H' \supsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} (Z(I_{H'}))^c \right) \cup \gamma_\xi(H) \\
&= \left(\bigcup_{\substack{H' \supsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} \bigcup_{\substack{H'' \supseteq H' \\ H'' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H'') \right) \cup \gamma_\xi(H) && \text{by induction hypothesis} \\
&= \left(\bigcup_{\substack{H' \supsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H') \right) \cup \gamma_\xi(H) \\
&= \bigcup_{\substack{H' \supseteq H \\ H' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H')
\end{aligned}$$

This concludes the induction. The case $H = 1$ gives:

$$\mathrm{Spec}(R)(k) = Z(I_1)^c = \bigsqcup_{H' \in \mathrm{Sub}_{G,D}} \gamma_\xi(H').$$

Finally:

$$\begin{aligned} Z(I_H) &= \mathrm{Spec}(R)(k) \setminus Z(I_H)^c \\ &= \left(\bigsqcup_{H' \in \mathrm{Sub}_{G,D}} \gamma_\xi(H') \right) \setminus \left(\bigsqcup_{\substack{H' \supsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H') \right) \\ &= \bigsqcup_{\substack{H' \in \mathrm{Sub}_{G,D} \\ H \text{ not contained in } H'}} \gamma_\xi(H'). \end{aligned}$$

Since $Z(I_H)^* = Z(I_H) \cup \gamma_\xi(H)$, it follows that:

$$Z(I_H^*) = \bigsqcup_{\substack{H' \in \mathrm{Sub}_{G,D} \\ H \text{ not strictly contained in } H'}} \gamma_\xi(H').$$

— Let us prove, by increasing induction on the cardinality of a subgroup $H \in \mathrm{Sub}_{G,D}$, that:

$$Z(J_H^*) = \bigcup_{\substack{H' \subseteq H \\ H' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H')$$

Let $H \in \mathrm{Sub}_{G,D}$ and assume every $H' \in \mathrm{Sub}_{G,D}$ of smaller cardinality satisfies the equality above. Then:

$$\begin{aligned} Z(J_H^*) &= \gamma_\xi(H) \cup Z(J_H) && \text{by Proposition 5.2.2} \\ &= \gamma_\xi(H) \cup \left(\bigcup_{\substack{H' \subsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} Z(J_{H'}^*) \right) && \text{by Proposition 5.2.1 (ii)} \\ &= \gamma_\xi(H) \cup \left(\bigcup_{\substack{H' \subsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} \bigcup_{\substack{H'' \subseteq H' \\ H'' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H'') \right) && \text{by induction hypothesis} \\ &= \gamma_\xi(H) \cup \left(\bigcup_{\substack{H' \subsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H') \right) \\ &= \bigcup_{\substack{H' \subseteq H \\ H' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H'). \end{aligned}$$

Since $Z(J_H) = Z(J_H^*) \setminus \gamma_\xi(H)$, it follows that:

$$Z(J_H) = \bigsqcup_{\substack{H' \subsetneq H \\ H' \in \mathrm{Sub}_{G,D}}} \gamma_\xi(H').$$

□

Remark 5.2.4. We can state Proposition 5.1.3 algebraically: if $\mathfrak{m}$ is a maximal ideal of R, then there is a unique subgroup $G(\mathfrak{m}) \in \mathrm{Sub}_{G,D}$ such that $\mathfrak{m}$ contains $I^*_{G(\mathfrak{m})}$ but does not contain $I_{G(\mathfrak{m})}$.

Remark: *Algebraic form of Proposition 5.1.3*

5.3. On nilpotent elements of the ring of components

The goal of this section is to prove Theorem 5.3.1, which states that the ring of components satisfies a weak asymptotic form of reducedness. We need Theorem 5.3.1 for subsequent results: since k-points of the spectrum do not distinguish between ideals and their radical, reducedness-like results ensure that the geometry of the spectrum does not miss too much information.

In the whole section, we fix a nontrivial D-generated subgroup H of G. For $n \in \mathbb{N}$, denote by $R_{n,H}$ the k-vector space spanned by components of group H and of degree n, and by $N_{n,H}$ the subspace of $R_{n,H}$ consisting of elements nilpotent in R. We can now state the theorem:

Theorem 5.3.1. $\dim_k N_{n,H} = O\left(n^{\Omega(D_H)-1}\right)$.

Theorem: *There are few high-degree nilpotent elements in rings of components.*

This should be compared to Theorem 4.4.2 (ii), which says that $\dim_k R_{n,H} = O^\sharp\left(n^{\Omega(D_H)}\right)$. We deduce from this comparison that, in some sense, most high-degree elements of R are not nilpotent. The methods used for the proof are diverse:

— The main tool is Lemma 5.3.2, a result about the monoid of components. The proof involves the lifting invariant from [EVW12; Woo21], which we have presented in Subsection 3.4.7.

— The case of characteristic p is Corollary 5.3.3, which follows from the properties of the Frobenius morphism. We first prove the result in positive characteristic because it is tricky to prove that a sum is not nilpotent: if x is a sum of n terms then x^2 is a sum of $n + \binom{n}{2}$ terms, and it is hard to ensure that these additional terms do not cause unexpected cancellations. A way to get rid of the extra terms is to assume $2 = 0$. Then one just has to ensure that the powers of the original terms do not cancel.

— The case of characteristic 0 is Corollary 5.3.4. We deduce it from the case of positive characteristic using classical results from model theory.

5.3.1. Torsion in the monoid of components

Let c_H be the union of the conjugacy classes of D_H. We use the notation from Subsection 3.4.7. In particular, we fix a constant $M = M_{H,c_H}$ as in Theorem 3.4.39. We prove the following lemma, which implies that the monoid of components is « not far » from being torsionfree (a monoid is torsionfree if $x^n = y^n$ for $n \geq 1$ implies $x = y$):

Lemma 5.3.2. *Let $\underline{g}_0, \underline{g}_1 \in H^n$ be two n-tuples such that $\pi\underline{g}_0 = \pi\underline{g}_1 = 1$ and $\left\langle \underline{g}_0 \right\rangle = \left\langle \underline{g}_1 \right\rangle = H$. Assume that, for some integer $p \in \mathbb{N}$ coprime with $|G|$, the tuples $\underline{g}_0^p$ and $\underline{g}_1^p$ are equivalent. Assume moreover that every conjugacy class $\gamma \in D_H$ occurs at least M times in $\underline{g}_0$. Then the tuples $\underline{g}_0$ and $\underline{g}_1$ are braid equivalent.*

Lemma: *The monoid of components is not far from being torsion-free*

Proof. Since $\underline{g}_0^p$ and $\underline{g}_1^p$ are equivalent, the tuples $\underline{g}_0$ and $\underline{g}_1$ have the same (H, c_H)-multidiscriminant, whose coordinates are all $\geq M$. By Theorem 3.4.39, the map Π_{H,c_H} is injective when restricted to tuples whose (H, c_H)-multidiscriminant ψ satisfies $\min(\psi) \geq M$, so it suffices to prove that $\Pi(\underline{g}_0) = \Pi(\underline{g}_1)$.

Since $\pi\underline{g}_0 = \pi\underline{g}_1 = 1$, the elements $\Pi(\underline{g}_0)$ and $\Pi(\underline{g}_1)$ commute, and since $\underline{g}_0^p \sim \underline{g}_1^p$, their p-th powers are equal. It follows that $\Pi(\underline{g}_0)\Pi(\underline{g}_1)^{-1}$ is an element of p-torsion of $U_1(H, c_H)$, with trivial image in $\mathbb{Z}^{D_H}$. By Corollary 3.4.46, this element corresponds to some element of p-torsion in $H_2(H, c_H)$. Since $H_2(H, \mathbb{Z})$ is of $|H|$-torsion, its quotient $H_2(H, c_H)$ is of $|H|$-torsion too. Since p is coprime with $|H|$, there is no nontrivial p-torsion in $H_2(H, c_H)$. We conclude that $\Pi(\underline{g}_0)\Pi(\underline{g}_1)^{-1} = 1$ and finally $\underline{g}_0 \sim \underline{g}_1$. □

5.3.2. **The case of positive characteristic**

By Lemma 4.5.1, we know that there is a constant $\widetilde{C}$ such that the number of components $x \in \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(H, D_H, \xi_H)$ of group H and degree n whose multidiscriminant ψ satisfies $\min(\psi) \geq M$ is bounded above by $\widetilde{C} \cdot n^{\Omega(D_H)-1}$.

Corollary: *Theorem 5.3.1 when the characteristic of k is nonzero*

Corollary 5.3.3. *Assume the characteristic of k is positive and coprime to $|G|$. Then for all $n \in \mathbb{N}$:*

$$\dim_k N_{n,H} \leq \widetilde{C} \cdot n^{\Omega(D_H)-1}.$$

Proof. Fix some $n \in \mathbb{N}$. Let u^r be the k-linear map $R_{n,H} \to R_{np^r,H}$ induced by $x \mapsto x^{p^r}$ on components. We deduce from Lemma 5.3.2 and Lemma 4.5.1 that, for all $r \in \mathbb{N}$:

$$\dim_k \ker(u^r) \leq \widetilde{C} \cdot n^{\Omega(D_H)-1}.$$

Choose a basis $x_1, \ldots, x_D$ of $N_{n,H}$, and complete it into a basis:

$$\underbrace{x_1, \ldots, x_D}_{\in N_{n,H}}, x_{D+1}, \ldots, x_{D'}$$

of $R_{n,H}$. Note that $D = \dim N_{n,H}$ and $D' = \dim R_{n,H}$. Express the vectors $x_1, \ldots, x_{D'}$ in the basis $m_1, \ldots, m_{D'}$ of $R_{n,H}$ given by all components of group H and of degree n:

$$x_i = \sum_{j=1}^{D'} \lambda_{i,j} m_j.$$

Since $x_1, \ldots, x_D$ are nilpotent, we fix $r \geq 1$ such that $x_i^{p^r} = 0$ for all $i = 1, \ldots, M$. Define, for $i = 1, \ldots, D'$:

$$\widetilde{x}_i \overset{\text{def}}{=} \sum_{j=1}^{D'} \lambda_{i,j}^{p^r} m_j.$$

The family $\widetilde{x}_i$ is still a basis of $R_{n,H}$. Indeed, the determinant of the matrix $(\lambda_{i,j}^{p^r})_{i,j}$ is the p^r-th power of the determinant of the matrix $(\lambda_{i,j})_{i,j}$ which is nonzero because $x_1, \ldots, x_{D'}$ is a basis. In particular, the vectors $\widetilde{x}_1, \ldots, \widetilde{x}_D$ are linearly independent.

Now if $i \in 1, \ldots, D$, we have:

$$u^r(\widetilde{x}_i) = \sum_{j=1}^{D'} \lambda_{i,j}^{p^r} u^r(m_j) = \sum_{j=1}^{D'} \lambda_{i,j}^{p^r} m_j^{p^r} = x_i^{p^r} = 0.$$

So $\widetilde{x}_1, \ldots, \widetilde{x}_D$ is a linearly independent family of D vectors in $\ker(u^r)$. Finally:

$$\dim N_{n,H} = D \leq \dim \ker(u^r) \leq \widetilde{C} \cdot n^{\Omega(D_H)-1}.$$

□

5.3.3. **The case of characteristic zero**

The setting and the notation are the same as in Subsection 5.3.2.

Corollary: *Theorem 5.3.1 when the characteristic of k is zero*

Corollary 5.3.4. *Assume the characteristic of k is zero. Then for all $n \in \mathbb{N}$:*

$$\dim_k N_{n,H} \leq \widetilde{C} \cdot n^{\Omega(D_H)-1}.$$

Proof. Since dimensions do not change by field extensions (by flatness of the extension $\overline{k} \mid k$), we may assume that k is algebraically closed.

Let $n \in \mathbb{N}$. We denote by F the finite set of components of degree n and group H. We define, for each $r \geq 1$, the following finite subset of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$:

$$F^{\wedge r} = \{m_1 m_2 \cdots m_r \mid m_1, m_2, \ldots, m_r \in F\}.$$

Let K be a field. Consider an element x in the K-vector space spanned by F and write it as:

$$x = \sum_{m \in F} \lambda_m m.$$

For every $r \geq 1$, we have the following equality in $K[\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)]$:

$$\begin{aligned} x^r &= \sum_{m_1, m_2, \ldots, m_r \in F} \lambda_{m_1}\lambda_{m_2}\cdots\lambda_{m_r} \cdot (m_1 m_2 \cdots m_r) \\ &= \sum_{m \in F^{\wedge r}} \left(\sum_{\substack{m_1, m_2, \ldots, m_r \in F \\ m_1 m_2 \cdots m_r = m}} \lambda_{m_1}\lambda_{m_2}\cdots\lambda_{m_r} \right) m. \end{aligned}$$

If $\underline{\lambda} = (\lambda_m)$ is a set of variables indexed by F, denote by $Nilp_r(\underline{\lambda})$ the following conjunction:

$$\bigwedge_{m \in F^{\wedge r}} \left(\sum_{\substack{m_1, m_2, \ldots, m_r \in F \\ m_1 m_2 \cdots m_r = m}} \lambda_{m_1}\lambda_{m_2}\cdots\lambda_{m_r} = 0 \right).$$

The property $Nilp_r(\underline{\lambda})$ expresses the fact that the element $x = \sum_m \lambda_m m$ satisfies $x^r = 0$ in $K[\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)]$. This may not look like a first-order property, but one must see $\bigwedge_{m \in F^{\wedge r}}$ as an abbreviation for a long conjunction of finitely many properties, and similarly $\sum_{\substack{m_1, m_2, \ldots, m_r \in F \\ m_1 m_2 \cdots m_r = m}}$ may be expanded into a long explicit sum for each $m \in F^{\wedge r}$.

Let $d = \widetilde{C} \cdot n^{\Omega(D_H)-1} + 1$. If $\underline{\lambda}^{(1)}, \ldots, \underline{\lambda}^{(d)}$ are d sets of variables, each indexed by F, we denote by $Indep(\underline{\lambda}^{(1)}, \ldots, \underline{\lambda}^{(d)})$ the first-order property:

$$\forall x_1, \ldots, \forall x_d, \left(\bigwedge_{m \in F} x_1 \lambda_m^{(1)} + \cdots + x_d \lambda_m^{(d)} = 0 \right) \Rightarrow (x_1 = 0 \wedge x_2 = 0 \wedge \ldots \wedge x_d = 0)$$

which expresses the fact that the elements $x^{(i)} = \sum_m \lambda_m^{(i)} m$ are linearly independent.

Finally, we define the first-order property φ_r as:

$$\forall \underline{\lambda}^{(1)}, \ldots, \forall \underline{\lambda}^{(d)}, \left(Nilp_{F,r}(\underline{\lambda}^{(1)}) \wedge \ldots \wedge Nilp_{F,r}(\underline{\lambda}^{(d)}) \right) \Rightarrow \neg Indep(\underline{\lambda}^{(1)}, \ldots, \underline{\lambda}^{(d)})$$

which expresses the fact that if $x^{(1)}, \ldots, x^{(d)}$ are elements of $\mathrm{Span}_K(F)$ whose r-th powers are all zero in $K[\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)]$, then they are always linearly dependent, i.e. that the dimension of the subspace of elements of $\mathrm{Span}_K(F)$ whose r-th powers are zero is at most $d - 1 = \widetilde{C} \cdot n^{\Omega(D_H)-1}$.

By Corollary 5.3.3, we know that the field $\overline{\mathbb{F}_p}$ satisfies the property φ_r for all $r \in \mathbb{N}$ when p is a prime coprime to $|G|$. Let $\mathcal{U}$ be a non-principal ultrafilter on the set $\mathcal{P}$ of primes coprime to $|G|$ and define:

$$\mathbb{K} = \left(\prod_{p \in \mathcal{P}} \overline{\mathbb{F}_p} \right) / \mathcal{U}.$$

By Łoś's theorem [Maro2, Exercise 2.5.18], $\mathbb{K}$ is an algebraically closed field of characteristic zero, and it satisfies φ_r for all $r \geq 1$. Since the theory of algebraically closed fields of characteristic zero is complete [Maro2, Corollary 3.2.3], this is true for k. So the dimension of the space $N_{n,H,r}$ of elements of $R_{n,H}$ whose r-th power vanishes is at most $\widetilde{C} \cdot n^{\Omega(D_H)-1}$, for all $r \geq 1$. Now:

$$N_{n,H} = \bigcup_{r=1}^{\infty} N_{n,H,r}.$$

This union is an increasing union. Thus:

$$\dim N_{n,H} = \sup_{r \geq 1} \left(\dim N_{n,H,r} \right) \leq \widetilde{C} \cdot n^{\Omega(D_H)-1}.$$

□

5.4. The dimension of $\gamma_{\xi}(H)$ and the splitting number

In this section, we prove Theorem 5.1.4. We fix a nontrivial D-generated subgroup $H \in \mathrm{Sub}_{G,D}$, and we prove that the Krull dimension of the set $\gamma_{\xi}(H)$ is related to the splitting number $\Omega(D_H)$ by the formula:

$$\dim \left(\gamma_{\xi}(H) \right) = \Omega(D_H) + 1.$$

The section is organized in the following way:

— In Subsection 5.4.1, we describe an ideal Γ_H and prove that it corresponds to the closed subset $\overline{\gamma_{\xi}(H)}$ of $\mathrm{Spec}(R)(k)$ (Theorem 5.4.1 (vi)).

— In Subsection 5.4.2, we prove Proposition 5.4.3, which is a variant of the Hilbert-Serre theorem for algebras with generators of unequal degrees.

— In Subsection 5.4.3, we prove Lemma 5.4.7, which estimates the number of elements of degree n in an ideal.

— In Subsection 5.4.4, we put the pieces together to prove Theorem 5.1.4. The proof requires the lemmas proved in Subsections 5.4.1 to 5.4.3 as well as Theorem 5.3.1 and Theorem 4.4.2 (ii) from the previous chapter.

— In Subsection 5.4.5, we discuss the degree of $\gamma_{\xi}(H)$, seen as embedded in projective space. For this, we use the results of the whole section as well as the computations of leading coefficients from Section 4.5.

5.4.1. The ideal Γ_H

In this subsection, we give an explicit description of the ideal of R corresponding to the closed subset $\overline{\gamma_{\xi}(H)}$.

Theorem: *The radical ideal Γ_H*

Theorem 5.4.1. *Define the following subset of R:*

$$\Gamma_H \stackrel{def}{=} \left\{ x \in R \,\middle|\, (x) \cap \sqrt{I_H} \subseteq \sqrt{I_H^*} \right\}.$$

The following properties hold:

(i) Let I be an ideal of R. Then $I \cap \sqrt{I_H} \subseteq \sqrt{I_H^*}$ if and only if I is contained in any maximal ideal m which contains I_H^* and does not contain I_H.

(ii) The set Γ_H is the intersection of all maximal ideals which contain I_H^* and do not contain I_H.

(iii) The set Γ_H is a radical ideal.

(iv) An ideal I satisfies $I \cap \sqrt{I_H} \subseteq \sqrt{I_H^*}$ if and only if I is contained in Γ_H.

(v) $\Gamma_H \subseteq \mathfrak{o}$.

(vi) $Z(\Gamma_H) = \overline{\gamma_\xi(H)}$.

(vii) The point 0 belongs to $\overline{\gamma_\xi(H)}$.

Proof.

(i) We prove both directions:

($\Rightarrow$) Assume $I \cap \sqrt{I_H} \subseteq \sqrt{I_H^*}$ and let m be a maximal ideal containing I_H^* and not containing I_H. Then:

$$I \cap \sqrt{I_H} \subseteq \sqrt{I_H^*} \subseteq m.$$

Since m is prime and does not contain $\sqrt{I_H}$, it contains I.

($\Leftarrow$) Assume that I is contained in any maximal ideal containing I_H^* and not containing I_H. If m is a maximal ideal containing I_H^*, then either m contains I_H, or $I \subseteq m$. In both cases, we obtain $I \cap I_H \subseteq m$. Now:

$$I \cap \sqrt{I_H} \subseteq \sqrt{I \cap I_H} = \bigcap_{\substack{m \text{ maximal} \\ I \cap I_H \subseteq m}} m \subseteq \bigcap_{\substack{m \text{ maximal} \\ I_H^* \subseteq m}} m = \sqrt{I_H^*}.$$

(ii) Follows from (i) by considering the case $I = (x)$.

(iii) By (ii), Γ_H is an intersection of maximal ideals and is thus a radical ideal.

(iv) Follows directly from (i) and (ii).

(v) Consider some element not in $\mathfrak{o}$. It is of the form $\lambda + x$, with $x \in \mathfrak{o}$ and $\lambda \in k^\times$.

Take a component y of group exactly H. Then $(\lambda + x)y$ is a linear combination of components of group containing H, hence $(\lambda + x)y \in (\lambda + x) \cap \sqrt{I_H}$. For all $n \geq 1$, the term of smallest degree of $((\lambda + x)y)^n$ is $\lambda^n y^n$ whose group is H, and it cannot be compensated by other terms, which have strictly higher degree. This shows that $((\lambda + x)y)^n \notin I_H^*$ for all n and thus $(\lambda + x)y \notin \sqrt{I_H^*}$.

So $(\lambda + x) \cap \sqrt{I_H}$ is not contained in $\sqrt{I_H^*}$, i.e. $\lambda + x \notin \Gamma_H$. This proves $\Gamma_H \subseteq \mathfrak{o}$;

(vi) By (iv), Γ_H is the biggest possible radical ideal such that $\Gamma_H \cap \sqrt{I_H} = \sqrt{I_H^*}$. Hence $Z(\Gamma_H)$ is the smallest possible closed set such that $Z(I_H^*) = Z(\Gamma_H) \cup Z(I_H)$, i.e.:

$$Z(\Gamma_H) = \overline{Z(I_H^*) \setminus Z(I_H)} = \overline{\gamma_\xi(H)}.$$

(vii) Follows directly from (v) and (vi).

□

Proposition: *The Krull dimension of the subset $\gamma_{\tilde{\xi}}(H)$ is equal to that of the algebra R/Γ_H*

Proposition 5.4.2. *We have* $\dim \gamma_{\tilde{\xi}}(H) = \dim \overline{\gamma_{\tilde{\xi}}(H)} = \dim R/\Gamma_H$.

Proof. The first equality follows from [Har77, Proposition I.1.10]. The second equality follows from Theorem 5.4.1 (vi). □

5.4.2. **Hilbert functions of weighted algebras**

The result of this subsection, Proposition 5.4.3, is a variant of the Hilbert-Serre theorem. The case of standard algebras is classical, see for example [Har77, Theorem I.7.5]. We did not find a reference for the variant we needed so we decided to include a proof[3].

[3] We do not claim that the result is new. The following mathoverflow post by A. Aizenbud shows that this was known to him in 2016: `https://mathoverflow.net/questions/254655/the-growth-of-the-hilbert-function-of-a-graded-ring`. The result is also related to the equality between Krull and Gelfand-Kirillov dimensions for finitely generated commutative algebras.

Proposition 5.4.3. *Let A be a finitely generated graded commutative k-algebra of nonzero Krull dimension. We do not assume that A is generated by elements of degree 1. Then its Hilbert function* $\mathrm{HF}_A(n) = \dim_k(A_n)$ *satisfies:*

$$\mathrm{HF}_A(n) = O^\sharp\left(n^{\dim_{Krull} A - 1}\right).$$

We prove Proposition 5.4.3 in multiple steps. First, we fix a graded commutative k-algebra A of finite nonzero Krull dimension, generated by elements $g_1, \dots, g_N$ of respective degrees $d_1, \dots, d_N$. Let W be the least common multiple of $d_1, \dots, d_N$. We prove the following lemma:

Lemma 5.4.4. *There exist (uniquely defined) polynomials $Q_0, \dots, Q_{W-1}$ such that, for all $m \in \{0, \dots, W-1\}$ and n large enough, we have:*

$$\mathrm{HF}_A(Wn + m) = Q_m(n).$$

Proof. Introduce the following formal power series, known as the Hilbert-Poincaré series:

$$F(t) = \sum_{n \geq 0} \mathrm{HF}_A(n) t^n.$$

The Hilbert-Serre theorem states that, for some polynomial $P \in \mathbb{Z}[X]$:

$$F(t) = \frac{P(t)}{\prod_{i=1}^N (1 - t^{d_i})}.$$

Since $(1 - t^{d_i})$ divides $(1 - t^W)$, we have:

$$F(t) = \frac{P_2(t)}{(1 - t^W)^N}.$$

for some polynomial $P_2 \in \mathbb{Z}[X]$. Moreover:

$$(1 - t^W)F(t) = \sum_{n \geq 0} \left(\mathrm{HF}_A(n) - \mathrm{HF}_A(n - W)\right) t^n,$$

where we use the convention $\mathrm{HF}_A(n - W) = 0$ if $n < W$. Denote by Δ the "finite difference" operator:

$$\Delta u_n = u_{n+1} - u_n.$$

and let $u_n^{(m)} = \mathrm{HF}_A(Wn+m)$. We have:

$$F(t) = \sum_{m=0}^{W-1} \sum_{n \geq 0} u_n^{(m)} t^{Wn+m}$$

and thus:

$$(1-t^W)F(t) = \sum_{m=0}^{W-1} \sum_{n \geq 0} - \left(\Delta u_n^{(m)}\right) t^{Wn+m}.$$

Continuing that way, we finally get:

$$P_2(t) = (1-t^W)^N F(t) = \sum_{m=0}^{W-1} \sum_{n \geq 0} (-1)^N \left(\Delta^N u_n^{(m)}\right) t^{Wn+m}.$$

This equality implies that $\Delta^N u_n^{(m)}$ is zero except for finitely many values of n and m. Fix an $m \in \{0, \ldots, W-1\}$. The sequence $(\Delta^N u_n^{(m)})$ is zero for large n, thus the sequence $(\Delta^{N-1} u_n^{(m)})$ is eventually constant, thus the sequence $(\Delta^{N-2} u_n^{(m)})$ is eventually linear, etc. We conclude that $u_n^{(m)}$ coincides, for n large enough, with a polynomial of degree $\leq N$: we have found the polynomial Q_m. This concludes the proof. □

We fix polynomials $Q_0, \ldots, Q_{W-1}$ as in Lemma 5.4.4. We show that the degree of the polynomial Q_0 is the expected exponent $\dim(A) - 1$:

Lemma 5.4.5. *The degree of the polynomial Q_0 is equal to* $\dim(A) - 1$.

Proof. The function $n \mapsto \mathrm{HF}_A(Wn)$ is the Hilbert function of the W-th truncation of A, i.e. of the k-algebra $A^{(W)}$ generated by homogeneous elements whose degree is a multiple of W. In the case of $A^{(W)}$, the Hilbert function is eventually polynomial (equal to Q_0), and it is well-known that the degree of this polynomial is $\dim A^{(W)} - 1$. Now, it follows from [EGA2, Proposition (2.4.7), page 30] that $\mathrm{Proj}(A) \simeq \mathrm{Proj}\left(A^{(W)}\right)$, and thus $\dim A^{(W)} = \dim A$. Putting everything together, we obtain:

$$\deg Q_0 = \dim A - 1.$$

□

Finally, we show that the other polynomials $Q_1, \ldots, Q_{W-1}$ have their degree bounded above by the degree of Q_0:

Lemma 5.4.6. *Let $m \in \{0, \ldots, W-1\}$. The degree of Q_m is at most equal to the degree of Q_0.*

Proof. The k-vector space A_{Wn+m} (of homogeneous elements of A of degree $Wn+m$) is generated by elements of the form:

$$x_{\underline{\alpha}} = \prod_{i=1}^{N} g_i^{\alpha_i}$$

for sequences $\underline{\alpha} \in (\{0, 1, \ldots\})^N$ such that $\sum_i \alpha_i d_i = Wn + m$. Given such a sequence, write the Euclidean division of each α_i by W:

$$\alpha_i = Wq_i + \alpha_i' \text{ with } \alpha_i' \in \{0, \ldots, W-1\}.$$

Now:

$$\sum_{i=1}^{N} \alpha'_i d_i = W\left(n - \sum_{i=1}^{N} q_i\right) + m.$$

Let $n' = n - \sum_i q_i$. We have:

$$Wn' + m = \sum_{i=1}^{N} \alpha'_i d_i \leq \sum_{i=1}^{N} W^2 = NW^2$$

and thus n' is bounded above by WN.

We have the factorization:

$$x_{\underline{\alpha}} = x_{\underline{\alpha}'} \times x_{\underline{q}}^{W}$$

with $x_{\underline{\alpha}'} \in A_{Wn'+m}$ and $x_{\underline{q}}^{W} \in A_{W(n-n')}$. This implies that the multiplication map on generators induces a surjection of vector spaces:

$$\bigoplus_{n'=0}^{WN} A_{Wn'+m} \otimes A_{W(n-n')} \twoheadrightarrow A_{Wn+m}.$$

Let D be the finite integer $\max_{n' \in \{0,1,\ldots,WN\}} \dim_k (A_{Wn'+m})$. We have:

$$\dim A_{Wn+m} \leq D \sum_{n'=0}^{WN} \dim A_{W(n-n')},$$

i.e., for n big enough:

$$Q_m(n) \leq D \sum_{n'=0}^{WN} Q_0(n - n')$$

which implies $\deg Q_m \leq \deg Q_0$. □

Put together, Lemmas 5.4.4 to 5.4.6 imply Proposition 5.4.3:

Proof of Proposition 5.4.3. By Lemma 5.4.4, we have:

$$\mathrm{HF}_A(n) \leq \sup_{m \in \{0,\ldots,W-1\}} Q_m\left(\frac{n-m}{W}\right).$$

By Lemmas 5.4.5 and 5.4.6, the degrees of the polynomials Q_m are at most $\dim(A) - 1$. Hence:

$$\mathrm{HF}_A(n) = O\left(n^{\dim(A)-1}\right).$$

Moreover, $\mathrm{HF}_A(n)$ coincides infinitely often (for every n multiple of W) with the polynomial $Q_0\left(\frac{n-m}{W}\right)$, which is of degree $\dim(A) - 1$ by Lemma 5.4.5. This shows that $\mathrm{HF}_A(n) \neq o\left(n^{\dim(A)-1}\right)$. This concludes the proof of Proposition 5.4.3. □

5.4.3. **The main lemma**

We now prove Lemma 5.4.7, which is a "technical" lemma. This result is the final ingredient needed for the proof of Theorem 5.1.4.

Lemma 5.4.7. *Let B be a finitely generated graded commutative k-algebra and I, J be homogeneous ideals of B. Assume that $I \cap J \subseteq \sqrt{0}$ and that any homogeneous ideal I' which satisfies $I' \cap J \subseteq \sqrt{0}$ is contained in $\sqrt{I}$. Let J' be the image of the ideal J in B/I. Then:*

$$\dim_k(J'_n) = O^\sharp\left(n^{\dim_{Krull}(B/I)-1}\right).$$

If moreover $\dim_k\left(\sqrt{I}\right)_n = O\left(n^{\dim_{Krull}(B/I)-2}\right)$, *then:*

$$\dim_k(J'_n) = \mathrm{HF}_{B/I}(n) + O\left(n^{\dim_{Krull}(B/I)-2}\right).$$

Proof. Replacing B by B/I, we may assume $I = 0$. This turns J into $J/(I \cap J) = J'$. The statement of the lemma becomes the following:

If every homogeneous ideal I' satisfying $I' \cap J \subseteq \sqrt{0}$ is included in $\sqrt{0}$, then $\dim_k(J_n) = O^\sharp\left(n^{\dim(B)-1}\right)$. If moreover $\dim_k(\sqrt{0})_n = O\left(n^{\dim(B)-2}\right)$, then

$$\dim_k(J_n) = \mathrm{HF}_B(n) + O\left(n^{\dim(B)-2}\right).$$

We assume that every homogeneous ideal I' satisfying $I' \cap J \subseteq \sqrt{0}$ is included in $\sqrt{0}$. First, since $J_n \subseteq B_n$, we have the obvious upper bound:

$$\dim(J_n) \leq \mathrm{HF}_B(n)$$

and in particular $\dim(J_n) = O\left(n^{\dim(B)-1}\right)$.

Let $p_1, \ldots, p_u$ be the minimal homogeneous prime ideals of B, whose number is finite since B is Noetherian.

Let $i \in \{1, \ldots, u\}$. We show that J is not contained in p_i. Assume by contradiction that $J \subseteq p_i$. Let V_i be the intersection of all minimal homogeneous primes of B distinct from p_i, i.e.:

$$V_i = p_1 \cap p_2 \cap \ldots \cap p_{i-1} \cap p_{i+1} \cap \ldots \cap p_u.$$

The ideal $V_i \cap p_i$ is the intersection of all minimal homogeneous primes of B, and is therefore equal to the nilradical $\sqrt{0}$. Since $J \subseteq p_i$, we have $V_i \cap J \subseteq V_i \cap p_i = \sqrt{0}$. By hypothesis, this implies $V_i \subseteq \sqrt{0}$. But then $V_i \subseteq p_i$ with p_i prime, and so one of the minimal prime ideals in the finite intersection defining V_i must be contained in p_i. This contradicts the minimality of p_i. We have shown that J is not contained in p_i.

For every $i \in \{1, \ldots, u\}$, choose a homogeneous element $H_i \in J \setminus p_i$, call its degree d_i, and denote by $\widetilde{H}_i$ its nonzero projection in the integral algebra B/p_i. The following map is injective:

$$\widetilde{H}_i^{W_i} : \begin{cases} (B/p_i)_{n-W_i d_i} & \to & (J/p_i)_n \\ x & \mapsto & \widetilde{H}_i^{W_i} x \end{cases}.$$

This proves that, for all $i \in \{1, \ldots, u\}$:

$$\dim_k((J/p_i)_n) \geq \dim_k((B/p_i)_{n-W_i d_i}) = \mathrm{HF}_{B/p_i}(n - W_i d_i). \tag{5.4.1}$$

For each B/p_i, let W_i be an integer and $Q_{i,0}, \ldots, Q_{i,W_i-1}$ be polynomials as in Lemma 5.4.4. Let also W and $Q_0, \ldots, Q_{W-1}$ be defined similarly for $B/\sqrt{0}$. By

Lemma 5.4.5, we know:

$$\deg(Q_{i,0}) = \dim(B/p_i) - 1 \qquad \text{for all } i \in \{1, \dots, u\}$$
$$\deg(Q_0) = \dim(B/\sqrt{0}) - 1$$

and by Lemma 5.4.6, we know that:

$$\deg(Q_{i,j}) \leq \dim(B/p_i) - 1 \qquad \text{for all } i \in \{1, \dots, u\} \text{ and } j \in \{0, \dots, W_i - 1\} \quad (5.4.2)$$
$$\deg(Q_j) \leq \dim(B/\sqrt{0}) - 1 \qquad \text{for all } j \in \{0, \dots, W - 1\}. \quad (5.4.3)$$

The ring $B/\sqrt{0}$ being reduced, we have (see Lemma 5.4.8 below):

$$\mathrm{HF}_{B/\sqrt{0}}(n) = \sum_{i=1}^{u} \mathrm{HF}_{B/p_i}(n) + O\left(n^{\dim(B/\sqrt{0})-2}\right) \quad (5.4.4)$$
$$\dim_k((J/\sqrt{0})_n) = \sum_{i=1}^{u} \dim_k((J/p_i)_n) + O\left(n^{\dim(B/\sqrt{0})-2}\right) \quad (5.4.5)$$

Combined with Equation (5.4.1), this yields:

$$\dim_k((J/\sqrt{0})_n) \geq \sum_{i=1}^{u} \mathrm{HF}_{B/p_i}(n - W_i d_i) + O\left(n^{\dim(B/\sqrt{0})-2}\right).$$

By the properties of the polynomials $Q_{i,j}$ (cf. Lemma 5.4.4 and Equation (5.4.2)), the function $\mathrm{HF}_{B/p_i}(n - W_i d_i)$ coincides with $\mathrm{HF}_{B/p_i}(n)$ up to a $O\left(n^{\dim(B/p_i)-2}\right)$, and thus also up to a $O\left(n^{\dim(B/\sqrt{0})-2}\right)$. Hence:

$$\dim_k((J/\sqrt{0})_n) \geq \sum_{i=1}^{u} \mathrm{HF}_{B/p_i}(n) + O\left(n^{\dim(B/\sqrt{0})-2}\right).$$

Using Equation (5.4.4):

$$\dim_k((J/\sqrt{0})_n) \geq \mathrm{HF}_{B/\sqrt{0}}(n) + O\left(n^{\dim(B/\sqrt{0})-2}\right).$$

Using the fact that $\dim_k(J_n) \geq \dim_k((J/\sqrt{0})_n)$ and $\dim(B) = \dim(B/\sqrt{0})$, we obtain:

$$\dim_k(J_n) \geq \mathrm{HF}_{B/\sqrt{0}}(n) + O\left(n^{\dim(B)-2}\right).$$

By Proposition 5.4.3, we have $\mathrm{HF}_{B/\sqrt{0}}(n) = O^\sharp\left(n^{\dim(B/\sqrt{0})-1}\right) = O^\sharp\left(n^{\dim(B)-1}\right)$. This is enough to establish the first half of the lemma[4].

Assume now that $\dim_k(\sqrt{0})_n = O\left(n^{\dim(B)-2}\right)$. We have:

$$\begin{aligned}\dim_k(J_n) &\geq \mathrm{HF}_{B/\sqrt{0}}(n) + O\left(n^{\dim(B)-2}\right)\\ &= \mathrm{HF}_B(n) - \dim_k(\sqrt{0})_n + O\left(n^{\dim(B)-2}\right)\\ &= \mathrm{HF}_B(n) + O\left(n^{\dim(B)-2}\right).\end{aligned}$$

This establishes the second half of the lemma. □

In the proof, we have used the following lemma:

[4] The first half of the lemma can be proved by applying Equation (5.4.1) to a single minimal prime ideal p such that $\dim(B/p) = \dim(B)$ (in particular, we do not need Lemma 5.4.8), cf. the proof in [Seg22].

Lemma 5.4.8. *Let A be a reduced finitely generated graded commutative k-algebra. Let $p_1, \dots, p_r$ be the minimal homogeneous prime ideals of A. Then:*

$$\mathrm{HF}_A(n) = \sum_{i=1}^{r} \mathrm{HF}_{A/p_i}(n) + O\left(n^{\dim(A)-2}\right).$$

Proof. For each $i \in \{1, \dots, r+1\}$, let $V_i = p_1 \cap \dots \cap p_{i-1}$. Note that $V_1 = A$, and $V_{r+1} = 0$ since A is reduced. We show the following result by induction on k: for each $k \in \{1, \dots, r+1\}$, we have:

$$\mathrm{HF}_{A/V_k}(n) = \sum_{i=1}^{k-1} \mathrm{HF}_{A/p_i}(n) + O\left(n^{\dim(A)-2}\right).$$

The case $k = 1$ is clear, and the case $k = r+1$ is the announced result.

Assume we have shown the result for some $k \in \{1, \dots, r\}$. We have the exact sequence of graded k-vector spaces:

$$0 \to A/V_{k+1} \to A/V_k \times A/p_k \to A/(V_k + p_k) \to 0. \tag{5.4.6}$$

Let us show $\dim(A/(V_k + p_k)) < \dim(A)$. If $k = 1$, this is clear, so we assume $k \geq 2$. Assume these Krull dimensions are equal; then, there is a sequence of $\dim(A) + 1$ homogeneous prime ideals $q_0 \subset \dots \subset q_{\dim(A)}$ such that:

$$V_k + p_k \subseteq q_0 \subset \dots \subset q_{\dim(A)}$$

We have an inclusion $p_k \subseteq q_0$ with p_k prime, and this inclusion cannot be strict since otherwise we have $\dim(A/p_k) \geq \dim(A) + 1 > \dim(A/p_k)$. Therefore $q_0 = p_k$. But then $V_k + p_k \subseteq p_k$ implies $V_k \subseteq p_k$. Since V_k is an intersection of finitely many ideals $p_1, \dots, p_{k-1}$ contained in the prime ideal p_k, we have $p_i \subsetneq p_k$ for some $i \in \{1, \dots, k-1\}$. This contradicts the minimality of p_k.

We have shown $\dim(A/(V_k + p_k)) < \dim(A)$. Consequently:

$$\dim(A/(V_k + p_k))_n = O\left(n^{\dim(A)-2}\right).$$

Combined with the exact sequence of Equation (5.4.6) and the induction hypothesis, this implies:

$$\mathrm{HF}_{A/V_{k+1}}(n) = \sum_{i=1}^{k} \mathrm{HF}_{A/p_i}(n) + O\left(n^{\dim(A)-2}\right).$$

We conclude by induction. □

5.4.4. The dimension of $\gamma_{\xi}(H)$

We are ready to prove Theorem 5.1.4 : the dimension of the set $\gamma_{\xi}(H)$ is one more than the splitting number $\Omega(D_H)$.

Proof of Theorem 5.1.4. We want to apply Lemma 5.4.7 with:

$$(B,\, J,\, I) = (R^H,\, I_H \cap R^H,\, \Gamma_H \cap R^H),$$

where Γ_H is as in Theorem 5.4.1. We check the hypotheses:

— R^H is a finitely generated graded commutative k-algebra. Indeed it is a quotient of R (Proposition 3.4.26) which is finitely generated (Corollary 3.4.18) and commutative.

— $I_H \cap R^H$ and $\Gamma_H \cap R^H$ are homogeneous ideals of R^H.

— Let us verify that $\Gamma_H \cap I_H \cap R^H \subseteq \sqrt{0}$, where $\sqrt{0}$ is the nilradical of R^H. We know that:

$$\Gamma_H \cap I_H \subseteq \Gamma_H \cap \sqrt{I_H} = \sqrt{I_H^*},$$

and so $\Gamma_H \cap I_H \cap R^H \subseteq \sqrt{I_H^*} \cap R^H = \sqrt{0}$.

— If $I' \cap I_H \cap R^H \subseteq \sqrt{0}$, then $I' \cap \sqrt{I_H} \subseteq \sqrt{I_H^*}$ and thus I' is contained in Γ_H by Theorem 5.4.1 (iv).

We can therefore apply the first part of Lemma 5.4.7. We obtain:

$$\dim_k \left(\frac{I_H \cap R^H}{\Gamma_H \cap I_H \cap R^H} \right)_n = O^\sharp\left(n^{\dim(R^H/(\Gamma_H \cap R^H))-1} \right) = O^\sharp\left(n^{\dim \gamma_\xi(H)-1} \right). \quad (5.4.7)$$

We have used Proposition 5.4.2 for the last step. Let $R_{n,H}$ be the space spanned by components of group H and of degree n and $N_{n,H}$ be the subspace of elements of $R_{n,H}$ nilpotent in R. We have:

$$\begin{aligned} \dim_k R_{n,H} &= \dim_k \left(I_H \cap R^H \right)_n \\ &= \dim_k \left(\frac{I_H \cap R^H}{\Gamma_H \cap I_H \cap R^H} \right)_n + O\Big(\dim_k(N_{n,H}) \Big). \end{aligned}$$

Using Equation (5.4.7), we get:

$$\dim_k R_{n,H} = O^\sharp\left(n^{\dim \gamma_\xi(H)-1} \right) + O\Big(\dim_k(N_{n,H}) \Big).$$

Now, Theorem 4.4.2 (ii) and Theorem 5.3.1 imply that $\dim_k R_{n,H} = O^\sharp\left(n^{\Omega(D_H)} \right)$ and $\dim_k N_{n,H} = o\left(\dim_k R_{n,H}\right)$. This implies:

$$\Omega(D_H) = \dim \gamma_\xi(H) - 1.$$

This concludes the proof. □

5.4.5. The degree of $\gamma_\xi(H)$

In this subsection, we detail how the results of Section 4.5 may be used to obtain more precise results concerning the geometry of the subsets $\gamma_\xi(H)$. We come back to where the proof of Theorem 5.1.4 ended, including all notation and hypotheses. To apply the second half of Lemma 5.4.7, we need to check:

$$\dim_k(\sqrt{\Gamma_H} \cap R^H)_n = O\left(n^{\dim(R^H/(\Gamma_H \cap R^H))-2} \right),$$

i.e.:

$$\dim_k(\Gamma_H \cap R^H)_n = O\left(n^{\Omega(D_H)-1} \right).$$

We do not write the details, as the proof of this fact is similar to previous proofs, cf. Section 5.3. We simply sketch the argument: Let y be an M-big component of group H (Definition 3.4.40). If $x \in R^H \cap \Gamma_H$, then $xy \in I_H$, and since $x \in \Gamma_H$ this implies $xy \in \sqrt{I_H^*} \cap R^H = \sqrt{0}$. But multiplication by y is injective for "most" elements x (i.e. for a subspace of the space of elements of degree n which is of codimension

$O\left(n^{\Omega(D_H)-1}\right)$, cf. Lemma 4.5.1 and Theorem 3.4.39), and therefore the dimension of $(\Gamma_H \cap R^H)_n$ is essentially bounded above by the dimension of the space of nilpotent elements of degree $n + \deg(y)$, which is a $O\left(n^{\Omega(D_H)-1}\right)$ by Theorem 5.3.1.

From the second half of Lemma 5.4.7, we therefore have:

$$\dim_k \left(\frac{I_H \cap R^H}{\Gamma_H \cap I_H \cap R^H}\right)_n = \mathrm{HF}_{R^H/(\Gamma_H \cap R^H)}(n) + O\left(n^{\Omega(D_H)-1}\right)$$

and thus:

$$\dim_k R_{n,H} = \mathrm{HF}_{R^H/(\Gamma_H \cap R^H)}(n) + O\left(n^{\Omega(D_H)-1}\right). \tag{5.4.8}$$

If we assume that all non-factorizable elements of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ have the same degree W, and that there are N of them, then the Proj of the ring of components embeds in the projective space $\mathbb{P}^N$, and we can compute the degree[5] of the closed subset $\overline{\gamma_\xi(H)}$ (we define the degree of a non-irreducible subset as the sum of the degrees of its irreducible components of maximal dimension) – note that we consider Proj instead of Spec: we have quotiented out by the action of $k^\times$ and all dimensions are one less than previously computed. In this case we know that $\mathrm{HF}_{R^H/(\Gamma_H \cap R^H)}(n)$ and $R_{n,H}$ are zero if n is not a multiple of W, and coincide with polynomials P_1, P_2 of degree $\Omega(D_H)$ when evaluated at big enough multiples of W. Moreover, by Equation (5.4.8), the leading monomials of these two polynomials are given by the same monomial:

$$\dim_k(R_{Wn,H}) \sim \mathrm{HF}_{R^H/(\Gamma_H \cap R^H)}(Wn) \sim \alpha(Wn)^{\Omega(D_H)}.$$

Classically, the number $\Omega(D_H)!\alpha$ computes the degree of $R^H/(\Gamma_H \cap R^H)$, i.e. of $\overline{\gamma_\xi(H)}$ embedded in $\mathbb{P}^N$. The results of Section 4.5 give computations of α, and consequently of the degree of $\overline{\gamma_\xi(H)}$, in various situations:

— If H is a non-splitter, then $\Omega(D_H) = 0$ and $\alpha = |H_2(H, c_H)|$. (cf. Subsection 4.5.4)

  In this case, $\overline{\gamma_\xi(H)}$ (seen as embedded in the projective space $\mathbb{P}^N$) is of dimension zero: it is a union of finitely many points. The degree is then precisely the number of these points: there are $|H_2(H, c_H)|$ of them.

  Remark 5.4.9. If one sees $\overline{\gamma_\xi(H)}$ as embedded in affine space $\mathbb{A}^N$ (as we do in other sections), it is a union of $|H_2(H, c_H)|$ lines going through the origin 0.

— Assume D consists of a single conjugacy class c of G and $\xi(c) = 1$. Let s be the number of conjugacy classes that c splits into in H. Then $\Omega(D_H) = s - 1$ and, by Remark 4.5.10:

$$\alpha = \frac{\mathrm{ord}(c)\,|H_2(H, c_H)|}{\left|H^{\mathrm{ab}}\right|\,(s-1)!}.$$

  The degree of $\overline{\gamma_\xi(H)}$, seen as embedded in $\mathbb{P}^N$, is then given by:

$$\frac{\mathrm{ord}(c)\,|H_2(H, c_H)|}{\left|H^{\mathrm{ab}}\right|}.$$

[5] A similar computation is possible when non-factorizable elements have different degrees – one should then take an average of the coefficients in front of $n^{\Omega(D_H)}$ –, but there does not seem to be a consensual notion of degree for subspaces of weighted projective spaces.

5.5. Description of the spectrum

In this section, we prove additional properties of the spectrum of the ring of components. Main results are Theorem 5.5.1 and Theorem 5.5.13. The section is organized as follows:

— In Subsection 5.5.1, we identify a subset of dimension 1 of $\gamma_{\xi}(H)$ (Theorem 5.5.1). In some situations, we prove that this is all of $\gamma_{\xi}(H)$.

— In Subsection 5.5.2, we define free factor families of subgroups of G and factored splitters, and we inspect the properties of these objects.

— In Subsection 5.5.3, we prove Theorem 5.5.13, which describes the spectrum entirely under strong assumptions.

5.5.1. A line in each $\gamma_{\xi}(H)$

We fix a nontrivial D-generated subgroup H of G. Let $p_1, \dots, p_N$ be the non-factorizable components of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$, ordered in such a way that the components whose group is contained in H come first: we denote by M their number, so they are $p_1, \dots, p_M$. Let $d(i)$ be the degrees of the components p_i for $i \in \{1, \dots, N\}$, and D be the greatest common divisor of $d(1), \dots, d(N)$. Let:

$$q(i) \overset{\text{def}}{=} \frac{d(i)}{D} \in \mathbb{N}.$$

Finally, for $\lambda \in k$, let $p_H(\lambda)$ be the following point of $\mathbb{A}^N(k)$ (with coordinates ordered as above):

$$p_H(\lambda) \overset{\text{def}}{=} (\lambda^{q(1)}, \lambda^{q(2)}, \dots, \lambda^{q(M)}, 0, \dots, 0).$$

We state and prove Theorem 5.5.1:

Theorem 5.5.1. *The set $\gamma_{\xi}(H)$ contains the points $p_H(\lambda)$ for $\lambda \in k^{\times}$. Moreover, if there is at most one component of group H for each degree*[6]*, then there are no other points: $\gamma_{\xi}(H) = p_H(k^{\times})$ and $\overline{\gamma_{\xi}(H)} = p_H(k)$.*

Theorem:
Description of a line in each $\gamma_{\xi}(H)$

[6] This hypothesis implies that H is a non-splitter and $H_2(H, c_H) = 1$ by Theorem 4.3.1 (ii). This result is an « effective » version of the case $H_2(H, c_H) = 1$ of Remark 5.4.9.

In particular, the set $\gamma_{\xi}(H)$ always contains the point:

$$p_H(1) = (\underbrace{1, 1, 1, \dots, 1}_{\text{non-factorizable components of group } \subseteq H}, \underbrace{0, \dots, 0}_{\text{other non-factorizable components}}).$$

Proof. Let A' be the homogeneous ideal generated by the differences $m - m'$, for couples m, m' of components of same degree whose groups are contained in H, and let $A = A' + J_H^*$. Then R/A is isomorphic to the following subring of $k[X]$:

$$k[X^{d(1)}, \dots, X^{d(M)}].$$

In particular, R/A is integral so A is a prime ideal of R.

— **Step 1: Describe $Z(A)$.** A point $(x_1, \dots, x_N) \in \mathrm{Spec}(R)(k)$ is in $Z(A)$ if $x_{M+1} = \dots = x_N = 0$ and every product of the x_i is equal to any other one when the degrees match. Using Bézout's identity, write:

$$D = \sum_{i=1}^{M} a_i d(i)$$

for some $(a_i) \in \mathbb{Z}^M$. For each $i \in \{1, \dots, M\}$, we have, in R/A:

$$p_i \left(\prod_{j \text{ s.t. } a_j \leq 0} p_j^{-a_j} \right)^{q(i)} = \left(\prod_{j \text{ s.t. } a_j \geq 0} p_j^{a_j} \right)^{q(i)}$$

because both sides are components of same degree, since $d(i) = q(i)D = q(i)\sum a_j d(j)$. Hence, $(x_1, \ldots, x_M, 0, \ldots, 0) \in Z(A)$ means that we have for all $i \in \{1, \ldots, M\}$:

$$x_i = \left(\prod_j x_j^{a_j}\right)^{q(i)} = \lambda^{q(i)}$$

for some $\lambda \in k$ independent of i. So $Z(A)$ is the set of points of $\mathbb{A}^N(k)$ of the form:

$$(\lambda^{q(1)}, \lambda^{q(2)}, \ldots, \lambda^{q(M)}, 0, \ldots, 0) \text{ with } \lambda \in k.$$

The coordinates of such a point satisfies the equalities defining R, since these are equalities between components of same degree and same group.

— **Step 2: Show that $Z(A) \setminus \{0\}$ is contained in $\gamma_{\xi}(H)$.** The ideal I_H contains the product of all non-factorizable components whose group is contained in H, i.e. the product $p_1 p_2 \cdots p_M$. This component cancels a point:

$$(x_1, x_2, \ldots, x_M, x_{M+1}, \ldots, x_N)$$

if and only if $x_1 x_2 \ldots x_M = 0$. Now if the point $(x_1, x_2, \ldots, x_N)$ belongs to $Z(A)$, it is of the form:

$$(\lambda^{q(1)}, \lambda^{q(2)}, \ldots, \lambda^{q(M)}, 0, \ldots, 0) \text{ for some } \lambda \in k.$$

So if $(x_1, x_2, \ldots, x_N)$ is in $Z(A) \cap Z(I_H)$, we must have $\lambda^{\sum_i q(i)} = 0$, i.e. $\lambda = 0$. This shows $Z(A) \cap Z(I_H) = \{0\}$, i.e. $Z(A) \setminus \{0\} \subseteq Z(I_H)^c$.

Since A contains J_H^*, we also have $Z(A) \subseteq Z(J_H^*)$, and thus $Z(A) \setminus \{0\} \subseteq Z(I_H)^c \cap Z(J_H^*) = \gamma_{\xi}(H)$. This is the first part of the theorem.

— **Step 3: Show that $Z(A) = \gamma_{\xi}(H) \cup \{0\}$ when there is at most one component of group H for each degree.** Let us show that $A \cap I_H = I_H^*$. If we work in $R' = R/I_H^*$, this amounts to showing that the restriction of the projection map $R' \twoheadrightarrow R/A$ to I_H/I_H^* is injective. Let S be the subset of $\{0, 1, \ldots\}$ consisting of values k such that there is a component of degree k of group H, and F_k be the only component of group H of degree k for $k \in S$. An element of I_H is of the form:

$$x = \sum_{k \in S} \lambda_k F_k + \underbrace{x_{\supsetneq H}}_{\in I_H^*}$$

which projects to $\sum_{k \in S} \lambda_k F_k$ in R'. The image of x in R/A, which we see as a subring of $k[X]$, is:

$$\sum_{k \in S} \lambda_k X^k.$$

and it is clear that this mapping is injective as a map $I_H/I_H^* \to R'/A$. So we have $A \cap I_H = I_H^*$ and thus:

$$Z(A) \cup Z(I_H) = Z(I_H^*)$$

and hence $\gamma_{\xi}(H) \subseteq Z(A)$. Since $Z(A)$ is closed we have:

$$Z(A) \supseteq \overline{\gamma_{\xi}(H)} \supseteq \gamma_{\xi}(H) \cup \{0\}.$$

We have already shown that $Z(A) \subseteq \gamma_{\xi}(H) \cup \{0\}$. We obtain the desired equality:

$$Z(A) = \overline{\gamma_{\xi}(H)} = \gamma_{\xi}(H) \cup \{0\}.$$

□

5.5.2. **Free factor families and factored splitters**

In this subsection, we describe $\mathrm{Spec}(R)(k)$ entirely in a particular case, essentially asking that all D-generated subgroups be products of non-splitters. This condition is satisfied in the case of symmetric groups which we study in Chapter 6. We start with some definitions:

Definition: *Free family of subgroups*

Definition 5.5.2. A family $H_1, \dots, H_k$ of subgroups of G is *free* if the two following conditions are met:

— For all disjoint subsets A, B of $\{1, \dots, k\}$, we have $\langle (H_i)_{i\in A}\rangle \cap \langle (H_j)_{j\in B}\rangle = 1$.

— Elements of H_i commute with elements of H_j when $i \neq j$.

Definition: *Product of a free family of subgroups (Zappa-Szép product)*

Definition 5.5.3. If $H_1, \dots, H_k$ is a free family of subgroups of G, the *product* of this family is the subgroup $\langle H_1, \dots, H_k\rangle$ of G.

The product of a free family $H_1, \dots, H_k$ is isomorphic, as a group, to the direct product of the groups H_i.

Definition: *Factor family*

Definition 5.5.4. A *factor family* of H is a family $H_1, \dots, H_k$ of D-generated subgroups contained in H such that every non-factorizable component whose group is contained in H has its group contained in one of the subgroups H_i.

Proposition: *Factor families are generating families*

Proposition 5.5.5. *Let $H \in \mathrm{Sub}_{G,D}$ and $H_1, \dots, H_k$ be a factor family of H. Then $H_1, \dots, H_k$ generate H.*

Proof. Using Proposition 3.2.22, we fix a component $x \in \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$ of group H. Write x as a product of non-factorizable components $x = x_1 \cdots x_r$. Since $H_1, \dots, H_k$ is a factor family, each factor in this product has its group contained in some H_i. Hence $H = \langle x\rangle = \langle x_1, \dots, x_r\rangle$ is contained in $\langle H_1, \dots, H_k\rangle$. □

Proposition: *Characterization of factor families and free families*

Proposition 5.5.6. *Let $H \in \mathrm{Sub}_{G,D}$ and $H_1, \dots, H_k$ be a family of subgroups of H, all D-generated. Denote by Φ the following morphism:*

$$\Phi : \begin{cases} R^{H_1} \otimes \dots \otimes R^{H_k} & \to & R^H \\ m_1 \otimes \dots \otimes m_k & \mapsto & m_1 \dots m_k \end{cases}.$$

Then:

(i) $H_1, \dots, H_k$ is a factor family if and only if Φ is surjective.

(ii) If $H_1, \dots, H_k$ is free, then Φ is injective.

Proof.

(i) Let us prove point (i).

($\Leftarrow$) Assume Φ is surjective and consider an arbitrary non-factorizable component $m \in R^H$. Since it is a component and it is in the image of Φ, it is equal to a product $m_1 \dots m_k$ with m_i a component in R^{H_i}. Since m is non-factorizable, at most one of the components m_i is non-trivial. Therefore, we have $m = m_i$ for some i, and thus m has its group included in some H_i. Since this holds for any non-factorizable component, $H_1, \dots, H_k$ is a factor family.

($\Rightarrow$) Conversely, assume $H_1, \dots, H_k$ is a factor family. To prove that Φ is surjective, it is enough to show that its image contains non-factorizable components. Let $m \in R^H$ be an arbitrary non-factorizable component. By hypothesis, it is contained in some R^{H_i}. Then $m = \Phi(1 \otimes \dots \otimes 1 \otimes m \otimes 1 \otimes \dots \otimes 1)$ lies in the image of Φ. This shows that Φ is surjective.

(ii) Let us prove point (ii).

Assume that the family (H_i) is free. To prove that Φ is injective, we assume that for some $m_j, m'_j \in R^{H_j}$, we have:

$$\prod_{j=1}^{k} m_j = \prod_{j=1}^{k} m'_j.$$

Since the subgroups H_i commute with each other, elementary braids do not change the elements or their position "among elements of the same subgroup" when they swap two elements from different subgroups H_i. Hence, one may assume that we have a braid linking $\prod_{j=1}^{k} m_j$ and $\prod_{j=1}^{k} m'_j$ in which no elementary braid exchanges elements belonging to different subgroups H_j. But from such a braid, one can extract braids relating m_j and m'_j for each $j \in \{1, \dots, k\}$. Thus Φ is injective.

□

Definition: *Factored splitter*

Definition 5.5.7. We say that $H \in \mathrm{Sub}_{G,D}$ is a *factored splitter* if there exists a free factor family of H of size at least 2.

Proposition: *Factored splitters are splitters*

Proposition 5.5.8. *If $H \in \mathrm{Sub}_{G,D}$ is generated by a free family $H_1, \dots, H_k$ of D-generated subgroups with $k \geq 2$, then it is a splitter.*

In particular, factored splitters are splitters, since they are generated by a free family by Proposition 5.5.5.

Proof. Consider a conjugacy class $c \in D$. Since the subgroups H_i are D-generated, $H_i \cap c$ is non-empty. Choose elements $g_1 \in H_1 \cap c$ and $g_2 \in H_2 \cap c$. It suffices to show that g_1 and g_2 are not conjugate in H to prove that H splits c.

Let $\gamma \in H$. Since $H_1, \dots, H_k$ is a free family that generates H, we can write γ uniquely as a product $\gamma_1 \dots \gamma_k$ with $\gamma_i \in H_i$. Now compute:

$$g_1^{\gamma} = \gamma_1 \dots \gamma_k g_1 \gamma_k^{-1} \dots \gamma_1^{-1} = \gamma_1 g_1 \gamma_1^{-1} \in H_1.$$

So g_1 is conjugate only with elements in $c \cap H_1$, and thus not with g_2. This argument actually shows that c splits into at least k conjugacy classes in H, and thus $\Omega(D_H) \geq |D|\,(k-1)$. □

We give a group-theoretical way to identify some factor families:

Proposition: *Group-theoretical criterion for factor families*

Proposition 5.5.9. *Assume that $|D| = 1$ and $\xi = 1$, i.e. consider a single conjugacy class c. Assume H is a subgroup of G generated by subgroups $H_1, \dots, H_k$ such that:*

— *For all $i \in \{1, \dots, k\}$, the subgroup H_i has a trivial intersection with $\langle (H_j)_{j \neq i} \rangle$.*

— $c \cap H = \bigsqcup_{i=1}^{k} (c \cap H_i)$.

Then $H_1, \dots, H_k$ is a factor family of H.

Proof. For $i \in \{1, \dots, k\}$, let $d_i = c \cap H_i$. Consider a non-factorizable component whose group is contained in H. Since braids can move conjugacy classes freely, one may choose a representing tuple of the form:

$$\underline{g} = (g_{1,1}, \dots, g_{1,n(1)}, \dots, g_{k,1}, \dots, g_{k,n(k)})$$

with $g_{i,j} \in d_i$. Now let $\pi_i = g_{i,1} \cdots g_{i,n(i)}$. We know that $\pi_i \in H_i$ but also $\pi_1 \cdots \pi_k = 1$. Hence $\pi_i = (\pi_{i+1} \cdots \pi_k \pi_1 \cdots \pi_{i-1})^{-1} \in \langle (H_j)_{j \neq i} \rangle$. This implies $\pi_i = 1$ since $H_i \cap \langle (H_j)_{j \neq i} \rangle = 1$.

Therefore, all the tuples $\underline{g}_i = (g_{i,1}, \dots, g_{i,n(i)}) \in d_i^{n(i)}$ define components. Since m is non-factorizable, it is equal to one of its factors and thus $\langle m \rangle$ is contained in some H_i. □

5.5.3. **Factored splitters and the spectrum of the ring of components**

Proposition: *A factor family of H gives a decomposition of $\gamma_\xi(H)$*

Proposition 5.5.10. *Let $H \in \mathrm{Sub}_{G,D}$ and $H_1, \dots, H_k$ a factor family of H. For each $j \in \{1, \dots, k\}$, denote by φ_j the map $\mathrm{Spec}(R^H)(k) \to \mathrm{Spec}(R^{H_j})(k)$ induced by the inclusion $R^{H_j} \hookrightarrow R^H$ and by γ_j the inverse image of $\gamma_\xi(H_j)$ (computed in R^{H_j}) by φ_j, which is a subset of $\mathrm{Spec}(R^H)(k)$. Then:*

$$\gamma_\xi(H) \supseteq \bigcap_{j=1}^{k} \gamma_j.$$

Moreover, if the family $(H_1, \dots, H_k)$ is free, we have:

$$\gamma_\xi(H) = \bigcap_{j=1}^{k} \gamma_j \simeq \prod_{j=1}^{k} \gamma_\xi(H_j).$$

Proof. We think in terms of subsets of $\mathrm{Spec}(R^H)(k) = Z(J_H^*)$ since all the sets considered are contained in $Z(J_H^*)$. Thus $\gamma_\xi(H) = Z(I_H^*) \setminus Z(I_H) = Z(I_H)^c$. Since $\left\langle (H_j)_{j \in \{1,\dots,k\}} \right\rangle = H$, we know:

$$Z(I_H) = \bigcup_{j=1}^{k} Z(I_{H_j}).$$

This implies:

$$\gamma_\xi(H) = \bigcap_{j=1}^{k} Z(I_{H_j})^c.$$

To prove the first point, it suffices to show, for each $j \in \{1, \dots, k\}$:

$$Z(I_{H_j})^c \supseteq \gamma_j.$$

Let $j \in \{1, \dots, k\}$. Order the non-factorizable components of R^H such that $p_1, \dots, p_M$ have group contained in H_j, and $p_{M+1}, \dots, p_N$ do not. In terms of coordinates, φ_j is the map:

$$(x_1, \dots, x_M, x_{M+1}, \dots, x_N) \mapsto (x_1, \dots, x_M).$$

And γ_j is the set of points of $\mathrm{Spec}(R^H)(k)$ of the form:

$$(x_1, \dots, x_M, x_{M+1}, \dots, x_N) \text{ with } (x_1, \dots, x_M) \in \gamma_\xi(H_j) = Z(J_{H_j}^*) \cap Z(I_{H_j})^c.$$

We can reformulate:

— γ_j is the set of points $(x_1, \dots, x_N)$ of $\mathrm{Spec}(R^H)(k)$ for which there is a component $p_{i_1} \dots p_{i_k}$ of group exactly H_j (which is necessarily in $R^{H_j} = k[p_1, \dots, p_M]$, and thus $i_1, \dots, i_k \leq M$) such that $x_{i_1} \dots x_{i_k} \neq 0$.

— $Z(I_{H_j})^c$ is the set of points $(x_1, \dots, x_N)$ of $\mathrm{Spec}(R^H)(k)$ such that there exists a component $p_{i_1} \dots p_{i_k}$ of group containing H_j such that $x_{i_1} \dots x_{i_k} \neq 0$.

With this description, it is clear that we always have $\gamma_j \subseteq Z(I_{H_j})^c$, and thus:

$$\gamma_\xi(H) \supseteq \bigcap_{j=1}^{k} \gamma_j.$$

We now assume that the family $H_1, \dots, H_k$ is free, and we show:

$$\gamma_j = Z(I_{H_j})^c.$$

Consider a point $x = (x_1, \dots, x_N) \in Z(I_{H_j})^c$. By the description above, one may choose a component $m = p_{i_1} \dots p_{i_k}$ of group $H' \supseteq H_j$ such that $x_{i_1} \dots x_{i_k} \neq 0$.

Let m_1 be the product of the non-factorizable components p_{i_t} of group contained in H_j, and m_2 be the product of the other factors. We have $m = m_1 m_2$. Let H_1' be the group generated by m_1 and H_2' the group generated by m_2. We know that $\langle H_1', H_2' \rangle = H' \supseteq H_j$.

We have: $H_1' \subseteq H_j = \langle p_1, \dots, p_M \rangle$ and $H_2' \subseteq \langle p_{M+1}, \dots, p_N \rangle$. Since the family $H_1, \dots, H_k$ is free, we know that H_1' and H_2' have trivial intersection and commute with each other.

Let us show that $H_1' = H_j$. Let $a \in H_j$. Then $a \in H'$ so we can write $a = a_1 a_2$ with $a_1 \in H_1'$, $a_2 \in H_2'$. But then $a a_1^{-1} = a_2$, with $a a_1^{-1} \in H_j$ and $a_2' \in H_2'$. Since $H_j \cap H_2' = 1$, this shows that $a a_1^{-1} = 1$, i.e $a = a_1$ and thus $a \in H_1'$.

So m_1 is a component of group exactly H_j. The corresponding coordinates x_{i_t} of x are nonzero by choice of m. Hence $x \in \gamma_j$ by the description above.

We have shown the equality $Z(I_{H_j})^c = \gamma_j$ and thus:

$$\gamma_\xi(H) = \bigcap_{j=1}^{k} \gamma_j.$$

Since the factor family is free, there is a partition $P_1, \dots, P_k$ of $\{1, \dots, N\}$ such that the non-factorizable components of group H_j are exactly the p_i for $i \in P_j$. Saying that a point is in γ_j means that the point obtained by keeping all coordinates x_i for $i \in P_j$ is in $\gamma_\xi(H_j)$. An element in $\bigcap_{j=1}^k \gamma_j$ can be transformed into an element of $\prod_{j=1}^k \gamma_\xi(H_j)$ by separating coordinates according to the partition, and reciprocally an element of $\prod_{j=1}^k \gamma_\xi(H_j)$ may be concatenated into an element of $\bigcap_{j=1}^k \gamma_j$. This gives an explicit version of the homeomorphism:

$$\gamma_\xi(H) \simeq \prod_{j=1}^{k} \gamma_\xi(H_j)$$

whose existence can also be deduced from Proposition 5.5.6. □

In what follows, let $p_1, \dots, p_N \in R$ be the non-factorizable components of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, D, \xi)$, let $d(1), \dots, d(N)$ be their respective degrees and denote by $e_1, \dots, e_N$ the corresponding basis elements of $\mathbb{A}^N(k)$.

Definition: *The point e_H*

Definition 5.5.11. If $H \in \mathrm{Sub}_{G,D}$, let:

$$e_H \overset{\text{def}}{=} \sum_{i \text{ such that } \langle p_i \rangle \subseteq H} e_i.$$

Definition: *Weighted span*

Definition 5.5.12. Let $x_1, \ldots, x_n$ be a family of vectors in $\mathbb{A}^N(k)$, which we decompose as:

$$x_j = \sum_{i=1}^{N} \xi_{i,j} e_i.$$

We define the *weighted span* of the family $x_1, \ldots, x_n$ as the set:

$$\left\{ \sum_{i=1}^{N} \sum_{j=1}^{n} \lambda_j^{d(i)} \xi_{i,j} e_i \;\middle|\; (\lambda_1, \ldots, \lambda_n) \in k^n \right\}.$$

We also define the *strict weighted span* of the family $x_1, \ldots, x_n$ as its weighted span, minus the weighted span of any of the n subfamilies of size $n-1$, i.e.:

$$\left\{ \sum_{i=1}^{N} \sum_{j=1}^{n} \lambda_j^{d(i)} \xi_{i,j} e_i \;\middle|\; (\lambda_1, \ldots, \lambda_n) \in (k^\times)^n \right\}.$$

When the degrees $d(i)$ are all equal, the weighted span of $x_1, \ldots, x_n$ is the regular vector subspace of k^N spanned by $x_1, \ldots, x_n$. For a more interesting example, take $N = 2, d(1) = 1, d(2) = r$. The weighted span of the point $(1,1)$ is the graph of $x \mapsto x^r$ in k^2.

We now prove Theorem 5.5.13, which gives a description of the sets $\gamma_\xi(H)$ for $H \in \mathrm{Sub}_{G,D}$. By Proposition 5.1.3, these sets form a partition of $\mathrm{Spec}(R)(k)$, so we obtain a full description of $\mathrm{Spec}(R)(k)$.

Theorem: 🔑 *Description of the spectrum of the ring of components*

Theorem 5.5.13. *Assume:*

— *Every nontrivial $H \in \mathrm{Sub}_{G,D}$ is either a non-splitter or a factored splitter.*

— *For every non-splitter $H \in \mathrm{Sub}_{G,D}$, there is at most one component of group H for each degree.*

Under these hypotheses, we describe $\gamma_\xi(H)$ for every $H \in \mathrm{Sub}_{G,D}$:

— *$\gamma_\xi(1)$ is the origin $(0, \ldots, 0)$.*

— *If H is a non-splitter, $\gamma_\xi(H)$ is the strict weighted span of e_H, i.e. the line from Theorem 5.5.1.*

— *Otherwise, H is a factored splitter, and we can write $H = H_1 \times \ldots \times H_k$ where the subgroups $H_1, \ldots, H_k$ form a free factor family of non-splitters. Then $\gamma_\xi(H)$ is the strict weighted span of $e_{H_1}, \ldots, e_{H_k}$.*

Proof. Consider a subgroup $H \in \mathrm{Sub}_{G,D}$. Choose a maximal free factor family $H_1, \ldots, H_k$ of H. For all $i \in \{1, \ldots, k\}$, the subgroup H_i is a non-splitter, since otherwise H_i is a factored splitter and we can construct a longer free factor family.

For each $i \in \{1, \ldots, k\}$, let $p'_{i,1}, \ldots, p'_{i,N(i)}$ be the non-factorizable components whose group is contained in H_i, and $p'_{0,1}, \ldots, p'_{0,N(0)}$ the non-factorizable components whose group is not contained in H. Since the family $H_1, \ldots, H_k$ is a factor family,

there are no other non-factorizable components, and since it is free these lists do not overlap.

We look at $\mathrm{Spec}(R)(k)$ as a subset of $\mathbb{A}^N(k)$ where we have ordered the coordinates as follows, the coordinate $x_{i,j}$ corresponding to the non-factorizable component $p_{i,j}$:

$$(x_{0,1}, \ldots, x_{0,N(0)}, x_{1,1}, \ldots, x_{1,N(1)}, \ldots, x_{k,1}, \ldots, x_{k,N(k)}).$$

Consider some $i \in \{1, \ldots, k\}$ and let d_i the greatest common divisor of the degrees of the non-factorizable components of R^{H_i}. Denote the degree of $p'_{i,j}$ by $q_i(j)d_i$. Then the ideal of R^{H_i} generated by components of group H_i corresponds to the closed set $Z_i = \mathrm{Spec}(R^{H_i})(k) \setminus \gamma_\xi(H_i)$. By the second part of Theorem 5.5.1, $\gamma_\xi(H_i)$ is exactly the set of points satisfying, for some $\lambda_i \in k \setminus \{0\}$:

$$x_{i,j} = \lambda_i^{q_i(j)} \text{ for all } j \in \{1, \ldots, N(i)\}.$$

Proposition 5.5.10 shows that $\gamma_\xi(H)$ is exactly the set of points satisfying all these equalities as well as $x'_{0,1} = \ldots = x'_{0,N(0)} = 0$, i.e. points of the form:

$$(\underbrace{0, \ldots, 0}_{N(0)}, \lambda_1^{q_1(1)}, \ldots, \lambda_1^{q_1(N(1))}, \lambda_2^{q_2(1)}, \ldots, \lambda_2^{q_2(N(2))}, \ldots, \lambda_k^{q_k(1)}, \ldots, \lambda_k^{q_k(N(k))})$$

with $\lambda_i \in k \setminus \{0\}$. This is the weighted span of $e_{H_1}, \ldots, e_{H_k}$. □

Corollary: *Krull dimension of R*

Corollary 5.5.14. *Assume that the first hypothesis of Theorem 5.5.13 is satisfied. Then, the Krull dimension of R is the maximal size of a free family of non-splitters.*

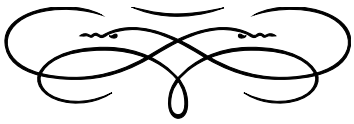
Proof. By Proposition 5.1.3, the Krull dimension of R is the maximal dimension of a subset $\gamma_\xi(H)$ with $H \in \mathrm{Sub}_{G,D}$. It follows from Proposition 5.5.10 that $\dim \gamma_\xi(H)$ is the sum of the dimensions of the sets $\gamma_\xi(H_i)$ where $H_1, \ldots, H_k$ is a free factor family of H consisting on non-splitters. By Theorem 5.1.4, the dimension of $\gamma_\xi(H_i)$ is equal to 1 when H_i is a non-splitter, and we obtain the result. □

Remark 5.5.15. Let $H \in \mathrm{Sub}_{G,D}$ be a non-splitter. The hypothesis that there is at most one component of group H for each degree implies, by Proposition 4.5.6, that the group $H_2(H, c_H)$ is trivial. Considering the conclusions of Subsection 5.4.5, this implies that the subset of $\overline{\gamma_\xi(H)}$ is a single point in projective space, i.e. the weighted span of a point in affine space. This is something we can also infer from Theorem 5.5.1.

However, the condition $H_2(H, c_H) = 1$ is not always satisfied. Consider the following example: a computation by Fried shows that for $G = \mathfrak{A}_5$ and c the conjugacy class of 3-cycles, there are exactly two components (in high enough degree) of group $\mathfrak{A}_5$ in $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{A}_5, c)$. In other words: $H_2(\mathfrak{A}_5, c) = \mathbb{Z}/2\mathbb{Z}$. In this case, the associated subset $\overline{\gamma(\mathfrak{A}_5)}$ is a union of two weighted lines: that from Theorem 5.5.1, and another one. This example illustrates that $\overline{\gamma_\xi(H)}$ is not irreducible in general. This is worth noting now, as similar phenomena will *not* happen in the context of Chapter 6.

Chapitre 6

A New Look at the Case of Symmetric Groups



Summary of the chapter

In this chapter, we examine the objects of Chapters 4 and 5 in the situation of $\mathfrak{S}_d$-covers of the projective line whose local monodromy elements are transpositions. The main results are a presentation by generators and relations of the monoid and ring of components (Theorem 6.1.1) and a description of the set of geometric points of the spectrum of the ring of components (Theorem 6.1.3).

The content of this chapter is largely taken from the preprint [Seg22].

Outline of the chapter

Quand je trouvais la ville trop noire,
Tu dorais des plages pour moi,
Tu mettais ton manteau de soie.
Et pour moi, qui ne voulais plus croire,
Et pour moi, pour pas que je me noie,
Tu faisais d'un chagrin une histoire,
Une joie.

— A. Sylvestre,
T'en souviens-tu, la Seine ?, 1964.

6.1. Introduction and main results

6.1.1. Introduction

Let $d > 2$ be an integer. In this chapter, we focus on the case where $X = \mathbb{P}^1(\mathbb{C})$, $G = \mathfrak{S}_d$, and c is the conjugacy class of transpositions in $\mathfrak{S}_d$. Our goal is to study the connected components of $\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c, n)$ for $n \in \mathbb{N}$.

This situation goes back to Hurwitz, Lüroth and Clebsch [Hur91]: they have showed that there is exactly one component of group $\mathfrak{S}_d$ for each even degree $\geq 2d-2$, i.e. $\mathrm{CHur}^*(\mathfrak{S}_d, c, n)$ is connected when nonempty.

We revisit this classical setting to observe what the objects studied in Chapters 4 and 5, notably the ring of components and its spectrum, look like in this well-known case.

6.1.2. Main results

We fix a field k of characteristic either zero or $> d$. Our first result is a presentation of the monoid and ring of components:

Theorem: 🔑 *Presentation of the monoid and ring of components of branched marked $\mathfrak{S}_d$-covers of $\mathbb{P}^1(\mathbb{C})$ whose local monodromy elements are transpositions*

Theorem 6.1.1. *The monoid of components* $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ *and the ring of components* $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ *admit the following presentations:*

$$\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) \simeq \left\langle (X_{ij})_{1\leq i<j\leq d} \;\middle|\; \begin{array}{ll} X_{ij}X_{kl} = X_{kl}X_{ij} & \text{for } i<j, k<l \\ X_{ij}X_{jk} = X_{ik}X_{jk} & \text{for } 1 \leq i < j < k \leq d \\ X_{ij}X_{jk} = X_{ij}X_{ik} & \text{for } 1 \leq i < j < k \leq d \end{array} \right\rangle,$$

$$R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) \simeq \frac{k[(X_{ij})_{1\leq i<j\leq d}]}{(X_{ij}X_{jk} - X_{ik}X_{jk},\, X_{ij}X_{jk} - X_{ij}X_{ik})_{1\leq i<j<k\leq d}},$$

where the generators X_{ij} have degree 2.

Let $\mathrm{HF}(n)$ be the total number of elements of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ of degree n, i.e. the count of connected components of $\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c, n)$. This is the Hilbert function of $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$. Our second result is a computation of this function:

Theorem: *The Hilbert function of the ring of components*

Theorem 6.1.2. *If n is odd, then $\mathrm{HF}(n) = 0$. We focus on the values of HF at even integers:*

(i) Let $d' = \lfloor d/2 \rfloor$. For $n \geq d-1$, the sequence $\mathrm{HF}(2n)$ coincides with a polynomial of leading monomial:

$$\begin{cases} \dfrac{d!}{2^{d'}(d')!(d'-1)!}\, n^{d'-1} & \text{if } d \text{ is even,} \\ \left(1+\dfrac{d'}{3}\right) \dfrac{d!}{2^{d'}(d')!(d'-1)!}\, n^{d'-1} & \text{if } d \text{ is odd.} \end{cases}$$

(ii) We have an exact formula for $\mathrm{HF}(2n)$:

$$\sum_{s=1}^{d-1} \sum_{w=1}^{d-s} \sum_{j=0}^{w} (-1)^{w-j} \binom{n-s+w-1}{w-1} \binom{d}{d-s-w,\, w-j,\, s+j} S(s+j,\, j)$$

where $S(d,s)$ denotes the Stirling numbers of the second kind[1].

[1] The Stirling number $S(d,s)$ is the number of partitions of a set of size s into d nonempty subsets.

Assume that k is algebraically closed. We describe $\mathrm{Spec}\,(R(\mathfrak{S}_d, c))\,(k)$ as a subset of $\mathbb{A}^{\frac{d(d-1)}{2}}(k)$. We use pairs (i,j) with $1 \leq i < j \leq d$ as indices for the coordinates, and we denote by $e_{i,j}$ the basis vector corresponding to the pair (i,j). If A is a subset of $\{1,\dots,d\}$, define the following vector:

$$e_A \overset{\text{def}}{=} \sum_{\substack{1 \leq i < j \leq d \\ i,j \in A}} e_{i,j}.$$

Note that $e_A = 0$ if $|A| \leq 2$.

Our final result is a full description of the k-points of the spectrum of the ring of components, embedded in affine space:

Theorem: *The spectrum of the ring of components of branched marked $\mathfrak{S}_d$-covers of $\mathbb{P}^1(\mathbb{C})$ whose local monodromy elements are transpositions*

Theorem 6.1.3. *The subset $\mathrm{Spec}\,(R(\mathfrak{S}_d, c))\,(k)$ of $\mathbb{A}^{\frac{d(d-1)}{2}}(k)$ is the union of the vector subspaces $\mathrm{Span}_k(e_{A_1}, \dots, e_{A_l})$ over all families $\{A_1, \dots, A_l\}$ of disjoint subsets of $\{1,\dots,d\}$.*

In particular, the dimension of $\mathrm{Spec}\left(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)\right)(k)$ is the maximal size of a family of disjoint subsets of $\{1,\dots,d\}$ of size ≥ 2, which is $\lfloor d/2 \rfloor$: this is consistent with the degree of the Hilbert polynomial computed in Theorem 6.1.2.

In the statement above, it is enough to consider the union over *maximal* families of disjoint subsets of $\{1,\dots,d\}$ of size at least 2. Theorem 6.1.3 is an application of Theorem 5.5.13.

6.1.3. Outline of the chapter

The chapter is organized as follows:

— In Section 6.2, we study the braid group action on lists of permutations. The first result is Theorem 6.2.6, which describes the braid group orbits of tuples of transpositions whose product is 1. We propose a visual proof of this result using multigraphs. We then use this description to obtain announced presentation of the monoid and ring of components (Theorem 6.1.1).

— In Section 6.3, we compute the Hilbert function of the ring of components $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ (Theorem 6.1.2).

— In Section 6.4, we describe the spectrum of the ring of components in the case of symmetric groups (Theorem 6.1.3). This is a direct application of Theorem 5.5.13.

6.2. The braid group action on lists of transpositions

We prove the main result of this section, Theorem 6.2.6, using *multigraphs*, i.e. non-oriented graphs where multiple edges can connect the same pair of distinct vertices. The relation between tuples of transpositions and multigraphs comes from this definition:

Definition: *The multigraph $\mathcal{G}(\underline{g})$ associated to a list of transpositions*

Definition 6.2.1. Let $\underline{g} = g_1, \dots, g_n$ be a list of transpositions in $\mathfrak{S}_d$. We define the multigraph $\mathcal{G}(\underline{g})$ whose vertices are the numbers $1, \dots, d$, with an edge between i and j for each appearance of the transposition (i, j) in $\underline{g}$.

Note that the multigraph $\mathcal{G}(\underline{g})$ determines the list $\underline{g}$ up to order.

6.2.1. 7-Γ-V-equivalent multigraphs

We prove a few graph-theoretic lemmas which will be used in the proof of Theorem 6.2.6.

Lemma 6.2.2. *If $\mathcal{G}$ is a connected multigraph with at least two vertices, there exists a vertex v in $\mathcal{G}$ such that the multigraph $\mathcal{G} \setminus v$ obtained by removing v is connected.*

Proof. Choose a spanning tree T of $\mathcal{G}$, i.e. a connected acyclic subgraph of $\mathcal{G}$ containing all vertices.[2] Removing any leaf from the tree T keeps it connected, and thus also keeps $\mathcal{G}$ connected. □

[2] Spanning trees always exist. To construct one, start from an arbitrary vertex v_0 and recursively add all edges connecting vertices already explored to vertices not yet explored. Eventually, all vertices have been explored, as one shows by induction on the minimal length of a path connecting a given vertex to v_0.

Lemma 6.2.3. *If $\mathcal{G}$ is a connected graph, all permutations of the vertices are products of transpositions $(a_i b_i)$ where a_i and b_i are vertices joined by an edge.*

Proof. We proceed by induction. For graphs of size 1, there are no nontrivial permutations. So we assume that $\mathcal{G}$ is a connected graph of size $d > 1$ and that the result holds for graphs that have strictly less vertices. Let $\sigma \in \mathfrak{S}_d$ be a permutation of the vertices. Using Lemma 6.2.2, choose an integer $v \in \{1, \dots, d\}$ such that the graph $\mathcal{G} \setminus v$ is connected. Now look at the integer $\sigma(v)$. By connectedness, we have a path in $\mathcal{G}$:

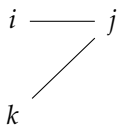
$$\sigma(v) = t_0 \to t_1 \to t_2 \to t_{w-1} \to t_w = v.$$

Let $P_1 = (t_w t_{w-1})(t_{w-1} t_{w-2}) \dots (t_2 t_1)(t_1 t_0)$ and $\sigma_2 = P_1 \sigma$. By construction, $\sigma_2(v) = v$, so we can see σ_2 as a permutation of the vertices of $\mathcal{G} \setminus v$. The graph $\mathcal{G} \setminus v$ is connected and strictly smaller than $\mathcal{G}$. By induction hypothesis, σ_2 is a product of transpositions (ij) for edges $i \to j$ of $\mathcal{G} \setminus v$. So $\sigma = P_1^{-1} \sigma_2$ is itself a product of transpositions (ij) where i and j are connected by an edge in $\mathcal{G}$. □

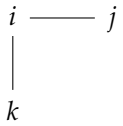
We now introduce an elementary transformation of a multigraph, the 7-Γ-*V-transformation*. We later show that this transformation is closely related to the action of elementary braids on tuples of transpositions.

Definition:
7-Γ-*V-transformation*
7-Γ-*V-equivalence*

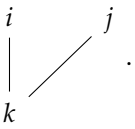
Definition 6.2.4. Two multigraphs $\mathcal{G}$ and $\mathcal{G}'$ (with same vertices) are *related by a* 7-Γ-*V-transformation* if there are vertices i, j, k such that $\mathcal{G}$ contains the following "7"-shaped triangle:



and $\mathcal{G}'$ is identical to $\mathcal{G}$ except that this triangle is replaced by the "Γ"-shaped triangle:



or by the "V"-shaped triangle:



Two multigraphs $\mathcal{G}$ and $\mathcal{G}'$ are 7-Γ-*V-equivalent* if they can be obtained from each other by a sequence of 7-Γ-V-transformations.

A 7-Γ-V-transformation is the action of letting an edge slide along another one. We characterize the equivalence classes for 7-Γ-V-equivalence:

Lemma:
Characterization of 7-Γ-*V-equivalent multigraphs*

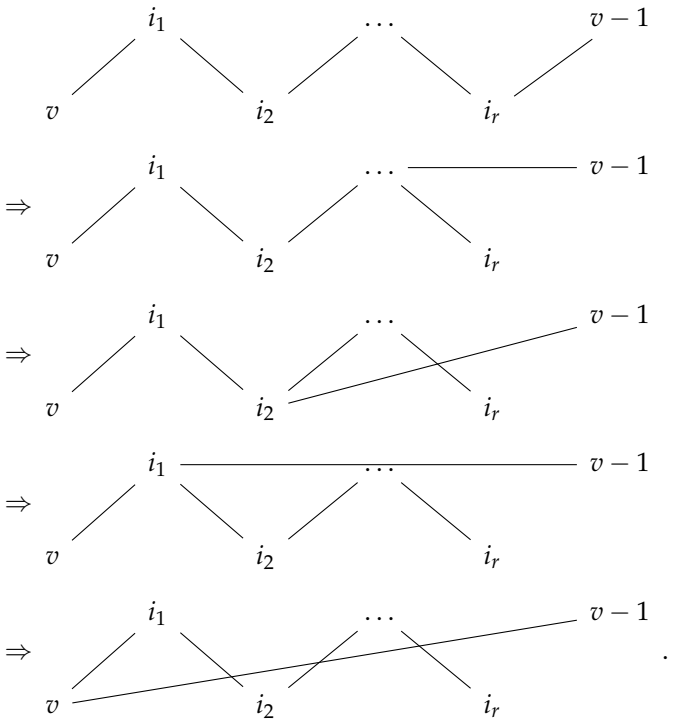
Lemma 6.2.5. *Two multigraphs $\mathcal{G}$ and $\mathcal{G}'$ with the same vertices are* 7-Γ-*V-equivalent if and only if they have the same connected components, and the same number of edges in each connected component.*

Proof. A 7-Γ-V transformation does not change the connected components or the number of edges of individual connected components.

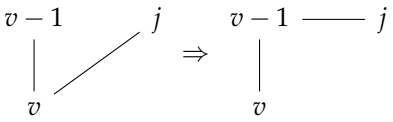
Conversely, we show that the connected components and their edge counts determine the multigraph up to 7-Γ-V-equivalence. We proceed independently for each connected component, so we assume that $\mathcal{G}$ is a connected multigraph with vertices $\{1, \dots, v\}$ and whose number of edges is e. We are going to show that $\mathcal{G}$ is 7-Γ-V-equivalent to a multigraph depending only on the numbers e and v, which proves the result.

Since the multigraph is connected, there is a path $(v, i_1, i_2, \dots, i_r, v-1)$ between v and $v-1$. We connect v and $v-1$ directly by an edge using the following transfor-

mations:

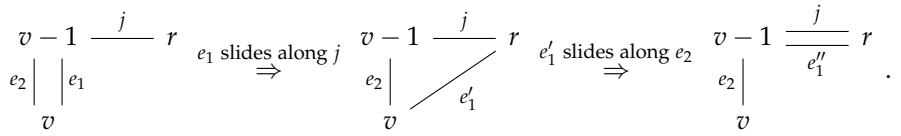


If there is a vertex $j \neq v-1$ that is connected to v, the transformation:

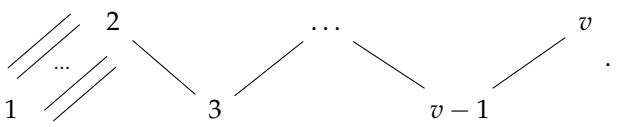


allows one to reduce the number of edges that connect v to a vertex other than $v-1$ until there is none.

Since the graph is connected, if $v \geq 3$, the vertex $v-1$ is connected to some vertex $1 \leq r \leq v-2$. If two different edges connect v and $v-1$, we apply the two successive transformations:



Repeating this operation allows one to assume v and $v-1$ are connected by exactly one edge. We can repeat this process for $v-1, v-2, \ldots$ and 3. In the end, our graph has one edge between k and $k-1$ for all $3 \leq k \leq v$ and since the number of edges is constant there are exactly $e-v+2$ edges between 1 and 2. So $\mathcal{G}$ is 7-Γ-V-equivalent to the following multigraph, uniquely determined by e and v:



This concludes the proof. □

6.2.2. **Braid orbits of tuples of transpositions**

We prove Theorem 6.2.6, which describes the braid group orbits of tuples of transpositions. This information is later used to describe the monoid and ring of components in Subsection 6.2.3 and the geometry of its spectrum in Section 6.4. To state Theorem 6.2.6, we introduce some notation and terminology:

— If $\underline{g}$ is a list of transpositions in $\mathfrak{S}_d$, the set $I(\underline{g})$ is the partition of the set $\{1,\dots,d\}$ corresponding to the connected components of the multigraph $\mathcal{G}(\underline{g})$ (Definition 6.2.1).

— If $\Sigma \in I(\underline{g})$ is a subset of $\{1,\dots,d\}$ corresponding to a connected component of $\mathcal{G}(\underline{g})$, the *subtuple of $\underline{g}$ associated to Σ* is the tuple formed by keeping only the transpositions (i,j) such that $i,j \in \Sigma$, in the order of their appearances in $\underline{g}$.

We now state the theorem and prove it:

Theorem: *Characterization of braid orbits of tuples of transpositions of product* 1

Theorem 6.2.6. *If $(g_1,\dots,g_n)$ is a list of transpositions of $\mathfrak{S}_d$ such that $g_1g_2\dots g_n = 1$, then:*

(i) n is even. Let $n = 2n'$.

(ii) $(g_1,\dots,g_n)$ is equivalent under the braid group action to an n-tuple of the form:

$$(h_1,h_1,h_2,h_2,\dots,h_{n'},h_{n'})$$

where the elements h_i are transpositions.

(iii) The subgroup of $\mathfrak{S}_d$ generated by $g_1,\dots g_n$ is a product of symmetric groups, namely $\prod_{\Sigma\in I(\underline{g})}\mathfrak{S}_\Sigma$, where $I(\underline{g})$ is the partition of $\{1,2,\dots,d\}$ associated to the list $\underline{g}$.

(iv) The braid group orbit of a tuple $(h_1,h_1,h_2,h_2,\dots,h_{n'},h_{n'})$ is determined by the 7-Γ-V-equivalence class of the multigraph $\mathcal{G}(h_1,\dots,h_{n'})$ (cf. Definitions 6.2.1 and 6.2.4).

(v) The braid group orbit of an n-tuple $\underline{g}$ is determined by the associated partition $I(\underline{g})$, and by the size of the subtuples associated to each subset $\Sigma \in I(\underline{g})$ in that partition.

Proof. (i) Looking at the signatures of both sides of the equality $g_1\dots g_n = 1$, we obtain the equality $(-1)^n = 1$, thus n is even.

(ii) Let us prove that $(g_1,\dots,g_n)$ is equivalent to a tuple of the form $(h_1,h_1,g_3',\dots,g_n')$. The result follows by induction. Without loss of generality, assume that $g_1 = (12)$. Then also $g_2\dots g_n = (12)$.

Let N_1 be the largest value of i such that g_i does not fix 1. We let $g_{N_1} = (1a_1)$. Then let N_2 be the largest value of $i < N_1$ such that g_i does not fix a_1, and $g_{N_2} = (a_1a_2)$, etc. At some point, we have $a_s = 2$ since 1 is mapped onto 2 by $g_2g_3\dots g_r$. So:

$$g_{N_s}g_{N_{s-1}}\dots g_{N_1} = (2a_{s-1})(a_{s-2}a_{s-3})\dots(a_2a_1)(a_11)$$

We can assume that the numbers a_i are distinct: if we have $a_i = a_j$ with $j > i$, we remove $g_{N_{i+1}},g_{N_{i+2}},\dots,g_{N_j}$ from the list. Use braids to move g_{N_s} to the second place, then move $g_{N_{s-1}}$ to the third place, and so on. The tuple $\underline{g}$ is equivalent to a tuple of the form:

$$((12),g_{N_s},g_{N_{s-1}},\dots,g_{N_1},g'_{s+2},g'_{s+3},\dots,g'_n)$$

Now move $g_{N_1} = (1a_1)$ to the second place. This conjugates all the transpositions $g_{N_i}, i > 1$ by g_{N_1}, so that $\underline{g}$ is equivalent to:

$$\begin{aligned}&((12), g_{N_1}, g_{N_s}^{g_{N_1}}, \ldots, g_{N_3}^{g_{N_1}}, g_{N_2}^{g_{N_1}}, g'_{s+2}, \ldots, g'_n)\\ =&((12), (1a_1), g_{N_s}, \ldots, g_{N_3}, (1a_2), g'_{s+2}, \ldots, g'_n)\end{aligned}$$

Move the newly obtained $(1a_2)$ to the third place, etc.:

$$\begin{aligned}\underline{g} \sim&((12), (1a_1), g_{N_s}, \ldots, g_{N_3}, (1a_2), g'_{s+2}, \ldots, g'_n)\\ \sim&((12), (1a_1), (1a_2), g_{N_s}, \ldots, g_{N_4}, (1a_3), g'_{s+2}, \ldots, g'_n)\\ \sim&\ldots\\ \sim&((12), (1a_1), (1a_2), (1a_3) \ldots, (a_{s-1}2), (1a_{s-1}), g'_{s+2}, \ldots, g'_n)\\ \sim&((12), (1a_1), (1a_2), (1a_3) \ldots, (1a_{s-1}), (12), g'_{s+2}, \ldots, g'_n)\\ \sim&((12), (12), (2a_1), (2a_2), (2a_3) \ldots, (2a_{s-1}), g'_{s+2}, \ldots, g'_n)\end{aligned}$$

This concludes the proof of this part.

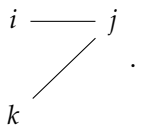
(iii) If a product of transpositions all taken from the list $\underline{g}$ maps an integer a to an integer b, this defines a path:

$$a = t_0 \to t_1 \to t_2 \to \ldots \to t_{w-1} \to t_w = b$$

such that all the transpositions (t_i, t_{i+1}) are in the list $\underline{g}$. Hence, the subgroup generated by $\underline{g}$ is contained in $\prod_{\Sigma \in I(\underline{g})} \mathfrak{S}_\Sigma$. To show that any permutation in $\prod_{\Sigma \in I(\underline{g})} \mathfrak{S}_\Sigma$ is a product of transpositions g_i, we can consider connected components of the multigraph independently; the result then follows from Lemma 6.2.3.

(iv) The multigraph $\mathcal{G}(h_1, \ldots, h_{n'})$ determines $h_1, \ldots, h_{n'}$ up to order, and since (h_i, h_i) commutes with (h_j, h_j) modulo the braid group action, the order does not matter for the braid group orbit of $\underline{h}$.

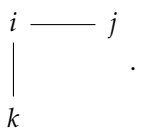
Now, in the multigraph, the tuple $((ij), (ij), (jk), (jk))$ corresponds to the following "7"-shaped triangle:



Applying these braid transformations:

$$((ij), (ij), (jk), (jk)) \sim ((ij), (ik), (ik), (ij)) \sim ((ij), (ij), (ik), (ik))$$

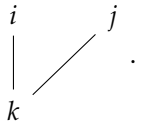
turns the triangle above into the "Γ"-shaped triangle:



And applying these other braid transformations:

$$((ij), (ij), (jk), (jk)) \sim ((jk), (ik), (ik), (jk)) \sim ((jk), (jk), (ik), (ik))$$

turns it into the "V"-shaped triangle:



This shows that 7-Γ-V-transformations do not change the braid group orbit of the tuple $\prod(h_i, h_i)$. This concludes the proof of this point.

(v) Two equivalent tuples define the same partition: this follows from point (iii) since their groups are the same subgroup H of $\mathfrak{S}_d$. That the subtuples formed using this partition are of the same size for both tuples follows from the fact that the (H, H)-multidiscriminant is invariant.

Conversely, if two tuples $(h_1, h_1, \dots, h_{n'}, h_{n'})$ and $(h'_1, h'_1, \dots, h'_{n'}, h'_{n'})$ define the same partition I and the subtuples associated to all subsets $\Sigma \in I$ are of the same size for both tuples, then the multigraphs $\mathcal{G}(h_1, \dots, h_{n'})$ and $\mathcal{G}(h'_1, \dots, h'_{n'})$ have the same connected components and the same numbers of edges in each connected component. By Lemma 6.2.5, these multigraphs are 7-Γ-V-equivalent, which implies that the tuples are equivalent by point (iv).

This concludes the proof. Note that we have shown that any equivalence between tuples can be deduced from the equivalences corresponding to 7-Γ-V-transformations.

□

6.2.3. **A presentation of the monoid and ring of components**

We recall and prove Theorem 6.1.1:

Theorem 6.1.1 (recalled). *The monoid of components* $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ *and the ring of components* $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ *admit the following presentations by generators and relations (as monoid and commutative k-algebra, respectively):* **Theorem 6.1.1 (recalled)**

$$\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) \simeq \left\langle (X_{ij})_{1\le i<j\le d} \;\middle|\; \begin{array}{ll} X_{ij}X_{kl} = X_{kl}X_{ij} & \text{for } i<j, k<l \\ X_{ij}X_{jk} = X_{ik}X_{jk} & \text{for } 1\le i<j<k\le d \\ X_{ij}X_{jk} = X_{ij}X_{ik} & \text{for } 1\le i<j<k\le d \end{array} \right\rangle,$$

$$R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c) \simeq \frac{k[(X_{ij})_{1\le i<j\le d}]}{(X_{ij}X_{jk} - X_{ik}X_{jk},\ X_{ij}X_{jk} - X_{ij}X_{ik})_{1\le i<j<k\le d}},$$

where the generators X_{ij} *have degree* 2.

Proof.

— By Theorem 6.2.6 (ii), the monoid of components is generated by braid orbits of transpositions repeated twice. We denote by X_{ij} the generator associated to the 2-tuple $((ij), (ij))$. There are $d(d-1)/2$ such generators, all of degree 2.

— A generating set of relations is given by equalities of the form $X_{ij}X_{jk} = X_{ik}X_{jk} = X_{ij}X_{ik}$ for $i < j < k$. These equalities correspond to 7-Γ-V-transformations of the associated multigraph, as observed in the proof of Theorem 6.2.6 (iv). The fact that they generate all relations follows from Theorem 6.2.6 (v) and Lemma 6.2.5.

— The description of the ring of components follows readily from that of the monoid of components.

□

Remark 6.2.7. The presentation of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ given in Theorem 6.1.1 is very close to the presentation of $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ deduced from Remark 3.4.2. In fact, up to a doubling of degrees, the monoid $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ is the abelianization of the monoid $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(\mathfrak{S}_d, c)$: the relations are precisely the braid relations, plus commutativity. One can ask how specific this phenomenon is to this situation.

In what follows, we systematically ignore degrees: we work in the category of (non-graded) monoids. Consider the case of a group G and a single conjugacy class c of G, whose elements have order $\mathrm{ord}(c)$. One can consider the map Φ that takes a tuple $\underline{g} \in G^n$ to the tuple:

$$\Phi(\underline{g}) = (\underbrace{g_1, \dots, g_1}_{\mathrm{ord}(c)}, \dots, \underbrace{g_n, \dots, g_n}_{\mathrm{ord}(c)}).$$

The first thing to notice is that Φ induces a well-defined map on braid orbits of tuples, compatible with multiplication. Therefore it is a morphism of (non-graded) monoids $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, c) \to \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$ which multiplies degrees by $\mathrm{ord}(c)$. Since $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$ is a commutative monoid, this morphism factors through the abelianization $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, c)^{\mathrm{ab}}$ of $\mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, c)$, which is generated by elements of c with the braid relations and commutativity as only relations. We obtain a morphism of commutative monoids $\widetilde{\Phi} : \mathrm{Comp}_{\mathbb{A}^1(\mathbb{C})}(G, c)^{\mathrm{ab}} \to \mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$.

In the case where G is a symmetric group and c is the class of transpositions, the morphism $\widetilde{\Phi}$ is an isomorphism, as we have illustrated earlier. Such a thing can not be expected in general, cf. Remark 3.4.20. Nevertheless, consider a tuple $\underline{g} \in G^n$ of size $n \geq |c| \,\mathrm{ord}(c)$. Then at least one element $g \in c$ appears $\mathrm{ord}(c)$ times in that tuple. This implies that $\underline{g}$ factorizes (modulo braids) as:

$$\underline{g} \sim (\underbrace{g, \dots, g}_{\mathrm{ord}(c)})\underline{g}'.$$

One can keep factorizing until the remaining tuple $\underline{g}'$ is of size less than $|c| \,\mathrm{ord}(c)$. Hence, the image of $\widetilde{\Phi}$ is large in the sense that there exists a finite list F of components such that every element of $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G, c)$ is the product of an element of $\mathrm{Im}(\widetilde{\Phi})$ and an element of F. In terms of rings of components, this means that $R_{\mathbb{P}^1(\mathbb{C})}(G, c)$ is a finitely generated $R_{\mathbb{A}^1(\mathbb{C})}(G, c)$-module (for the action $m.y = \Phi(m)y$). In particular, it is no surprise that the counts of components are similar for $\mathbb{A}^1(\mathbb{C})$ and $\mathbb{P}^1(\mathbb{C})$ up to a constant.

6.3. Counting components: the Hilbert function

Our goal is to count the number of components with $2n$ branch points, i.e.:

$$HF(2n) = \left|\pi_0 \mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c, 2n)\right|.$$

By Theorem 6.2.6, a component of degree $2n$ is uniquely defined by:

— A partition of $\{1,\dots,d\}$ into s non-empty sets $(C_1,\dots,C_s)$, such that at least one of these is not a singleton (if $n \geq 1$). These sets correspond to the connected components of the multigraph.

— An unordered list of numbers $(n_i)_{i\in\{1,\dots,s\}}$ such that $\sum_i n_i = n$, corresponding to the sizes of the sublists associated with each connected component of the multigraph. These integers must satisfy $n_i \geq |C_i| - 1$ for all $i \in \{1,\dots,s\}$, and $n_i = 0$ when $|C_i| = 1$.

The constraint $n_i \geq |C_i| - 1$ expresses the fact that n_i transpositions cannot generate a subgroup larger than $\mathfrak{S}_{n_i+1}$ (alternatively, a connected graph with v vertices has at least $v-1$ edges). Since there must be at least one transposition for $n \geq 1$, there is also at least one subset of size ≥ 2.

Choose a partition of $\{1,\dots,d\}$ into s non-empty sets $(C_1,\dots,C_s)$ which are not all singletons. Put all singletons at the end of the list, i.e. the singletons are the $(C_{w+1},\dots,C_s)$. There are $s-w$ singletons, and $w \geq 1$ subsets of size ≥ 2. The number of components of degree $2n$ associated with this partition is equal to the number of ways to write n as a sum $r_1 + \ldots + r_w$ with $r_i \geq |C_i| - 1$. This is also the number of ways to write $n - \sum_i(|C_i|-1) = n - d + s$ as a sum of w nonnegative integers, i.e.:

$$\binom{n-d+s+w-1}{w-1}.$$

Consequently, the total number of components of degree $2n$ is:

$$HF(2n) = \sum_{s=1}^{d-1}\sum_{w=1}^{s} \sum_{\substack{(C_1,\dots,C_s) \text{ partition of } \{1,\dots,d\} \text{ with} \\ s-w \text{ singletons and no empty subset.}}} \binom{n-d+s+w-1}{w-1}.$$

All that is left to do is to count the partitions of $\{1,\dots,d\}$ into s nonempty subsets with $s-w$ singletons ($w \geq 1$). In the next two subsections, we approach this question in two different ways.

6.3.1. The leading monomial of the Hilbert polynomial

In this subsection, we prove Theorem 6.1.2 (i):

Theorem 6.1.2 (i) (recalled). *Let $d' = \lfloor d/2 \rfloor$. For $n \geq d-1$, the sequence* $\mathrm{HF}(2n)$ *coincides with a polynomial of leading monomial:*

$$\begin{cases} \dfrac{d!}{2^{d'}(d')!(d'-1)!}\, n^{d'-1} & \text{if } d \text{ is even,} \\ \left(1+\dfrac{d'}{3}\right)\dfrac{d!}{2^{d'}(d')!(d'-1)!}\, n^{d'-1} & \text{if } d \text{ is odd.} \end{cases}$$

Theorem 6.1.2 (i) (recalled)

Proof. Recall that:

$$HF(2n) = \sum_{s=1}^{d-1}\sum_{w=1}^{s} \sum_{\substack{(C_1,\dots,C_s) \text{ partition of } \{1,\dots,d\} \text{ with} \\ s-w \text{ singletons and no empty subset.}}} \binom{n-d+s+w-1}{w-1}.$$

As soon as $n-d+s+w-1 \geq w-1$, i.e. when $n \geq d-s$, the binomial coefficient $\binom{n-d+s+w-1}{w-1}$ coincides with a polynomial in n of degree $w-1$ and of leading coefficient $\frac{1}{(w-1)!}$. So $HF(2n)$ coincides with a polynomial in n as soon as $n \geq d-1$, of leading monomial:

$$\frac{N(W)}{(W-1)!} \times n^{W-1} \tag{6.3.1}$$

where W is the maximum value reached by w and $N(W)$ is the number of partitions that reach that number. The partitions of $\{1,\dots,d\}$ with the highest numbers of non-singletons (i.e. w is maximal) are those that are mostly made of pairs. Specifically:

— When d is even, the highest possible number W of non-singleton subsets in a partition of $\{1,\dots,d\}$ is $d' = \frac{d}{2}$. This number is reached for any partition of $\{1,\dots,d\}$ made entirely of pairs (any other partition either has singletons or loses the opportunity to form a pair by grouping three elements together, and thus has less subsets). The number of **ordered** partitions of $\{1,\dots,d\}$ into d' pairs is:

$$\binom{d}{2,\dots,2} = \frac{d!}{2^{d'}}$$

Finally:

$$N(W) = N(d') = \frac{1}{d'!}\frac{d!}{2^{d'}} = \frac{d!}{2^{d'}d'!}.$$

— When d is odd ($d = 2d'+1$), the highest possible number W of non-singleton subsets in a partition of $\{1,\dots,d\}$ is also $W = d'$. It is reached for any partition in d' pairs with a singleton left out, and for any partition consisting of $d'-1$ pairs and a subset of size 3 (any other partition either has more singletons or has less subsets). The number of partitions of $\{1,\dots,d\}$ in d' pairs and one singleton is:

$$\underbrace{d}_{\text{one singleton}} \times \underbrace{\left(\frac{1}{d'!}\binom{d-1}{2,\dots,2}\right)}_{d' \text{ pairs}} = \frac{d(d-1)!}{2^{d'}d'!} = \frac{d!}{2^{d'}d'!}$$

and the number of partitions of $\{1,\dots,d\}$ in $d'-1$ pairs and one subset of size 3 is:

$$\underbrace{\binom{d}{3}}_{\text{one subset of size 3}} \times \underbrace{\left(\frac{1}{(d'-1)!}\binom{(d-3)!}{2,\dots,2}\right)}_{d'-1 \text{ pairs}} = \frac{d(d-1)(d-2)}{6}\frac{(d-3)!}{2^{d'-1}(d'-1)!}$$

$$= \frac{d!}{3 \times 2^{d'}(d'-1)!}.$$

We finally compute $N(W)$:

$$N(W) = N(d') = \frac{d!}{2^{d'}d'!} + \frac{d!}{3 \times 2^{d'}(d'-1)!} = \left(1+\frac{d'}{3}\right)\frac{d!}{2^{d'}d'!}.$$

The announced formulas for the leading monomial follow immediately using Equation (6.3.1) □

6.3.2. **An exact formula for the Hilbert polynomial**

Let $S^*(d,s,i)$ be the number of partitions of $\{1,\dots,d\}$ into s nonempty sets with exactly i singletons (where $i \leq s \leq d$). We have the equality:

$$HF(2n) = \sum_{s=1}^{d-1} \sum_{w=1}^{s} S^*(d,\, s,\, s-w) \binom{n-d+s+w-1}{w-1} \tag{6.3.2}$$

Moreover, we have the formula:

$$S^*(d,s,i) = \binom{d}{i} S^*(d-i, s-i, 0) \tag{6.3.3}$$

Indeed, there are $\binom{d}{i}$ ways to choose which elements go into the i singletons, and then we partition the $d-i$ remaining elements without any singletons.

Denote by $S(d,s)$ the Stirling numbers of the second kind (how many ways are there to put d things into s nonempty boxes?). A partition of $\{1,\dots,d\}$ into s nonempty sets must have some number i of singletons, hence:

$$S(d,s) = \sum_{i=0}^{s} S^*(d,s,i). \tag{6.3.4}$$

Combined with Equations (6.3.3) and (6.3.4), this implies:

$$S(d,s) = \sum_{i=0}^{s} \binom{d}{i} S^*(d-i, s-i, 0).$$

Let us now compute, for $s \leq d$:

$$\begin{aligned}
\sum_{j=0}^{s} (-1)^j \binom{d}{j} S(d-j, s-j) &= \sum_{j=0}^{s} \sum_{i=0}^{s-j} (-1)^j \binom{d}{j} \binom{d-j}{i} S^*(d-j-i, s-j-i, 0) \\
&= \sum_{j=0}^{s} \sum_{i=j}^{s} (-1)^j \binom{d}{j} \binom{d-j}{i-j} S^*(d-i, s-i, 0) \\
&= \sum_{i=0}^{s} \sum_{j=0}^{i} (-1)^j \binom{d}{j} \binom{d-j}{i-j} S^*(d-i, s-i, 0) \\
&= \sum_{i=0}^{s} \left(S^*(d-i, s-i, 0) \sum_{j=0}^{i} (-1)^j \frac{d!}{j!(i-j)!(d-i)!} \right) \\
&= \sum_{i=0}^{s} \left(S^*(d-i, s-i, 0) \binom{d}{i} \sum_{j=0}^{i} (-1)^j \binom{i}{j} \right) \\
&= \sum_{i=0}^{s} \binom{d}{i} S^*(d-i, s-i, 0) 0^i \\
&= S^*(d,s,0)
\end{aligned}$$

This lets us express the values of S^* in terms of Stirling numbers[3]:

$$S^*(d,s,i) = \sum_{j=0}^{s-i} (-1)^j \binom{d}{i, j, d-i-j} S(d-i-j, s-i-j).$$

[3] We could have used the inversion formula for binomial transforms.

Using Equation (6.3.2), we finally compute the total number of components:

$$\begin{aligned}
HF(2n) &= \sum_{s=1}^{d-1}\sum_{w=1}^{s}\binom{n-d+s+w-1}{w-1}S^*(d,s,s-w)\\
&= \sum_{s=1}^{d-1}\sum_{w=1}^{s}\sum_{j=0}^{w}(-1)^j\binom{n-d+s+w-1}{w-1}\binom{d}{s-w,\,j,\,d-s+w-j}S(d-s+w-j,w-j)\\
&= \sum_{s=1}^{d-1}\sum_{w=1}^{d-s}\sum_{j=0}^{w}(-1)^j\binom{n-s+w-1}{w-1}\binom{d}{d-s-w,\,j,\,s+w-j}S(s+w-j,w-j)\\
&= \sum_{s=1}^{d-1}\sum_{w=1}^{d-s}\sum_{j=0}^{w}(-1)^{w-j}\binom{n-s+w-1}{w-1}\binom{d}{d-s-w,\,w-j,\,s+j}S(s+j,j).
\end{aligned}$$

This is the second half of Theorem 6.1.2. A formula without Stirling numbers can be obtained using the equality:

$$S(n,k)=\frac{1}{k!}\sum_{j=0}^{k}(-1)^j\binom{k}{j}(k-j)^n.$$

These formulas are of little use. For instance, computing the leading monomial using them is tedious.

6.4. The spectrum of the ring of components

In this section, we assume that k is an algebraically closed field of characteristic either 0 or $> d$, and we prove Theorem 6.1.3, which describes the set of k-points of the spectrum of $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d,c)$ as a subset of $\mathbb{A}^{\frac{d(d-1)}{2}}(k)$. The proof relies on Theorem 5.5.13.

Coordinates of points of $k^{\frac{d(d-1)}{2}}$ are indexed by pairs $(i,j), 1\leq i<j\leq d$, and we denote the basis vector corresponding to the pair (i,j) by $e_{i,j}$. If A is a subset of $\{1,\dots,d\}$, we let:

$$e_A \overset{\text{def}}{=} \sum_{\substack{1\leq i<j\leq d\\ i,j\in A}} e_{i,j}.$$

We recall and prove Theorem 6.1.3:

Theorem 6.1.3 (recalled). *The subset* $\operatorname{Spec}\left(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d,c)\right)(k)$ *of* $\mathbb{A}^{\frac{d(d-1)}{2}}(k)$ *is the union of the vector subspaces* $\operatorname{Span}_k(e_{A_1},\dots,e_{A_l})$ *over all families* $\{A_1,\dots,A_l\}$ *of disjoint subsets of* $\{1,\dots,d\}$.

Theorem 6.1.3 (recalled)

Proof. Theorem 5.5.13 applies. Indeed:

— The subgroups $\mathfrak{S}_A$ corresponding to subsets $A\subseteq\{1,\dots,d\}$ of size at least 2 are non-splitters, since transpositions form a single conjugacy class in a symmetric group.

— All subgroups generated by transpositions are products of non-splitters, namely symmetric groups corresponding to disjoint subsets of size at least 2 (Theorem 6.2.6 (iii)). The factors form a free factor family by Proposition 5.5.9: indeed, a transposition in a product of symmetric groups lies in one of the symmetric groups.

— For a given degree n and subset $A \subseteq \{1, \dots, d\}$, there is at most one component of group $\mathfrak{S}_A$ of degree n. Indeed, the multigraph corresponding to a tuple representing such a component must have n edges, all contained in a single connected component (corresponding to A), and multigraphs of this kind are all 7-Γ-V-equivalent by Lemma 6.2.5. We conclude by Theorem 6.2.6 (v).

Moreover, all non-factorizable components have degree 2 by Theorem 6.2.6 (ii); thus, "weighted spans" are actual vector spans in this situation. We deduce from Theorem 5.5.13 that $\gamma_\xi(\mathfrak{S}_{A_1} \times \ldots \times \mathfrak{S}_{A_k})$ is the vector span of $\{e_{A_1}, \dots, e_{A_k}\}$, minus the vector span of any $k-1$ of these vectors. If A is a singleton or the empty set, then e_A is the null vector, so there is no need to exclude subsets of size ≤ 2 in the union. By Proposition 5.1.3, we have:

$$\begin{aligned}
&\operatorname{Spec}\left(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)\right)(k) \\
&= \bigsqcup_{H \in \operatorname{Sub}_{\mathfrak{S}_d, c}} \gamma_\xi(H) \\
&= \bigsqcup_{\substack{A_1, \dots, A_k \subseteq \{1, \dots, d\} \\ \text{disjoint}}} \left(\operatorname{Span}(e_{A_1}, \dots, e_{A_k}) \setminus \bigsqcup_{i=1}^{k} \operatorname{Span}(e_{A_1}, \dots, \widehat{e_{A_i}}, \dots, e_{A_k}) \right).
\end{aligned}$$

Since we are adding $\operatorname{Span}(e_{A_1}, \dots, \widehat{e_{A_i}}, \dots, e_{A_k})$ back anyway, we may as well never subtract it:

$$\operatorname{Spec}\left(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)\right)(k) = \bigcup_{\substack{A_1, \dots, A_k \subseteq \{1, \dots, d\} \\ \text{disjoint}}} \operatorname{Span}(e_{A_1}, \dots, e_{A_k}).$$

□

6.4.1. **Examples**

In this subsection, we obtain graphical representations of the spectrums of the rings of components for small values of d. All generators of $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ have the same degree 2: the issues mentioned in Remark 3.4.20 do not arise. Therefore, we draw the k-points of $\operatorname{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c))$. We have described an embedding of in the projective space of dimension $\frac{d(d+1)}{2} - 1$. Since drawing in large dimensions is uneasy, our depictions are very schematic.

— **Drawing of** $\operatorname{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_3, c))$**:** $\operatorname{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_3, c))$ has exactly four k-points. It is of dimension 0, so we are in the "non-splitting" case of [EVW16].

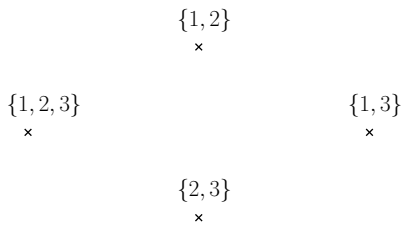


Figure 6.4.1.
$\mathrm{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_3, c))(k)$. Over each point we have indicated the corresponding subset of $\{1, 2, 3\}$.

— **Drawing of** $\mathrm{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_4, c))$**:** The set $\mathrm{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_4, c))(k)$ consists of five points (corresponding to the subsets of $\{1, 2, 3, 4\}$ of size ≥ 3) and two lines, (for the pairs of disjoint subsets of size 2). It is of dimension 1.

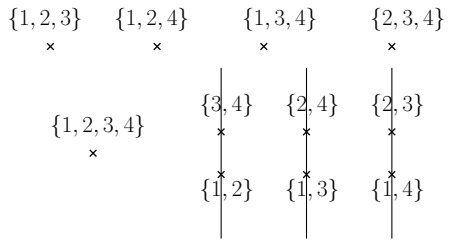


Figure 6.4.2.
$\mathrm{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_4, c))(k)$.

— **Partial drawing of** $\mathrm{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_6, c))$**:** The minimal example for which $R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_d, c)$ is of dimension 2 is obtained when $d = 6$. In this case, the irreducible components are 15 planes (one for each triple of disjoint pairs of elements of $\{1, 2, 3, 4, 5, 6\}$), 10 lines (for the pairs of disjoint subsets of size 3) and 22 points (for the subsets of size ≥ 4). These irreducible components intersect: for example the planes corresponding to the triples $(\{1, 2\}, \{3, 4\}, \{5, 6\})$ and $(\{1, 2\}, \{3, 5\}, \{4, 6\})$ intersect at the point associated to $\{1, 2\}$.

Since there is much to draw, we focus on the part corresponding to subsets of size 2, i.e. the 15 planes. We represent the planes as triangles, the lines corresponding to two disjoint subsets of size 2 as edges, and the subsets of size 2 as vertices. We use a tool by Iacopo Iacopini[4] designed to draw simplicial sets by simulating mechanical springs, using the Python library `networkx`. This yields the following drawing:

[4] Available at `https://github.com/iaciac/py-draw-simplicial-complex/blob/master/Draw2dsimplicialcomplex.ipynb`.

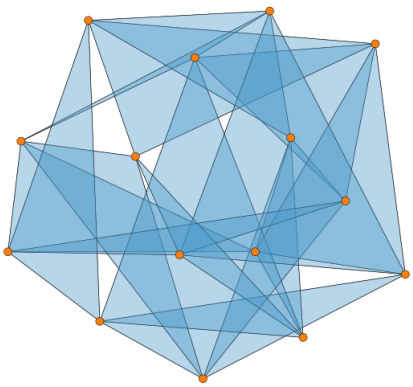


Figure 6.4.3.
A schematic drawing of a part of $\mathrm{Proj}(R_{\mathbb{P}^1(\mathbb{C})}(\mathfrak{S}_6, c))$

Chapitre 7

Théorie algébrique des G-revêtements et des espaces de Hurwitz

(A summary of this chapter in English may be found in Section 7.3)

Résumé du chapitre

Dans ce chapitre, nous énonçons des définitions et faits connus concernant les revêtements algébriques et leurs espaces de modules, les schémas de Hurwitz. On met l'accent sur les liens avec les constructions topologiques des chapitres 2 et 3 et avec le problème de Galois inverse. Ici aussi, un G-revêtement n'est pas nécessairement connexe.

Les définitions, notations et énoncés de ce chapitre sont utilisés dans le chapitre 8.

Organisation du chapitre

> Il y eut un son lointain d'une grande pureté, aigu et perçant, comme un cœur de souris qui se brise.
> « C'était quoi ? », demanda-t-il.
> Trymon pencha la tête.
> « Do dièse, je pense. »
>
> — T. Pratchett (trad. P. Couton), *Le Huitième Sortilège*, 1983.

Dans ce chapitre, nous revisitons les revêtements dans le cadre de la géométrie algébrique. Ce point de vue est largement employé dans le chapitre 8. De nombreux objets introduits dans les chapitres 2 et 3 ont un pendant algébrique : cela concerne notamment les espaces de configuration (Définition 7.1.2), les G-revêtements (Définition 7.1.4) et les espaces de Hurwitz (Section 7.2). Nous revisitons ces objets dans ce cadre, en explicitant les liens qui les unissent à leurs équivalents topologiques. Ce chapitre utilise la terminologie présentée dans la sous-section 1.4.4.

Dans ce qui suit, on considère uniquement les revêtements ramifiés de la droite projective $\mathbb{P}^1$, marquée au point à l'infini ∞, et on suppose toujours ces revêtements non-ramifiés au dessus du point à l'infini. Quand on emploie des notations des chapitres 2 et 3, on ne précise pas l'espace topologique X, qui est systématiquement la droite projective complexe $\mathbb{P}^1(\mathbb{C})$.

On fixe un groupe fini G et un corps de nombres K plongé dans $\overline{\mathbb{Q}}$, et on désigne par Γ_K le groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$ de K.

7.1. Revêtements algébriques

Dans cette section, nous définissons les revêtements et G-revêtements algébriques (Définitions 7.1.3 et 7.1.4). On explicite les liens qui relient ces revêtements au problème de Galois inverse (Corollaires 7.1.8 et 7.1.11) et aux revêtements topologiques du chapitre 2 (Sous-section 7.1.4). Enfin, on définit des notions arithmétiques importantes concernant ces revêtements, notamment leur corps de définition (Sous-section 7.1.5) et l'action du groupe de Galois absolu de K sur les revêtements algébriques (Sous-section 7.1.6).

7.1.1. Configurations algébriques

Au sens de la définition 2.3.8, une configuration est une liste non-ordonnée $\underline{t} = \{t_1, \ldots, t_n\}$ de n nombres complexes distincts. On note $\mathrm{Conf}_n(\mathbb{C})$ l'espace topologique de ces configurations, qui est $\mathrm{Conf}_{n,\mathbb{P}^1(\mathbb{C})}$ avec les notations de la définition 2.3.8.

Définition 7.1.1. Une configuration $\underline{t} \in \mathrm{Conf}_n(\mathbb{C})$ est *définie sur K* lorsque les éléments $t_1, \ldots, t_n$ sont tous algébriques sur $\mathbb{Q}$ et que l'ensemble $\{t_1, \ldots, t_n\}$ est globalement invariant sous l'action du groupe de Galois absolu $\Gamma_K = \mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$. On note $\mathrm{Conf}_n(K)$ l'ensemble des configurations définies sur K.

Définition:
Configuration définie sur K

L'espace des configurations de n points de la droite projective a un pendant schématique. En effet, choisir une configuration $\underline{t} = \{t_1, \ldots, t_n\}$ équivaut au choix d'un polynôme unitaire $(X - t_1) \cdots (X - t_n)$, de degré n et sans racine multiple. On peut paramétrer ces polynômes par leurs coefficients plutôt que par leurs racines. Ce point de vue rend inutile de quotienter par l'action du groupe symétrique $\mathfrak{S}_n$: les configurations vues comme polynômes sont naturellement non-ordonnées. Cela conduit à la définition suivante :

Définition 7.1.2. Le schéma Conf_n est la sous-variété ouverte de $\mathbb{A}^n$ obtenue en enlevant le sous-ensemble Zariski-fermé Δ (la *grosse diagonale*) défini par l'équation polynomiale correspondant au discriminant de $X^n + a_1 X^{n-1} + \ldots + a_{n-1} X + a_n$.

Définition:
Espace des configurations (algébrique)

Les $\mathbb{C}$-points de Conf_n sont en bijection avec les éléments de $\mathrm{Conf}_n(\mathbb{C})$, et cette correspondance est un homéomorphisme si on équipe l'ensemble des $\mathbb{C}$-points de Conf_n de la topologie analytique. Cela rend la notation $\mathrm{Conf}_n(\mathbb{C})$ non-ambiguë. De même, les K-points de Conf_n sont en bijection avec les configurations définies sur K et cela justifie la notation $\mathrm{Conf}_n(K)$.

7.1.2. Les k-G-revêtements algébriques

Soit k un corps, qu'on suppose de caractéristique première à l'ordre $|G|$ du groupe G. On définit les revêtements algébriques de $\mathbb{P}^1_k$ (on ne précisera en général pas « ramifié ») de la manière suivante :

Définition 7.1.3. Un *revêtement algébrique de* $\mathbb{P}^1_k$ est un morphisme fini, plat et génériquement étale d'une courbe projective lisse Y sur k dans la droite projective $\mathbb{P}^1_k$, non-ramifié au dessus du point à l'infini ∞.

Définition:
Revêtement algébrique de $\mathbb{P}^1_k$

Les $\bar{k}$-points de $\mathbb{P}^1_k$ au dessus desquels un revêtement algébrique est ramifié définissent une configuration[1] définie sur k : c'est le *lieu de branchement* du revêtement algébrique. En dehors de ce lieu de branchement, un revêtement algébrique de $\mathbb{P}^1_k$ définit un morphisme fini étale dans $\mathbb{P}^1_k \setminus \underline{t}$.

[1] La finitude du lieu de branchement résulte du fait qu'un morphisme génériquement étale entre courbes lisses est étale en dehors d'un fermé, voir [Stacks, Lemma 0C1C].

Enfin, on réservera l'expression « k-G-revêtement » aux revêtements ramifiés de $\mathbb{P}^1_k$ munis d'une action de G. Comme dans le cas topologique, on ne suppose pas ces revêtements irréductibles :

Définition 7.1.4. Un *k-G-revêtement* est la donnée d'un revêtement algébrique $p : Y \to \mathbb{P}^1_k$ et d'un morphisme de groupes de G dans le groupe $\mathrm{Aut}_{\mathbb{P}^1_k}(Y)$ des automorphismes du revêtement, tel que l'action de G induite sur chaque fibre géométrique non-ramifiée soit libre et transitive.

Définition:
k-G-revêtement

Donnons rapidement la définition d'un morphisme de k-G-revêtements entre $p : Y \to \mathbb{P}^1_k$ et $q : Y' \to \mathbb{P}^1_k$. Il s'agit d'un morphisme de schémas $Y \to Y'$ qui fait commuter le diagramme :

$$\begin{array}{ccc} Y & \longrightarrow & Y' \\ & {\scriptstyle p}\searrow \quad \swarrow{\scriptstyle q} & \\ & \mathbb{P}^1_k & \end{array}$$

et qui commute avec l'action d'un $g \in G$ quelconque :

$$\begin{array}{ccc} Y & \longrightarrow & Y' \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ Y & \longrightarrow & Y' \end{array}.$$

Cette notion définit une catégorie des k-G-revêtements ramifiés de $\mathbb{P}^1$.

Définition: *k-G-revêtement marqué*

Définition 7.1.5. Si k est un corps algébriquement clos, un *k-G-revêtement marqué* est la donnée d'un k-G-revêtement et d'un k-point dans la fibre non-ramifiée au dessus du point à l'infini ∞.

Nous ne définissons volontairement pas la notion de k-G-revêtement marqué lorsque k n'est pas algébriquement clos car il y a deux définitions raisonnables entre lesquelles nous souhaitons éviter toute confusion :

— La donnée d'un k-G-revêtement et d'un point géométrique (c'est-à-dire un $\overline{k}$-point) du revêtement au dessus du point à l'infini.

  Cette notion correspond aux revêtements qui sont classifiés par les *groupes fondamentaux étales* $\pi_1^{\text{ét}}(\mathbb{P}^1_k \setminus \underline{t}, \infty)$ (pour des configurations $\underline{t} \in \mathrm{Conf}_n(k)$). Autrement dit, une classe d'isomorphisme de k-G-revêtements munis d'un point géométrique marqué au dessus du point à l'infini, et non-ramifiés hors d'une configuration $\underline{t} \in \mathrm{Conf}_n(k)$, correspond à un morphisme :

$$\pi_1^{\text{ét}}(\mathbb{P}^1_k \setminus \underline{t}, \infty) \to G.$$

— La donnée d'un k-G-revêtement et d'un k-point du revêtement au dessus du point à l'infini.

  Cette notion, plus restrictive, correspond aux $\overline{k}$-G-revêtements qui sont invariants sous l'action du groupe de Galois absolu Γ_k que nous définissons dans la sous-section 7.1.6.

Des deux, la notion la plus utile pour nous sera la deuxième. Nous choisissons une terminologie non-ambiguë pour désigner ces revêtements :

Définition: *k-G-revêtement muni d'un k-point marqué*

Définition 7.1.6. Un *k-G-revêtement muni d'un k-point marqué* est la donnée d'un k-G-revêtement et d'un k-point dans la fibre au dessus du point à l'infini.

7.1.3. **Revêtements algébriques et extensions de corps de fonctions**

Si $p : Y \to \mathbb{P}^1_k$ est un k-G-revêtement avec Y irréductible, alors le corps de fonctions $k(Y)$ de Y est une extension galoisienne de $k(T)$ dont le groupe de Galois est isomorphe à G. Si, de plus, Y est géométriquement irréductible, cette extension est *régulière* : les seuls éléments de $k(Y)$ qui sont algébriques sur k sont les éléments de k.

Dans le cas des courbes, le foncteur « corps de fonctions » définit une équivalence de catégories, voir [Stacks, Theorem $0BY1$] :

Proposition: *Équivalence entre revêtements algébriques de $\mathbb{P}^1_k$ et extensions de $k(T)$*

Proposition 7.1.7. *Les deux catégories suivantes sont équivalentes :*

— *La catégorie des k-G-revêtements irréductibles.*

— *La catégorie des extensions finies galoisiennes F de $k(T)$ munies d'un isomorphisme entre* $\mathrm{Gal}(F \mid k(T))$ *et G.*

La proposition 7.1.7 lie le problème de Galois inverse sur les corps de fonctions à l'étude des k-G-revêtements :

Corollaire: *Reformulation du problème de Galois inverse sur les corps de fonctions en termes de revêtements*

Corollaire 7.1.8. *Un groupe G est réalisable comme groupe de Galois sur $k(T)$ si et seulement s'il existe un k-G-revêtement irréductible. De plus, il existe une réalisation régulière de G sur $k(T)$ si et seulement s'il existe un k-G-revêtement géométriquement irréductible.*

7.1.3.1. Le théorème d'irréductibilité de Hilbert On présente à présent le théorème d'irréductibilité de Hilbert, qui entraîne l'existence de liens entre le problème de Galois inverse sur $k(T)$ et celui sur k lorsque k est un corps de nombres. La forme la plus connue du théorème d'irréductibilité de Hilbert est la suivante :

Théorème: *Théorème d'irréductibilité de Hilbert*

Théorème 7.1.9. *Soit $n \geq 2$ un entier et $P(x_1, \ldots, x_n) \in \mathbb{Q}(x_1)[x_2, \ldots, x_n]$ un polynôme irréductible. Il existe une infinité de nombres rationnels $x^* \in \mathbb{Q}$ tels que le polynôme $P(x^*, x_2, \ldots, x_n)$, en $n-1$ variables, soit irréductible dans $\mathbb{Q}[x_2, \ldots, x_n]$.*

Ce théorème peut être amélioré de plusieurs façons :

— On peut remplacer $\mathbb{Q}$ par n'importe quel corps de nombres L.

Le théorème original dit que $\mathbb{Q}$ est *hilbertien*, et on sait aussi que toute extension finie d'un corps hilbertien est hilbertienne [FJo8, Corollary 12.2.3]. Mentionnons qu'il existe d'autres corps hilbertiens, tels que $\mathbb{Q}^{\mathrm{ab}}$, ou n'importe quelle extension abélienne d'un corps de nombres.

— Soit L un corps de nombres et L' une extension finie de L. Si le polynôme $P(x_1, \ldots, x_n) \in L'(x_1)[x_2, \ldots, x_n]$ est irréductible, alors on peut choisir un x^* dans le « petit corps » L de sorte que $P(x^*, x_2, \ldots, x_n)$ soit irréductible dans $L'[x_2, \ldots, x_n]$, autrement dit sur le « gros corps ». Pour une référence, on peut consulter [FJo8, Corollary 12.2.3] ou [Völ96, Corollary 1.8. (2)].

— On peut géométriser le théorème 7.1.9 (voir par exemple [BSFP14]) en remplaçant le polynôme par un morphisme fini étale depuis une variété sur L, qu'on suppose irréductible même après extension des scalaires à L', dans une sous-variété ouverte Y de $\mathbb{A}^n_L$, avec $n \geq 1$. Le théorème entraîne alors qu'il existe des L-points de Y au dessus desquels la fibre est irréductible sur L', c'est-à-dire que ses points géométriques sont transitivement permutés par l'action de $\mathrm{Gal}\left(\overline{\mathbb{Q}} \mid L'\right)$.

Un énoncé raffiné possible est le suivant, qui sert dans le chapitre 8 pour la démonstration du théorème 8.4.5 :

Théorème: *Théorème d'irréductibilité de Hilbert, le dernier cri*

Théorème 7.1.10. *Soit L un corps de nombres, L' une extension finie de L, et $p : X \to Y$ un morphisme fini étale d'une variété X sur L dans une sous-variété ouverte Y de $\mathbb{A}^n_L$. On suppose que l'extension des scalaires $X_{L'}$ de X à L' est irréductible. Il existe alors un L-point $t \in Y(L)$ tel que l'action de $\mathrm{Gal}(\overline{\mathbb{Q}} \mid L')$ sur les $\overline{\mathbb{Q}}$-points de X qui sont envoyés sur t par p soit transitive.*

Last but not least, le théorème d'irréductibilité de Hilbert a le corollaire suivant (voir [Völ96, Proposition 1.7 (i)]) qui le rend central dans l'étude du problème de Galois inverse :

Corollaire: *La réalisation de G comme groupe de Galois sur $k(T)$ entraîne sa réalisation sur k*

Corollaire 7.1.11. *Soit k un corps de nombres. S'il existe une extension galoisienne de $k(T)$ dont le groupe de Galois est isomorphe à G (c'est-à-dire, étant donné le corollaire 7.1.8, s'il existe un k-G-revêtement irréductible), alors il existe une extension galoisienne de k dont le groupe de Galois est isomorphe à G.*

7.1.4. Le théorème d'existence de Riemann

Le théorème d'existence de Riemann entraîne que tout revêtement analytique est algébrique. Plus précisément, il induit une équivalence de catégories reliant, d'une part, les revêtements analytiques (ou topologiques, voir la remarque 3.1.1) finis ramifiés de la droite projective complexe et, d'autre part, les revêtements algébriques de $\mathbb{P}^1_k$ (finis, plats, génériquement étales). Au regard de la proposition 7.1.7, cela signifie que les extensions finies de $\mathbb{C}(T)$ dont le groupe de Galois est G sont en correspondance avec les G-revêtements topologiques ramifiés connexes de $\mathbb{P}^1(\mathbb{C})$. Vu le corollaire 2.4.17, cela entraîne une solution positive au problème de Galois inverse sur $\mathbb{C}(T)$:

Corollaire: *Réponse positive au problème de Galois inverse sur* $\mathbb{C}(T)$

Corollaire 7.1.12. *Tout groupe fini est isomorphe au groupe de Galois d'une extension galoisienne de* $\mathbb{C}(T)$.

Le théorème s'énonce également en termes de groupes fondamentaux : étant donnée une configuration $\underline{t} \in \mathrm{Conf}_n(\mathbb{C})$, le groupe fondamental étale $\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \underline{t}, \infty)$, qui par définition classifie les revêtements finis étales marqués, est le complété profini du groupe fondamental topologique $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \underline{t}, \infty)$, qui classifie les revêtements topologiques marqués (voir le théorème 2.2.26). Notamment, pour tout groupe fini G, les morphismes $\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \underline{t}, \infty) \to G$ sont en bijection avec les morphismes $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \underline{t}, \infty) \to G$.

Dans le cas d'une configuration $\underline{t} \in \mathrm{Conf}_n(\overline{\mathbb{Q}})$, constituée de points algébriques sur $\mathbb{Q}$, le groupe fondamental étale $\pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} \setminus \underline{t}, \infty)$ sur $\mathbb{C}$ est isomorphe au groupe fondamental étale $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \underline{t}, \infty)$ sur $\overline{\mathbb{Q}}$ (voir par exemple [Lan20]). En conséquence, on peut (à isomorphisme près) assimiler les G-revêtements topologiques de $\mathbb{P}^1(\mathbb{C})$, ramifiés en une configuration $\underline{t} \in \mathrm{Conf}_n(\overline{\mathbb{Q}})$, et les $\overline{\mathbb{Q}}$-G-revêtements ramifiés en $\underline{t}$.

Dans la suite, on ne justifie pas systématiquement d'alterner les points de vue : on identifie implicitement G-revêtements topologiques et $\mathbb{C}$-G-revêtements (ou $\overline{\mathbb{Q}}$-G-revêtements lorsque les points de branchement sont algébriques).

7.1.5. Corps de définition des G-revêtements

Le théorème d'existence de Riemann pose les bases d'une approche géométrique du problème de Galois inverse régulier : sur un corps algébriquement clos de caractéristique nulle, la situation se réduit à celle des revêtements topologiques. Le cas des corps non-algébriquement clos peut alors être envisagé du point de vue de la descente galoisienne : on cherche des critères, notamment géométriques, pouvant assurer que certains $\overline{\mathbb{Q}}$-G-revêtements proviennent, par extension des scalaires, de $\mathbb{Q}$-G-revêtements (dans l'exemple de $\mathbb{Q}$). D'après le corollaire 7.1.11, une telle conclusion entraîne que le groupe G est réalisable comme groupe de Galois sur $\mathbb{Q}$.

On définit le corps de définition d'un G-revêtement de la façon suivante :

Définition: *Revêtement défini sur k* *Corps de définition d'un revêtement*

Définition 7.1.13. Un $\mathbb{C}$-G-revêtement, ramifié en une configuration $\underline{t} \in \mathrm{Conf}_n(k)$, est *défini sur k* s'il est isomorphe au $\mathbb{C}$-G-revêtement obtenu par extension des scalaires d'un k-G-revêtement ramifié en $\underline{t}$. Un G-revêtement topologique de $\mathbb{P}^1(\mathbb{C})$, ramifié en $\underline{t}$, est *défini sur K* lorsque le $\mathbb{C}$-G-revêtement qui lui correspond par le théorème d'existence de Riemann (défini à isomorphisme près) est défini sur K. Dans cette situation, le corps K est un *corps de définition* du G-revêtement.

Le problème de Galois inverse régulier sur $K(T)$, pour le groupe G, est équivalent à

la question suivante : parmi les G-revêtements ramifiés connexes de $\mathbb{P}^1(\mathbb{C})$, en existe-t-il un qui soit défini sur K ?

On résume par un diagramme la stratégie suggérée par cette approche :

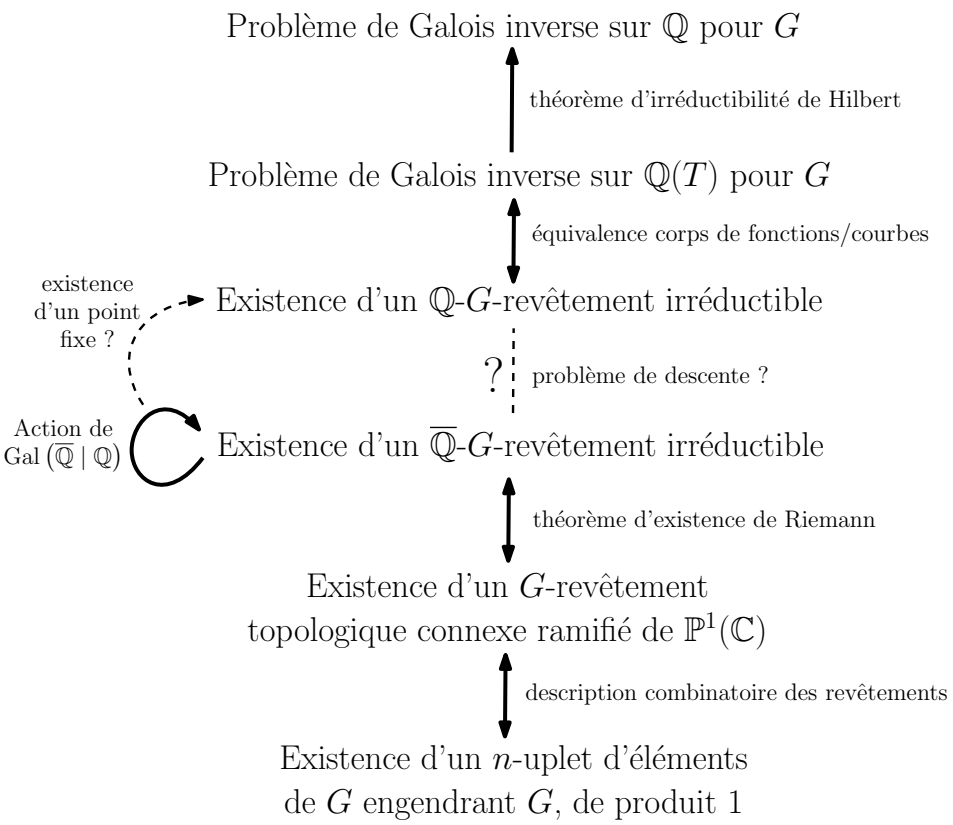


Figure 7.1.14.
La stratégie régulière pour le problème de Galois inverse sur $\mathbb{Q}$ pour le groupe G

Sans rentrer dans les détails, disons ici un mot sur la forme que prennent les critères géométriques qui permettent d'obtenir des informations sur les corps de définition des revêtements. Les critères connus sont des critères de *rigidité* : d'abord, on identifie des propriétés des G-revêtements qui sont, pour des raisons arithmétiques, invariantes sous l'action du groupe de Galois absolu $\mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$ – action qu'on décrit dans la sous-section 7.1.6. On montre ensuite, par des arguments géométriques, que (de façon exceptionnelle) ces invariants caractérisent de manière unique le G-revêtement qu'on considère. Cela entraîne alors que le G-revêtement en question est défini sur K. Des arguments similaires sont utilisés dans le chapitre 8.

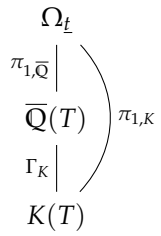
7.1.6. **L'action de Galois**

Dans cette sous-section, nous définissons une action du groupe de Galois $\Gamma_K = \mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$ sur les $\overline{\mathbb{Q}}$-G-revêtements.

7.1.6.1. Définitions. On fixe une configuration $\underline{t} \in \mathrm{Conf}_n(K)$, définie sur le corps de nombres K. On désigne par $\pi_{1,\overline{\mathbb{Q}}}$ le groupe fondamental étale "géométrique" $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \underline{t}, \infty)$ et par $\pi_{1,K}$ le groupe fondamental étale "arithmétique" $\pi_1^{\text{ét}}(\mathbb{P}^1_K \setminus \underline{t}, \infty)$.

On fixe une clôture algébrique $\overline{\mathbb{Q}(T)}$ de $\mathbb{Q}(T)$ qui contient $\overline{\mathbb{Q}}$, puis on définit le corps suivant : $\Omega_{\underline{t}}$ est la sous-extension maximale de $\overline{\mathbb{Q}(T)} \mid \overline{\mathbb{Q}}(T)$ qui est non-ramifiée hors des places correspondant à $\underline{t}$.[2] On a la chaîne d'extensions :

[2] Il faut envisager cette extension de $\overline{\mathbb{Q}}(T)$ comme un équivalent du revêtement universel de $\mathbb{P}^1(\mathbb{C}) \setminus \underline{t}$.



dont on tire la suite exacte courte suivante :

$$1 \longrightarrow \pi_{1,\overline{\mathbb{Q}}} \longrightarrow \pi_{1,K} \longrightarrow \Gamma_K \longrightarrow 1 \ . \tag{7.1.1}$$

Le corps $\Omega_{\underline{t}}$ est plongé dans $\overline{\mathbb{Q}(T)}$, lui-même plongé dans le corps des séries de Puiseux sur $\overline{\mathbb{Q}}$ qu'on note $\overline{\mathbb{Q}}\left(\!\left((1/T)^{1/\infty} \right)\!\right)$. Le groupe de Galois absolu $\Gamma_K = \mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$ agit sur le corps $\overline{\mathbb{Q}}\left(\!\left((1/T)^{1/\infty} \right)\!\right)$ des séries de Puiseux en agissant sur chaque coefficient d'une telle série.

Considérons un automorphisme $\sigma \in \Gamma_K$. La configuration $\underline{t}$ étant définie sur K, l'image par σ d'une extension de $\overline{\mathbb{Q}}(T)$ non-ramifiée hors de $\underline{t}$ est elle-aussi non-ramifiée hors de $\underline{t}$: le corps $\Omega_{\underline{t}}$ est donc stable sous l'action de Γ_K. Il y a ainsi une action de Γ_K sur $\Omega_{\underline{t}}$, triviale sur $K(T)$. Cette action correspond à un morphisme de groupes :

$$s : \Gamma_K \to \mathrm{Gal}\left(\Omega_{\underline{t}} \mid K(T)\right) \simeq \pi_{1,K}.$$

Le morphisme s est une section de la suite exacte courte de l'équation (7.1.1) :

$$1 \longrightarrow \pi_{1,\overline{\mathbb{Q}}} \longrightarrow \pi_{1,K} \underset{\curvearrowleft s}{\longrightarrow} \Gamma_K \longrightarrow 1.$$

On définit une action de Γ_K sur le groupe fondamental étale $\pi_{1,\overline{\mathbb{Q}}}$ en utilisant le morphisme s :

Définition: *Action de Galois sur le groupe fondamental étale $\pi_{1,\overline{\mathbb{Q}}}$*

Définition 7.1.15. Pour tout $\sigma \in \Gamma_K$ et $\gamma \in \pi_{1,\overline{\mathbb{Q}}}$, on pose :

$$\sigma.\gamma \overset{\text{def}}{=} \gamma^{s(\sigma)}.$$

Il s'agit bien un élément de $\pi_{1,\overline{\mathbb{Q}}}$, puisque ce sous-groupe est normal dans $\pi_{1,K}$.

Enfin, on définit l'action de Γ_K sur les G-revêtements marqués :

Définition: *Action de Galois sur les G-revêtements marqués*

Définition 7.1.16. L'action d'un automorphisme $\sigma \in \Gamma_K$ sur une classe d'isomorphisme de G-revêtements marqués de $\mathbb{P}^1(\mathbb{C})$ ramifiés en $\underline{t}$, vue comme un morphisme $\varphi : \pi_{1,\overline{\mathbb{Q}}} \to G$, est définie par l'égalité suivante pour tout $\gamma \in \pi_{1,\overline{\mathbb{Q}}}$:

$$(\sigma.\varphi)(\gamma) \overset{\text{def}}{=} \varphi(\sigma.\gamma) = \varphi\left(\gamma^{s(\sigma)}\right).$$

Cette action préserve le groupe de monodromie d'un G-revêtement ramifié en $\underline{t}$. De plus, on a l'égalité $\sigma.(\varphi^g) = (\sigma.\varphi)^g$ pour tout $g \in G$: le groupe Γ_K agit donc aussi sur les classes d'isomorphisme de G-revêtements *non-marqués* ramifiés en $\underline{t}$.

7.1.6.2. Corps de définition et action de Galois. L'action de Galois permet de caractériser les corps de définition des G-revêtements non-marqués :

Proposition: *Corps de définition et action de Galois*

Proposition 7.1.17. *Soit φ un morphisme de groupes $\pi_{1,\overline{\mathbb{Q}}} \to G$. Les deux propriétés suivantes sont équivalentes :*

1. *Il existe un morphisme de groupes $\rho : \Gamma_K \to G$ tel que :*

$$\forall \sigma \in \Gamma_K,\ \sigma.\varphi = \varphi^{\rho(\sigma)}.$$

Cette propriété est plus forte que la condition « l'orbite de φ sous l'action de conjugaison de G est invariante sous l'action de Γ_K », qui correspond au cas où ρ est une simple application. Cependant, si le centralisateur dans G de l'image de φ est trivial, alors $\rho(\sigma)$ est uniquement défini s'il existe, l'application ρ est donc nécessairement un morphisme si elle existe, et les deux notions sont alors équivalentes.

2. *Le morphisme φ s'étend à $\pi_{1,K}$, c'est-à-dire qu'il existe un morphisme de groupes $\widetilde{\varphi} : \pi_{1,K} \to G$ tel que le diagramme suivant commute :*

$$\begin{array}{ccc} \pi_{1,\overline{\mathbb{Q}}} & \hookrightarrow & \pi_{1,K} \\ & \searrow^{\varphi} & \downarrow{\scriptstyle \widetilde{\varphi}} \\ & & G \end{array}.$$

Cette condition correspond au fait que le G-revêtement non-marqué correspondant à l'orbite de φ sous l'action de conjugaison provienne d'un K-G-revêtement non-marqué, c'est-à-dire que ce G-revêtement soit défini sur K.

Démonstration. Commençons par donner des noms aux morphismes de groupes intervenant dans la suite exacte de l'équation (7.1.1) :

$$\pi_{1,\overline{\mathbb{Q}}} \overset{\iota}{\hookrightarrow} \pi_{1,K} \overset{w}{\twoheadrightarrow} \Gamma_K.$$

Rappelons que le morphisme $s : \Gamma_K \to \pi_{1,K}$ est une section de w, c'est-à-dire que $w \circ s = \mathrm{id}_{\pi_{1,K}}$.

(2 ⇒ 1) Supposons que φ s'étende en un morphisme $\widetilde{\varphi} : \pi_{1,K} \to G$ tel que $\varphi = \widetilde{\varphi} \circ \iota$. Pour tout $\gamma \in \pi_{1,\overline{\mathbb{Q}}}$, on a :

$$\sigma.\varphi(\gamma) = \varphi\left(\gamma^{s(\sigma)}\right) = \widetilde{\varphi}\left(\gamma^{s(\sigma)}\right) = \widetilde{\varphi}(\gamma)^{\widetilde{\varphi}(s(\sigma))} = \varphi(\gamma)^{\widetilde{\varphi}(s(\sigma))}.$$

On a alors la première propriété avec $\rho = \widetilde{\varphi} \circ s$.

(1 ⇒ 2) Supposons qu'il existe un morphisme de groupes $\rho : \Gamma_K \to G$ tel que $\sigma.\varphi = \varphi^{\rho(\sigma)}$ pour tout $\sigma \in \Gamma_K$. Soit $\gamma \in \pi_{1,K}$. Nous avons :

$$w\left(\gamma s(w(\gamma))^{-1}\right) = w(\gamma)w(s(w(\gamma)))^{-1} = w(\gamma)w(\gamma)^{-1} = 1,$$

et par conséquent (la suite de l'équation (7.1.1) étant exacte) l'élément $\gamma s(w(\gamma))^{-1}$ appartient à $\pi_{1,\overline{\mathbb{Q}}}$. On définit alors l'application suivante :

$$\widetilde{\varphi} : \begin{cases} \pi_{1,K} & \to & G \\ \gamma & \mapsto & \varphi(\gamma s(w(\gamma))^{-1})\rho(w(\gamma)) \end{cases}.$$

Si $\gamma \in \pi_{1,\overline{\mathbb{Q}}}$, alors $w(\gamma) = 1$ et donc $\widetilde{\varphi}(x) = \varphi(x)$. Ainsi $\varphi = \widetilde{\varphi} \circ \iota$: l'application $\widetilde{\varphi}$ étend bien φ. Reste à vérifier que l'application $\widetilde{\varphi}$ est un morphisme de groupes. Pour tous éléments $x, y \in \pi_{1,K}$, on a :

$$\begin{aligned}
\widetilde{\varphi}(x)\widetilde{\varphi}(y) &= \varphi\big(xs(w(x))^{-1}\big)\rho\big(w(x)\big)\,\varphi\big(ys(w(y))^{-1}\big)\rho\big(w(y)\big) && \text{définition de } \widetilde{\varphi}\\
&= \varphi\big(xs(w(x))^{-1}\big)\,\varphi\big(ys(w(y))^{-1}\big)^{\rho\left(w(x)\right)}\,\rho\big(w(xy)\big) && \rho \text{ est un morphisme}\\
&= \varphi\big(xs(w(x))^{-1}\big)\,\big(w(x).\varphi\big)\big(ys(w(y))^{-1}\big)\,\rho\big(w(xy)\big) && \text{définition de } \rho\\
&= \varphi\big(xs(w(x))^{-1}\big)\,\varphi\Big(s\big(w(x)\big)ys\big(w(y)\big)^{-1}s\big(w(x)\big)^{-1}\Big)\,\rho\big(w(xy)\big) && \text{définition 7.1.16}\\
&= \varphi(xys(w(xy))^{-1})\rho(w(xy))\\
&= \widetilde{\varphi}(xy) && \text{définition de } \widetilde{\varphi}
\end{aligned}$$

Ceci conclut la preuve.

□

On a également un énoncé pour les G-revêtements marqués :

Proposition: *Corps de définition et action de Galois, cas marqué*

Proposition 7.1.18. *Soit φ un morphisme de groupes $\pi_{1,\overline{\mathbb{Q}}} \to G$. Les deux propriétés suivantes sont équivalentes :*

1. *Le morphisme φ est invariant sous l'action de Galois, c'est-à-dire que pour tout $\sigma \in \Gamma_K$, on a :*
$$\sigma.\varphi = \varphi.$$
2. *Le morphisme φ s'étend à $\pi_{1,K}$ par un morphisme $\widetilde{\varphi} : \pi_{1,K} \to G$ qui est trivial sur l'image $\mathrm{Im}(s)$ du morphisme s.*

   Cette condition correspond au fait que le G-revêtement marqué correspondant à φ provienne d'un K-G-revêtement muni d'un K-point marqué.

Démonstration. Il suffit de reprendre la preuve de la proposition 7.1.17 : pour $(2 \Rightarrow 1)$, on a $\rho = \widetilde{\varphi} \circ s = 1$; pour $(1 \Rightarrow 2)$, on part avec $\rho = 1$ et ainsi $\widetilde{\varphi}(\gamma)$ est défini comme $\varphi\big(\gamma s(w(\gamma))^{-1}\big)$ qui vaut 1 lorsque $\gamma \in \mathrm{Im}(s)$. □

Remarque 7.1.19. L'image de l'extension $\widetilde{\varphi} : \pi_{1,K} \to G$ de φ est généralement plus grande que l'image φ. Cela est lié au fait que le K-G-revêtement correspondant au morphisme $\widetilde{\varphi}$ puisse être irréductible ($\widetilde{\varphi}$ est surjective) sans être géométriquement irréductible (φ n'est pas surjective).

7.2. Les schémas de Hurwitz

Dans la remarque 3.1.1, on a mentionné que les espaces de Hurwitz pouvaient être munis d'une structure naturelle de variétés analytiques complexes, comme revêtements finis d'espaces de configurations. Des résultats de type « G.A.-G.A. »[3] entraînent que ces espaces sont alors aussi des variétés algébriques complexes, en l'occurrence des $\mathbb{C}$-schémas avec un morphisme fini étale dans les espaces de configuration $(\mathrm{Conf}_n)_{\mathbb{C}}$. En réalité, les espaces de Hurwitz sont définis sur $\mathbb{Q}$ – une façon de s'en rendre compte est d'observer qu'on a (partiellement) défini plus haut une action de $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ sur les $\overline{\mathbb{Q}}$-points des espaces de Hurwitz ; un critère de descente dû à Weil assure alors que cette action provient bien de l'action de $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ sur les points géométriques d'un $\mathbb{Q}$-schéma.[4] Pour la construction de ces espaces, on peut consulter [RW06, Theorem 4.11].

[3] « Géométrie Algébrique et Géométrie Analytique » [Ser56] ; le théorème d'existence de Riemann vu précédemment est un exemple de tel résultat.

[4] En réalité, les espaces de Hurwitz sont même définis sur $\mathbb{Z}[1/|G|]$, mais nous les voyons ici toujours comme $\mathbb{Q}$-schémas.

7.2.1. **Espaces de Hurwitz algébriques**

Nous présentons désormais les espaces de Hurwitz que nous considérons, en mentionnant leurs propriétés les plus importantes :

— Le $\mathbb{Q}$-schéma $\mathcal{H}^*(G,n)$ est l'espace de Hurwitz des G-revêtements marqués de $\mathbb{P}^1$, ramifiés en n points, et non-ramifiés au dessus du point à l'infini. Il s'agit d'un revêtement fini étale, en général non irréductible, du $\mathbb{Q}$-schéma Conf_n.

L'ensemble des $\mathbb{C}$-points de $\mathcal{H}^*(G,n)$, muni de la topologie analytique, est homéomorphe à l'espace de Hurwitz topologique $\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(G,n)$. Ainsi, les points géométriques du schéma $\mathcal{H}^*(G,n)$ correspondent aux G-revêtements topologiques marqués de $\mathbb{P}^1(\mathbb{C})$, ramifiés en n points. L'action de Γ_K sur les $\overline{\mathbb{Q}}$-points au-dessus d'un K-point de Conf_n coïncide avec l'action de la définition 7.1.16.

Le $\mathbb{Q}$-schéma $\mathcal{CH}^*(G,n)$ est le sous-schéma de $\mathcal{H}^*(G,n)$ obtenu en ne considérant que les G-revêtements marqués géométriquement connexes. L'ensemble des $\mathbb{C}$-points de $\mathcal{CH}^*(G,n)$, muni de la topologie analytique, est homéomorphe à $\mathrm{CHur}^*_{\mathbb{P}^1(\mathbb{C})}(G,n)$.

Ces espaces de Hurwitz sont des espaces de modules fins. En particulier, leurs K-points correspondent aux K-G-revêtements (géométriquement connexes dans le cas de $\mathcal{CH}^*(G,n)$), munis d'un K-point marqué dans la fibre non-ramifiée au dessus du point à l'infini.

L'existence d'un $\mathbb{Q}$-point de $\mathcal{CH}^*(G,n)$ entraîne qu'il existe une extension galoisienne régulière de $\mathbb{Q}(T)$, de groupe de Galois G, ramifiée en n places, et telle qu'il existe un premier non-ramifié de degré 1 (le $\mathbb{Q}$-point marqué). En particulier, cela donne une réponse positive au problème de Galois inverse pour G sur $\mathbb{Q}$ par le théorème d'irréductibilité de Hilbert (plus précisément le corollaire 7.1.11).

— Le $\mathbb{Q}$-schéma $\mathcal{H}(G,n)$ est l'espace de Hurwitz des G-revêtements non-marqués de $\mathbb{P}^1$, ramifiés en n points, et non-ramifiés au dessus du point à l'infini. Il s'agit d'un revêtement fini étale, en général non irréductible, du $\mathbb{Q}$-schéma Conf_n.

L'ensemble des $\mathbb{C}$-points de $\mathcal{H}(G,n)$, muni de la topologie analytique, est homéomorphe à l'espace de Hurwitz topologique $\mathrm{Hur}_{\mathbb{P}^1(\mathbb{C})}(G,n)$. Ainsi, les points géométriques de $\mathcal{H}(G,n)$ correspondent aux G-revêtements topologiques non-marqués de $\mathbb{P}^1(\mathbb{C})$, ramifiés en n points. L'action de Γ_K sur les $\overline{\mathbb{Q}}$-points au-dessus d'un K-point de Conf_n coïncide avec l'action induite par celle de la définition 7.1.16.

Le $\mathbb{Q}$-schéma $\mathcal{CH}(G,n)$ est le sous-schéma de $\mathcal{H}(G,n)$ obtenu en ne considérant que les G-revêtements géométriquement connexes. L'ensemble des $\mathbb{C}$-points de $\mathcal{CH}(G,n)$, muni de la topologie analytique, est homéomorphe à $\mathrm{CHur}_{\mathbb{P}^1(\mathbb{C})}(G,n)$.

Ces espaces de Hurwitz sont, en général, des espaces de modules grossiers[5]. Un G-revêtement défini sur K donne lieu à un K-point, mais les K-points ne correspondent pas nécessairement à des revêtements définis sur K. En effet, un point géométrique est invariant sous l'action de Galois lorsque le morphisme de monodromie d'un marquage arbitraire du G-revêtement correspondant satisfait :

$$\forall \sigma \in \Gamma_K,\ \exists \rho(\sigma) \in G,\ \sigma.\varphi = \varphi^{\rho(\sigma)}.$$

Cependant, il faut pouvoir assurer que ρ ne soit pas une simple application, mais un morphisme, pour que le G-revêtement soit défini sur K (voir la

[5] $\mathcal{H}(G,n)$ est l'espace de modules grossier du champ de Deligne-Mumford obtenu comme quotient de $\mathcal{H}^*(G,n)$ par l'action de conjugaison de $\mathrm{Inn}(G)$.

proposition 7.1.17). Si le groupe G est de centre trivial (par exemple si G est simple), alors $\mathcal{CH}(G,n)$ est un espace de modules fin, et ses K-points correspondent à des K-G-revêtements géométriquement irréductibles. Dans ce cas, l'existence d'un $\mathbb{Q}$-point de $\mathcal{CH}(G,n)$ implique également une réponse positive au problème de Galois inverse pour G sur $\mathbb{Q}$.

Il est possible de relier k-G-revêtements et k-points des espaces de Hurwitz lorsque le centre de G n'est pas trivial, mais cela induit des complications. On pourra consulter [DD97] pour plus d'informations sur le sujet, et regarder les deux preuves de [ETW17, Proposition 8.4] pour une situation où ces difficultés sont surmontées.

Les propriétés des espaces de Hurwitz suggèrent une stratégie pour le problème de Galois inverse :

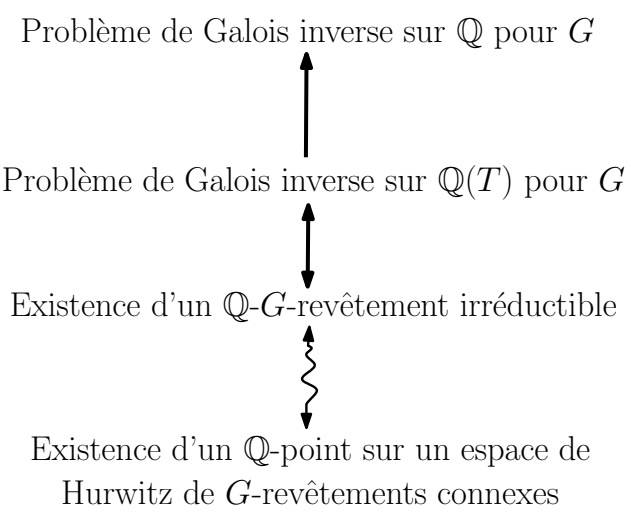


Figure 7.2.1. Une stratégie pour le problème de Galois inverse

7.2.2. **Composantes des espaces de Hurwitz**

7.2.2.1. Description dans le cas algébriquement clos. Les composantes géométriquement connexes de $\mathcal{H}^*(G,n)$, c'est-à-dire les composantes connexes de l'extension des scalaires de $\mathcal{H}^*(G,n)$ à n'importe quel corps non-algébriquement clos de caractéristique nulle, sont en bijection avec les composantes connexes de $\mathrm{Hur}^*(G,n)$. Par conséquent (voir le théorème 3.3.7), ces composantes sont en bijection avec les orbites sous l'action du groupe des tresses de n-uplets $\underline{g} \in G^n$ dont le produit $\pi\underline{g} = g_1 \cdots g_n$ vaut 1. En particulier, l'opération de recollement des composantes (voir la sous-section 3.4.1) peut être vue comme une opération de recollement entre composantes géométriquement connexes. Les éléments de degré n du monoïde des composantes $\mathrm{Comp}(G)$ peuvent alors être assimilés aux composantes de $\mathcal{H}^*(G,n)_{\mathbb{C}}$, ou de manière équivalente de $\mathcal{H}^*(G,n)_{\overline{\mathbb{Q}}}$. On fait assez librement l'identification entre :

1) les composantes connexes de $\mathcal{H}^*(G,n)_{\overline{\mathbb{Q}}}$ ou de $\mathcal{H}^*(G,n)_{\mathbb{C}}$,
2) les composantes connexes de $\mathrm{Hur}^*(G,n)$,
3) les éléments de degré n de $\mathrm{Comp}(G)$.

Bien sûr, on obtient également des descriptions combinatoires, identiques à celles de la sous-section 3.3.2, pour les composantes géométriquement connexes

de $\mathcal{CH}^*(G,n)$, de $\mathcal{H}(G,n)$ et de $\mathcal{CH}(G,n)$: ces composantes correspondent respectivement aux composantes connexes de $\mathrm{CHur}^*(G,n)$, $\mathrm{Hur}(G,n)$ et $\mathrm{CHur}(G,n)$ et admettent les mêmes descriptions combinatoires.

7.2.2.2. Corps de définition des composantes. Si l'espace de Hurwitz $\mathcal{H}^*(G,n)$ pris dans son ensemble est un $\mathbb{Q}$-schéma, les composantes géométriquement connexes prises indépendamment ne proviennent en général pas de sous-schémas de $\mathcal{H}^*(G,n)$ par extension des scalaires. Pour cause, l'action du groupe de Galois absolu $\Gamma_K = \mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$ sur les G-revêtements marqués (c'est-à-dire les points géométriques de $\mathcal{H}^*(G,n)$) induit une action, bien définie, de Γ_K sur les composantes géométriquement connexes de $\mathcal{H}^*(G,n)$, c'est-à-dire sur l'ensemble gradué $\mathrm{Comp}(G)$[6], et cette action n'est en général pas triviale : les composantes sont permutées par l'action du groupe de Galois.

On introduit, comme pour les revêtements, la notion de corps de définition pour les composantes :

[6] Il ne s'agit pas d'une action sur le monoïde $\mathrm{Comp}(G)$, autrement dit cette action n'est a priori pas compatible avec l'opération de recollement. Ce point est au centre du chapitre 8.

Définition: *Corps de définition d'une composante*

Définition 7.2.2. Une composante géométriquement connexe x de $\mathcal{H}^*(G,n)$, c'est-à-dire un élément $x \in \mathrm{Comp}(G)$ de degré n, est *définie sur K* si elle provient d'un sous-schéma de $\mathcal{H}^*(G,n)$ par extension des scalaires, ou de manière équivalente si $\sigma.x = x$ pour tout $\sigma \in \Gamma_K$ (voir la proposition 1.4.13). Dans ce cas, le corps K est un *corps de définition* de la composante x.

On dit d'une composante géométriquement connexe de $\mathcal{H}(G,n)$, représentée par l'orbite sous l'action de conjugaison de G d'un élément $x \in \mathrm{Comp}(G)$, qu'elle est *définie sur K* lorsque pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$, il existe $g \in G$ tel que $\sigma.x = x^g$.

Remarque 7.2.3. L'action de Γ_K sur l'ensemble gradué $\mathrm{Comp}(G)$ induit une action, qui préserve le degré, sur l'espace vectoriel gradué $R_{\mathbb{P}^1(\mathbb{C})}(G,n)$ (c'est-à-dire l'anneau des composantes de la définition 3.4.12, dont on oublie la structure d'anneau). Pour cette action, les sous-espaces vectoriels que constituent les idéaux I_G, I_G^*, J_G et J_G^* et le sous-anneau R^G sont tous stables sous l'action de Galois (qui n'affecte pas le groupe de monodromie des revêtements).

7.2.3. **Le lemme des cycles de branchement**

L'action du groupe de Galois Γ_K sur les G-revêtements et leurs composantes est difficile à décrire en général. Cependant, l'action sur les multidiscriminants (Définitions 1.4.6 et 2.3.29) est très bien décrite par le *lemme des cycles de branchements* de Fried.

Soit $\underline{t} = \{t_1, \dots, t_n\} \in \mathrm{Conf}_n(K)$ une configuration définie sur K et un automorphisme $\sigma \in \Gamma_K$. L'automorphisme σ permute les points de branchement de $\underline{t}$. On note également σ la permutation de l'ensemble $\{1, \dots, n\}$ telle que $\sigma.t_i = t_{\sigma(i)}$.

Soit un G-revêtement marqué ramifié en $\underline{t}$, qu'on voit comme un morphisme de groupes $\varphi : \pi_{1,\overline{\mathbb{Q}}} \to G$. Soit $(\gamma_1, \dots, \gamma_n) \in \pi_{1,\overline{\mathbb{Q}}}^n$ l'image dans $\pi_{1,\overline{\mathbb{Q}}}$ d'un bouquet topologique associé à $\underline{t}$.

Le résultat suivant est classique (voir [Fri77], ou [Cau12, Lemme 2.2] pour un énoncé plus proche du nôtre) :

Lemme 7.2.4. *L'élément local de monodromie $(\sigma.\varphi)(\gamma_i)$ est conjugué à $\left(\varphi(\gamma_{\sigma^{-1}(i)})\right)^{\chi(\sigma)^{-1}}$.*

Lemme: *Le lemme des cycles de branchement*

Autrement dit, la classe de monodromie, au point t_i, du G-revêtement sur lequel σ a agi est la puissance $\chi(\sigma)^{-1}$-ième de la classe de monodromie, au point $\sigma^{-1}(t_i)$, du G-revêtement original.

On réécrit le lemme 7.2.4 en termes de multidiscriminants de composantes. Soit $\underline{g} = (\varphi(\gamma_1), \ldots, \varphi(\gamma_n))$ la description des cycles de branchement de φ, et $\sigma.\underline{g} = (\varphi(\sigma.\gamma_1), \ldots, \varphi(\sigma.\gamma_n))$ la description des cycles de branchement de $\sigma.\varphi$. Soit H un sous-groupe de G contenant $\left\langle \underline{g} \right\rangle$, et c un sous-ensemble de H invariant par conjugaison, K-rationnel (voir la définition 1.4.2), et qui contient les éléments du uplet g_i. On note D^* l'ensemble des classes de conjugaison de H contenues dans c. Pour tout $\sigma \in \Gamma_K$, on note p_σ l'application $D^* \to D^*$ induite par la puissance $\chi(\sigma)$-ième (cette application existe car c est K-rationnel).

Soit $x \in \mathrm{Comp}(G)$ la composante représentée par le uplet $\underline{g}$. On rappelle (Définitions 1.4.6 et 2.3.29)) que le (H,c)-multidiscriminant $\mu_{H,c}(x)$ de x est l'application qui associe à chaque classe de conjugaison $\gamma \in D^*$ le nombre d'occurrences de la classe de conjugaison γ dans le uplet $\underline{g}$.

Définition 7.2.5. La composante *x a un (H,c)-multidiscriminant K-rationnel* si l'égalité suivante est satisfaite pour tout $\sigma \in \Gamma_K$:

Définition: *(H,c)-multidiscriminant K-rationnel*

$$\mu_{H,c}(x) = \mu_{H,c}(x) \circ p_\sigma.$$

Autrement dit, chaque classe de conjugaison $\gamma \in D^*$ apparaît autant de fois dans le uplet $\underline{g}$ que la classe $\gamma^{\chi(\sigma)}$, quel que soit $\sigma \in \Gamma_K$.

Un produit de composantes ayant un (H,c)-multidiscriminant K-rationnel a lui-même un (H,c)-multidiscriminant K-rationnel.

Du lemme 7.2.4, on déduit le corollaire 7.2.6. Le corollaire 7.2.6 (ii) donne une condition nécessaire facile à vérifier pour qu'une composante soit définie sur K – et le corollaire 7.2.6 (iii) dit que cette condition est suffisante dans le cas abélien :

Corollaire 7.2.6.

Corollaire: *Le lemme des cycles de branchement en termes de multidiscriminants*

(i) Pour tout $\sigma \in \Gamma_K$, les (H,c)-multidiscriminants des composantes x et $\sigma.x$ sont liés par l'égalité :

$$\mu_{H,c}(\sigma.x) = \mu_{H,c}(x) \circ p_\sigma.$$

(ii) Si la composante x est définie sur K, alors elle a un (H,c)-multidiscriminant K-rationnel.

(iii) Si la composante x a un (H,c)-multidiscriminant K-rationnel et que le groupe H est abélien, alors la composante x est définie sur K.

Démonstration. (i) Soit $\gamma \in D^*$ une classe de conjugaison. L'entier $\mu_{H,c}(\sigma.x)(\gamma)$ est le nombre d'occurrence de γ dans le uplet $\sigma.\underline{g}$. Par le lemme 7.2.4, ce nombre est égal au nombre d'occurrence de la classe de conjugaison $\gamma^{\chi(\sigma)}$ dans $\underline{g}$, c'est-à-dire à l'entier $\mu_{H,c}(x)(\gamma^{\chi(\sigma)})$.

(ii) Puisque x est définie sur K, nous avons l'égalité $\sigma.x = x$ pour chaque $\sigma \in \Gamma_K$. Par le point (i), cela entraîne $\mu_{H,c}(x) = \mu_{H,c}(x) \circ p_\sigma$, c'est-à-dire que x a un (H,c)-multidiscriminant K-rationnel.

(iii) Le groupe H étant abélien, les classes de conjugaison de H peuvent être identifiées aux éléments de H, et les composantes sont simplement des listes non-ordonnées d'éléments de H dont le produit vaut 1 (le groupe des tresses n'agit que par permutation). Ainsi, deux composantes sont égales exactement lorsque leurs (H,c)-multidiscriminants sont égaux.

La composante x ayant un (H,c)-multidiscriminant K-rationnel, elle a, par le point (i), le même (H,c)-multidiscriminant que la composante $\sigma.x$ pour tout $\sigma.x$; ces composantes sont donc égales.

□

Exemple 7.2.7. Supposons que le groupe G soit abélien. Le corollaire 7.2.6 (iii) permet de déterminer le corps de définition des composantes. Par exemple, la composante représentée par le uplet $\underline{g} \in G^n$ est définie sur $\mathbb{Q}$ si et seulement si tout élément $g \in G$ apparaît autant de fois dans le uplet $\underline{g}$ que chaque élément g^k où k est premier avec l'ordre de g. Donnons des exemples :

— La composante $(1,1,1) \in \mathrm{Comp}(\mathbb{Z}/3\mathbb{Z})$ n'est pas définie sur $\mathbb{Q}$, puisque 1 n'apparaît pas autant de fois que -1.

— La composante $(1,-1) \in \mathrm{Comp}(\mathbb{Z}/n\mathbb{Z})$ est définie sur $\mathbb{Q}$ lorsque $n \in \{2,3,4,6\}$, et n'est pas définie sur $\mathbb{Q}$ si $n = 5$ ou $n \geq 7$.

Exemple 7.2.8. Il suit du théorème 6.2.6 que les composantes de $\mathfrak{S}_d$-revêtements dont les éléments locaux de monodromie sont des transpositions sont entièrement déterminées par leur groupe de monodromie H et par leur (H,H)-multidiscriminant. Les transpositions étant des involutions, on déduit de corollaire 7.2.6 (i) que l'action de $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ préserve le multidiscriminant des composantes. Par conséquent, ces composantes sont toutes définies sur $\mathbb{Q}$.

Remarque 7.2.9. Soit D un ensemble de sous-ensembles de G disjoints et invariants par conjugaison, et ξ une application $D \to \{1,2,\ldots\}$. Le lemme des cycles de branchement donne les conditions pour définir un espace de Hurwitz $\mathcal{H}^*(G,D,\xi)$, défini sur $\mathbb{Q}$ et dont les $\mathbb{C}$-points correspondent aux points de $\mathrm{Hur}^*(G,D,\xi)$: il faut et il suffit qu'il existe, pour tout automorphisme $\sigma \in \Gamma_K$, une application $p_\sigma : D \to D$ telle que les puissances $\chi(\sigma)$-ièmes des éléments d'un $\gamma \in D$ soient des éléments de $p_\sigma(\gamma) \in D$ et telle que $\xi \circ p_\sigma = \xi$. Dans le cas où D est un singleton $\{c\}$, cela revient à demander que c soit K-rationnel.

7.2.4. **Comparaison entre le cas marqué et le cas non-marqué**

Soit m une composante de $\mathcal{H}^*(G,n)_{\overline{\mathbb{Q}}}$, et $\widetilde{m}$ la composante de $\mathcal{H}(G,n)_{\overline{\mathbb{Q}}}$ obtenue en oubliant les points marqués des G-revêtements dans m. La composante m est définie sur K lorsque $\sigma.m = m$ pour tout $\sigma \in \Gamma_K$. Demander à ce que $\widetilde{m}$ soit définie sur K est, en général, une propriété plus faible : cela revient à dire que pour chaque $\sigma \in \Gamma_K$ il existe un élément $\gamma \in G$ tel que $\sigma.m = m^\gamma$.

Distinguons deux situations :

— Si $\langle m \rangle = G$ (c'est-à-dire que les G-revêtements appartenant à m sont connexes), alors nous avons l'égalité $m^\gamma = m$ pour tout élément $\gamma \in G$, d'après la proposition 3.3.11 (v). Dans cette situation, la composante m est donc définie sur

K si et seulement $\widetilde{m}$ est définie sur K : il n'y a pas de différence entre les deux propriétés.

— Si $\langle m \rangle$ est un sous-groupe strict H de G, on définit la composante m_H de $\mathcal{H}^*(H,n)_{\overline{\mathbb{Q}}}$ obtenue en enlevant à chaque G-revêtement contenu dans m toutes les composantes connexes excepté celle du point marqué : ainsi, les G-revêtements marqués de groupe de monodromie H deviennent des H-revêtements connexes marqués (voir la proposition 2.2.23). On introduit enfin la composante $\widetilde{m}_H$ de $\mathcal{H}(H,n)_{\overline{\mathbb{Q}}}$, obtenue en oubliant les points marqués des H-revêtements connexes contenus dans la composante m_H.

Par le point précédent, les corps de définition des composantes m_H et $\widetilde{m}_H$ sont identiques. Par ailleurs, la définition de l'action de Galois $\sigma.m$ ne dépendant aucunement du groupe ambient, il apparaît aussi que m est définie sur K et et seulement si m_H est définie sur K. En revanche, $\widetilde{m}$ peut parfaitement être définie sur K sans que m ne le soit (voir l'exemple 7.2.12). Nous résumons la situations par le dessin ci-dessus :

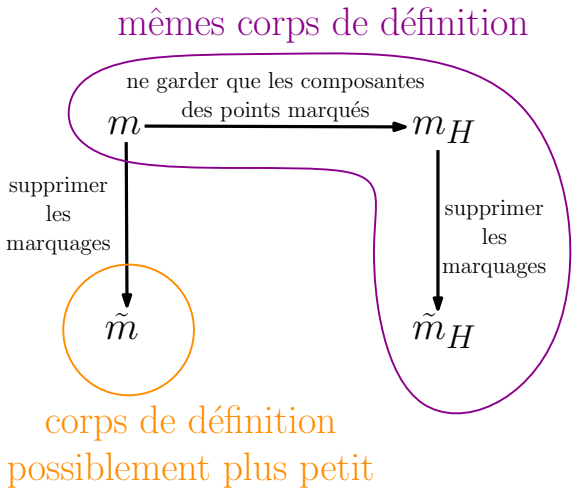


Figure 7.2.10. Un résumé de la situation

Cette discussion entraîne qu'il est équivalent de regarder les corps de définition des composantes de G-revêtements marqués ayant H pour groupe de monodromie ou de regarder les corps de définition des composantes de H-revêtements connexes non-marqués. Dans [Cau12], l'auteur choisit le second point de vue. Nous choisissons la première approche car elle permet un traitement unique des composantes tout en donnant lieu à une structure algébrique plus simple (le monoïde des composantes).

Il y a des situations où on peut relier les corps de définition de $\widetilde{m}$ et de m. Le lemme suivant en donne un exemple :

Lemme 7.2.11. *Supposons que la composante $\widetilde{m}$ soit définie sur K. Chacune des deux hypothèses suivantes entraîne que m est elle-aussi définie sur K :*

- *Le groupe H est son propre normalisateur dans G.*
- *Tous les automorphismes de H sont intérieurs.*

Démonstration. Soit σ un élément de Γ_K. L'égalité $\sigma.m = m^\gamma$ entraîne $H = H^\gamma$. Ainsi, la conjugaison par l'élément $\gamma \in G$ définit un automorphisme de H.

– Si H est son propre normalisateur, alors on doit avoir $\gamma \in H$.
– Si tout automorphisme de H est intérieur, alors il existe un $\gamma' \in H$ tel que $h^\gamma = h^{\gamma'}$ pour tout $h \in H$. En particulier, $\sigma.m = m^\gamma = m^{\gamma'}$.

Dans les deux cas, on déduit de la proposition 3.3.11 (v) que $\sigma.m = m$. La composante m est alors définie sur K. □

Enfin, nous donnons un exemple de situation où le corps de définition de $\widetilde{m}$ est strictement plus petit que celui de m :

Exemple 7.2.12. Soit $G = \mathfrak{S}_n$ avec $n \geq 3$. On a un morphisme injectif ρ de $\mathbb{Z}/n\mathbb{Z}$ dans G donné par :

$$\rho(k)(l) = (k + l \mod n).$$

On note H l'image de ρ, qui est un sous-groupe de G isomorphe à $\mathbb{Z}/n\mathbb{Z}$. La décomposition en cycles de $\rho(k)$ ne dépend que de l'ordre de k dans $\mathbb{Z}/n\mathbb{Z}$: il y a $n/\mathrm{ord}(k)$ cycles, chacun de taille $\mathrm{ord}(k)$. Ainsi, tous les éléments de même ordre dans $\mathbb{Z}/n\mathbb{Z}$ ont leur image par ρ conjuguée dans G.

Maintenant, l'image par un automorphisme $\sigma \in \Gamma_{\mathbb{Q}}$ de la composante m de l'espace de Hurwitz $\mathcal{H}^*(\mathfrak{S}_n, n)_{\overline{\mathbb{Q}}}$ qui est représentée par le n-uplet $\underline{g} = (\underbrace{\rho(1), \rho(1), \ldots, \rho(1)}_{n})$ est, par le lemme des cycles de branchement, représentée par le n-uplet $\sigma.\underline{g}$ formé de n copies de $\rho\big(\chi(\sigma) \mod n\big)$. En particulier, cette composante de $\mathfrak{S}_n$-revêtements marqués n'est pas définie sur $\mathbb{Q}$. Cependant, puisque $(\chi(\sigma) \mod n)$ est d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$, les deux uplets $\underline{g}$ et $\sigma.\underline{g}$ sont conjugués par un élément de $\mathfrak{S}_n$, et cela pour tout $\sigma \in \Gamma_{\mathbb{Q}}$: la composante correspondante $\widetilde{m}$ de $\mathfrak{S}_n$-revêtements non-marqués est définie sur $\mathbb{Q}$.

7.3. Summary of the chapter in English

In this section, we summarize some of the content of Chapter 7 in English. The focus is on stating only key definitions and results which are used in Chapter 8.

We fix a finite group G and a number field K seen as embedded in $\overline{\mathbb{Q}}$. We let $\Gamma_K = \mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$.

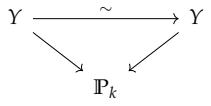
7.3.1. **Algebraic covers**

In this chapter, we focus on branched generically étale G-covers of the projective line.

Let $n \in \mathbb{N}$. The *configuration scheme* Conf_n is the open $\mathbb{Q}$-subvariety of $\mathbb{A}^n_{\mathbb{Q}}$ obtained by removing the zero locus of the discriminant (Definition 7.1.2). Its $\mathbb{C}$-points, equipped with the analytic topology, form a space $\mathrm{Conf}_n(\mathbb{C})$ homeomorphic to the space $\mathrm{Conf}_{n,\mathbb{P}^1(\mathbb{C})}$ from Definition 2.3.8: the configuration scheme is the scheme counterpart of the configuration space. The set of its K-points $\mathrm{Conf}_n(K)$ is the set of configurations $\underline{t} \in \mathrm{Conf}_{n,\mathbb{P}^1(\mathbb{C})}$ consisting of points whose coordinates belong to $\overline{\mathbb{Q}}$, and such that the points are globally preserved by the Galois action of $\mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$; we say that such configurations are *defined over* K.

Let k be a field of characteristic not dividing $|G|$. In this work, a *k-G-cover* is a finite, flat, generically étale morphism from a smooth projective curve Y over k to the projective line $\mathbb{P}^1_k$, unramified above the point at infinity, and equipped with a morphism from G to the automorphism group[7] $\mathrm{Aut}_{\mathbb{P}^1_k}(Y)$ which induces a free

[7] i.e. the group of automorphisms of Y which commute with the map to $\mathbb{P}^1_k$:



transitive action of G on all unramified fibers of $Y \to k$ (Definitions 7.1.4 and 7.1.5). A *k-G-cover equipped with a marked k-point* is moreover equipped with a k-point in the unramified fiber above the point at infinity (Definition 7.1.6).

7.3.2. Fields of definition of G-covers and the inverse Galois problem

The equivalence between curves and their function fields defines an equivalence of categories between irreducible k-G-covers and Galois field extensions of $k(T)$ with Galois group G (Proposition 7.1.7). In particular, when k is a number field, the existence of an irreducible k-G-cover implies the existence of a Galois extension of k with Galois group G, and therefore a positive answer to the inverse Galois problem for G over k (Corollary 7.1.8 and Corollary 7.1.11). This is a consequence of *Hilbert's irreducibility theorem*, which we recall under the following form:

Theorem 7.1.10 (translated). *Let L be a number field, L' be a finite extension of L, and $p : X \to Y$ be a finite étale morphism from an L-variety X to an nonempty open subvariety Y of $\mathbb{A}^n_L$. We assume that the extension of scalars $X_{L'}$ of X to L' is irreducible. Then, there exists an L-point $t \in Y(L)$ such that the action of $\mathrm{Gal}(\overline{\mathbb{Q}} \mid L')$ on the set of $\overline{\mathbb{Q}}$-points of X which are mapped to t by p is transitive.*

Theorem 7.1.10 (translated)

Riemann's existence theorem (Subsection 7.1.4) implies that $\mathbb{C}$-G-covers and topological branched G-covers of $\mathbb{P}^1(\mathbb{C})$ form equivalent categories: when k is an algebraically closed field of characteristic zero, the study of k-G-covers reduces to topology. Using this correspondance, a positive answer to the inverse Galois problem over $\mathbb{C}(T)$ or $\overline{\mathbb{Q}}(T)$ follows from Corollary 2.4.17. Riemann's existence theorem is behind the following isomorphism, for any $\underline{t} \in \mathrm{Conf}_n(\overline{\mathbb{Q}})$:

$$\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \underline{t}, \infty) \simeq \widehat{\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \underline{t}, \infty)}$$

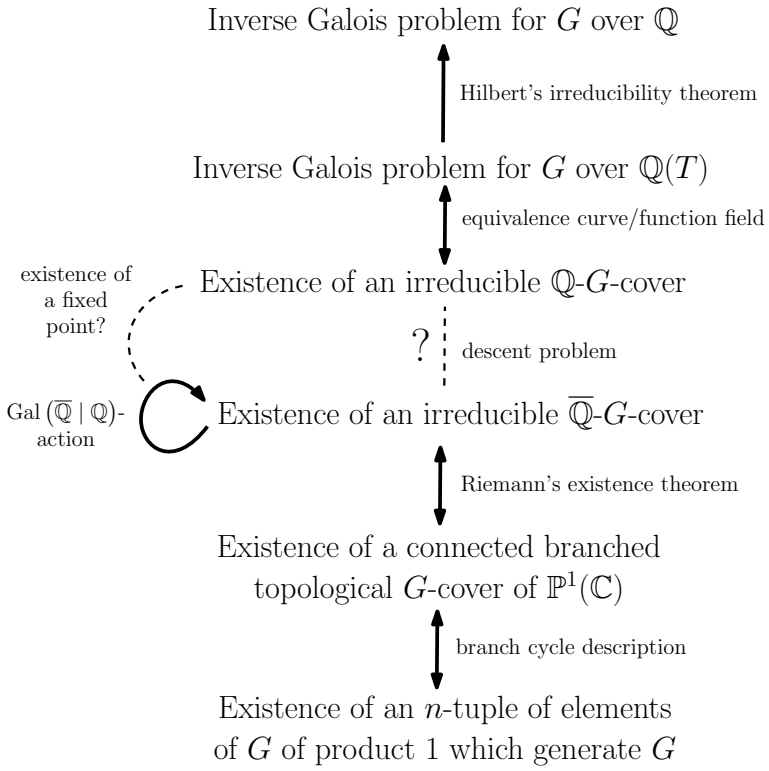
which implies that isomorphism classes of topological marked G-covers of $\mathbb{P}^1(\mathbb{C})$ branched at $\underline{t} \in \mathrm{Conf}_n(\overline{\mathbb{Q}})$ are in one-to-one correspondance with group morphisms from $\pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \underline{t}, \infty)$ to G.

Another approach to K-G-covers is to start with $\overline{\mathbb{Q}}$-G-covers, which are well-understood, and try to determine which of these G-covers come from K-G-covers via extension of scalars: such a G-cover is said to be *defined over K*, and K is then a *field of definition* of the G-cover (Definition 7.1.13). A G-cover is defined over K if and only if the corresponding morphism $\varphi : \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \underline{t}, \infty)$ extends into a morphism $\widetilde{\varphi} : \pi_1^{\text{ét}}(\mathbb{P}^1_K \setminus \underline{t}, \infty)$:

$$\begin{array}{ccc} \pi_1^{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \underline{t}, \infty) & \hookrightarrow & \pi_1^{\text{ét}}(\mathbb{P}^1_K \setminus \underline{t}, \infty) \\ & \searrow^{\varphi} & \downarrow \widetilde{\varphi} \\ & & G \end{array} .$$

A marked G-cover is *defined over K* it is comes from a K-G-cover equipped with a marked K-point via extension of scalars (Definition 7.1.13). There is an action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$ on marked G-covers of $\mathbb{P}^1(\mathbb{C})$ branched at a configuration $\underline{t} \in \mathrm{Conf}_n(K)$ (Subsection 7.1.6); this action preserves the monodromy group. A marked G-cover is defined over K if and only if it is invariant under this action (Proposition 7.1.17).

If one finds a connected G-cover which is defined over $\mathbb{Q}$, then the group G is realizable as a Galois group over $\mathbb{Q}(T)$ and consequently over $\mathbb{Q}$. This suggests the following strategy for realizing a given finite group G as a Galois group over $\mathbb{Q}$:



7.3.3. **Hurwitz schemes**

Hurwitz moduli spaces of G-covers of $\mathbb{P}^1(\mathbb{C})$ branched at n points have counterparts which are $\mathbb{Q}$-schemes:

— We denote by $\mathcal{H}^*(G,n)$ the scheme counterpart of $\mathrm{Hur}^*_{\mathbb{P}^1(\mathbf{C})}(G,n)$.

This $\mathbb{Q}$-scheme is an finite étale cover of Conf_n. The set of its $\mathbb{C}$-points forms a space homeomorphic to $\mathrm{Hur}^*_{\mathbb{P}^1(\mathbf{C})}(G,n)$, and its K-points correspond to marked G-covers defined over K, i.e. to K-G-covers equipped with a marked K-point.

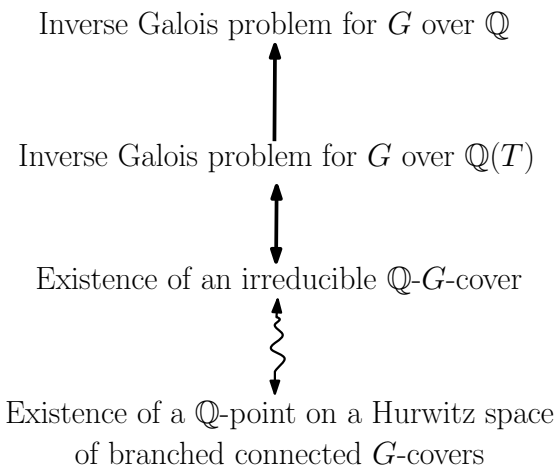
If one finds a $\mathbb{Q}$-point on the subscheme $\mathcal{CH}^*(G,n)$ corresponding to connected marked G-covers, then the group G is realizable as a Galois group over $\mathbb{Q}$.

— We denote by $\mathcal{H}(G,n)$ the scheme counterpart of $\mathrm{Hur}_{\mathbb{P}^1(\mathbf{C})}(G,n)$.

This $\mathbb{Q}$-scheme is an finite étale cover of Conf_n. The set of its $\mathbb{C}$-points forms a space homeomorphic to $\mathrm{Hur}_{\mathbb{P}^1(\mathbf{C})}(G,n)$.

In general, this moduli space is *coarse*. However, if the group G is centerless, then K-points of the subscheme $\mathcal{CH}(G,n)$ corresponding to connected G-covers correspond to G-covers defined over K; in particular, finding a $\mathbb{Q}$-point of this subscheme implies that the group G is realizable as a Galois group over $\mathbb{Q}$.

The properties of these space suggest the following strategy for realizing a finite group G as a Galois group over $\mathbb{Q}$:



Geometrically connected components of $\mathcal{H}^*(G,n)$ are in one-to-one correspondance with connected components of the topological space $\mathrm{Hur}^*_{\mathbb{P}^1(\mathbb{C})}(G,n)$, and consequently with braid group orbits of n-tuples $\underline{g} \in G^n$ whose product $\pi\underline{g} = g_1 \cdots g_n$ is equal to 1. We freely identify geometrically connected components of $\mathcal{H}^*(G,n)$ and elements of degree n in the monoid of components $\mathrm{Comp}(G)$. We obtain analogous descriptions for geometrically connected components of $\mathcal{CH}^*(G,n)$, $\mathcal{H}^*(G,n)$ and $\mathcal{H}(G,n)$; cf. Subsection 3.3.2.

The Galois action of $\Gamma_K = \mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$ on marked G-covers induces an action on geometrically connected components of $\mathcal{H}^*(G,n)$, i.e. on the graded set $\mathrm{Comp}(G)$ (not on the monoid!). We say that a geometrically connected component $x \in \mathrm{Comp}(G)$ is *defined over K* if it is invariant under this action, or equivalently if it comes from a connected component of the Hurwitz space $\mathcal{H}^*(G,n)_K$ over K via extension of scalars. (Definition 7.2.2)

7.3.4. **The branch cycle lemma**

The Galois action on multidiscriminants (Definitions 1.4.6 and 2.3.29) of components is described by the *branch cycle lemma*.

Let H be a subgroup of G and c be a subset of H which is conjugation-invariant and K-rational (Definition 1.4.2). We let D^* be the set of conjugacy classes of H contained in c and, for each $\sigma \in \Gamma_K$, we denote by p_σ the map $D^* \to D^*$ defined by the $\chi(\sigma)$-th power of conjugacy classes.

Let $x \in \mathrm{Comp}(H,c)$. Recall that the (H,c)-multidiscriminant $\mu_{H,c}(x)$ of x is the map $D^* \to \mathbb{Z}$ which maps a class $\gamma \in D^*$ to the number of its elements of γ in a tuple representing x (Definitions 1.4.6 and 2.3.29). We say that *x has a K-rational multidiscriminant* if $\mu_{H,c}(x) = \mu_{H,c}(x) \circ p_\sigma$ for all $\sigma \in \Gamma_K$ (Definition 7.2.5).

The branch cycle lemma is the following result, which gives an easily checked necessary condition for a component to be defined over K:

Corollary 7.2.6 (translated). **Corollary 7.2.6 (translated)**

(i) For all $\sigma \in \Gamma_K$, we have $\mu_{H,c}(\sigma.x) = \mu_{H,c}(x) \circ p_\sigma$.

(ii) If the component x is defined over K, then it has a K-rational (H,c)-multidiscriminant.

(iii) If H is abelian and the component x has a K-rational (H,c)-multidiscriminant, then x is defined over K.

As an application of Corollary 7.2.6 (iii), the component $(1,-1) \in \mathrm{Comp}(\mathbb{Z}/n\mathbb{Z})$ is defined over $\mathbb{Q}$ if $n \in \{2,3,4,6\}$ and is not defined over $\mathbb{Q}$ if $n = 5$ or $n \geq 7$ (Example 7.2.7).

Chapitre 8

Fields of Definition of Components of Hurwitz Spaces

Summary of the chapter

In this chapter, we study the fields of definition of geometrically connected components of Hurwitz moduli schemes of branched G-covers of the projective line, where G is a fixed finite group. The main focus is on determining whether components obtained by "gluing" two components, both defined over a number field K, are also defined over K. We present a list of situations in which a positive answer is obtained (Theorem 8.1.2).

As an application, when G is a semi-direct product of symmetric groups or the Mathieu group M_{23}, components defined over $\mathbb{Q}$ of small dimension (6 and 4, respectively) are shown to exist (Examples 8.2.6 and 8.4.6).

The content of this chapter is largely taken from the preprint [Seg23].

Outline of the chapter

> Consider a difficult problem A. Rather than solve it as such, consider a more general and more difficult problem B. Next, weaken the requirements in the problem B and try to solve the problem C obtained in such a way. We shall call this activity an *approach to the problem* A, even though "the intersection" of A and C is empty.
>
> — V. V. Ishkanov, B. B. Lure, D. K. Faddeev, *The Embedding Problem in Galois Theory*, 1997.

8.1. Introduction and main results

8.1.1. Introduction

Let G be a finite group and K be a field of characteristic zero. Hurwitz schemes are moduli spaces of branched G-covers of $\mathbb{P}^1$. Their K-points are significant for number theory since they are tightly related to the inverse Galois problem for G over $K(t)$; see [Fri77; FV91; RW06][1].

[1] see also Subsection 7.1.3

When K is algebraically closed, Riemann's existence theorem implies that the theory reduces to topology. Specifically, $\mathbb{C}$-points of Hurwitz schemes correspond to isomorphism classes of topological G-covers of punctured Riemann spheres[2]. A classical topological construction lets one "glue" two marked covers – one with r_1 branch points and one with r_2 branch points – into a single marked cover with $r_1 + r_2$ branch points[3]. This gluing operation plays a central role in [EVW16].

[2] cf. Subsection 7.1.4

[3] cf. Subsection 2.4.2

When K is a complete valued field, Harbater defined an analogous *patching* operation to construct covers defined over K with a specified monodromy group by patching together covers with smaller monodromy groups; see [Har03; HV96; Liu95]. This construction leads to a positive answer to the inverse Galois problem over $K(T)$.

For number theorists, the most interesting case is that of number fields. However, no gluing or patching operation is known in this case, although it would be a game-changing tool for inverse Galois theory. In this chapter, we focus not on G-covers themselves but on geometrically connected components of Hurwitz schemes, and we study the possibility of gluing these components over a number field.

Identifying components defined over $\mathbb{Q}$ is a crucial first step in finding rational points on these schemes. The question of the fields of definition of these components is a well-studied topic; see [Cau12; DE06; EVW12; FV91][4].

[4] see also Subsection 7.2.2

8.1.2. **Main results**

Assume K is a number field. The gluing operation over $\overline{K}$ induces a monoid structure[5] on the set $\mathrm{Comp}(G)$ of geometrically connected components of Hurwitz moduli schemes of marked branched G-covers of $\mathbb{P}^1$. To understand the arithmetic properties of the topological gluing operation, a prominent question is the following:

[5] $\mathrm{Comp}(G)$ is the monoid of components $\mathrm{Comp}_{\mathbb{P}^1(\mathbb{C})}(G)$ in the notation of Section 3.4. We systematically omit "$\mathbb{P}^1(\mathbb{C})$".

Question 8.1.1. Let $x, y \in \mathrm{Comp}(G)$ be components defined over K. Is the component xy, obtained by gluing x and y, defined over K?

Question:
Is gluing of components possible over number fields?

Question 8.1.1 and related problems are the main focus of this chapter. Our main result is that the answer is positive in situations (i), (ii) and (iii) below:

Theorem 8.1.2. *Let $x, y \in \mathrm{Comp}(G)$ be components defined over K. Denote by H_1 and H_2 the monodromy groups of the marked G-covers contained in x and y respectively, and let $H = \langle H_1, H_2 \rangle$. Then:*

Theorem:
Positive answers to Question 8.1.1 in various situations

(i) If $H_1 H_2 = H$, then the glued component xy is defined over K.

(ii) If every conjugacy class of H that is a local monodromy class of the covers in the component xy occurs at at least M branch points (for some constant M which depends only on the group G), then xy is defined over K.

(iii) There are elements $\gamma, \gamma' \in H$ satisfying $\left\langle H_1^{\gamma}, H_2^{\gamma'} \right\rangle = H$ such that the component $x^{\gamma} y^{\gamma'}$, obtained by letting γ, γ' act on x, y and by gluing the resulting components, is defined over K.

The three parts of Theorem 8.1.2 are proved in three corresponding sections:

— Theorem 8.1.2 (i) (which is Theorem 8.2.3 (iii)) is proved using techniques introduced by [Cau12] and lemmas about the braid group action on tuples. In Section 8.2, we present this result, including a generalized version, and propose applications. Cases of interest include the situation where H_1 or H_2 is normal in H, notably if one is included in the other. An application is given in Example 8.2.6: if G is a semi-direct product of symmetric groups, there is a component defined over $\mathbb{Q}$ of connected G-covers with six branch points. This improves on a similar example of Cau where twelve branch points were used. Another consequence of our ideas is presented in Subsection 8.2.4: we show that the Galois action on components is entirely determined by the Galois action on components with few branch points; precise statements are given in Propositions 8.2.8 and 8.2.9.

— Theorem 8.1.2 (ii) (which is Theorem 8.3.1 (iii)) is proved using the *lifting invariant* presented in [EVW12; Woo21][6]. In Section 8.3, we use this invariant to determine the fields of definition of glued components.

[6] see also Subsection 3.4.7

— Theorem 8.1.2 (iii) (which is Theorem 8.4.5) is based on *patching results* over complete valued fields. We follow the algebraic patching approach from [HV96]. By patching covers over infinitely many complete valued fields, we obtain a result in the number field case. Section 8.4 is concerned with the proof of this theorem. An application is given in Example 8.4.6: when G is the Mathieu group M_{23}, there is a component defined over $\mathbb{Q}$ of connected G-covers with only four branch points.

We do not know if the answer to Question 8.1.1 is always positive. Finding counterexamples is difficult because there are few tools available to prove that components

are not defined over Q. For instance, the lifting invariant cannot be used to find a counterexample, as established by Theorem 8.3.4. Indeed, the lifting invariant of a product of components defined over K is preserved by the Galois action: from the point of view of this invariant, products of components defined over K are indistinguishable from components defined over K.

Remark 8.1.3. We include non-connected G-covers, i.e. covers whose monodromy groups are proper subgroups of G, because we are interested in patching-like results. Typically, we want to construct components with monodromy group G by gluing components with smaller monodromy groups. If we do not take this phenomenon into account, the answer to Question 8.1.1 is "yes": the concatenation of two components defined over K of connected G-covers is always defined over K. This follows from Theorem 8.1.2 (i). In [Cau12], a different but equivalent choice is made: instead of considering components of marked non-connected G-covers, Cau considers components of unmarked connected H-covers where H is a subgroup of G. The links between these two approaches are discussed in Subsection 7.2.4.

8.1.3. **Notation**

We fix some notation and terminology. The content of this subsection partly overlaps Section 1.4.

We fix a finite group G and a number field K. Number fields are always equipped with an embedding into $\overline{\mathbb{Q}}$. We denote by Γ_K the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}} \mid K)$. The cyclotomic character of K is denoted by $\chi : \Gamma_K \to \widehat{\mathbb{Z}}^\times$.

Let $\underline{g} = (g_1, \dots, g_n)$ be a tuple of elements of G. Then:

— Its *size* $\deg(\underline{g})$ is the number n of elements in the tuple.

— Its *group* $\left\langle \underline{g} \right\rangle$ is the subgroup of G generated by $g_1, \dots, g_n$.

— The *product* of $\underline{g}$ is $\pi\underline{g} = g_1 g_2 \cdots g_n \in G$.

— Let H be a subgroup of G containing $\left\langle \underline{g} \right\rangle$. A conjugacy class γ of H *appears in* $\underline{g}$ if there is some i for which $g_i \in \gamma$. The set of the conjugacy classes of H which appear in $\underline{g}$ is denoted by $D_H(\underline{g})$.

— Let H be a subgroup of G which contains $\left\langle \underline{g} \right\rangle$ and c be a conjugation-invariant subset of H which contains $g_1, \dots, g_n$. If γ is a conjugacy class of H contained in c, we denote by $\mu_{H,c}(\underline{g})(\gamma)$ the count of its appearances in $\underline{g}$, i.e.:

$$\mu_{H,c}(\underline{g})(\gamma) = \left| \left\{ i \in \{1, \dots, n\} \;\middle|\; g_i \in \gamma \right\} \right|.$$

This defines an integer-valued map $\mu_{H,c}(\underline{g})$ on the set D^* of all conjugacy classes of H contained in c. We call this map the (H,c)-*multidiscriminant of* $\underline{g}$.

All these objects and properties are preserved by the braid group action on tuples (Proposition 3.3.8). Therefore, we extend these notations when the tuple $\underline{g}$ is replaced by a braid group orbit of a tuple, i.e. an element $x \in \mathrm{Comp}(G)$.

8.2. The group-theoretic approach

In this section, we propose new applications of ideas introduced in [Cau12], which we recall in Subsection 8.2.1. In Subsection 8.2.2, we prove the main result Theorem 8.2.3 (iii), which corresponds to Theorem 8.1.2 (i): this result gives a sufficient group-theoretic condition for the product of two components defined over K to be defined over K. This theorem is generalized in Subsection 8.2.5 and examples are given in Subsection 8.2.3. In Subsection 8.2.4, we use similar methods to reduce the Galois action to components of small size, cf. Propositions 8.2.8 and 8.2.9. Our approach is based on braid manipulations and group-theoretic criteria.

8.2.1. **Cau's theorem**

Following [Cau12], if $x_1, \dots, x_n \in \mathrm{Comp}(G)$ and H is a subgroup of G which contains $\langle x_1, \dots, x_n \rangle$, we define the following subset of $\mathrm{Comp}(G)$:

$$\mathrm{ni}_H(x_1, \dots, x_n) = \left\{ \prod_{i=1}^{n} x_i^{\gamma_i} \;\middle|\; \gamma_i \in H \right\}.$$

We also introduce the following subset, which always contains $x_1 \cdots x_n$:

$$\mathrm{ni}_H^\natural(x_1, \dots, x_n) = \left\{ \prod_{i=1}^{n} x_i^{\gamma_i} \;\middle|\; \begin{array}{c} \gamma_i \in H \\ \langle x_1^{\gamma_1} \cdots x_n^{\gamma_n} \rangle = \langle x_1 \cdots x_n \rangle \end{array} \right\}.$$

When H is not specified, it is assumed that $H = \langle x_1 \cdots x_n \rangle$.

In Cau's terminology, a family of elements of $\mathrm{Comp}(G)$ corresponds to a *degenerescence structure* Δ, and elements of $\mathrm{ni}_H(\Delta)$ are called Δ-*components*. Cau gave a criterion to identify whether a given component is a Δ-component depending on the existence of a specific "Δ-admissible cover" on its boundary. This characterization is key for his proof of the following theorem, which is [Cau12, Théorème 3.2]:

Theorem 8.2.1. *Let $x_1, \dots, x_n$ be components, H a subgroup of G which contains $\langle x_1, \dots, x_n \rangle$, and $\sigma \in \Gamma_K$. The action of σ on components induces a bijection:*

$$\mathrm{ni}_H(x_1, \dots, x_n) \to \mathrm{ni}_H(\sigma.x_1, \dots, \sigma.x_n)$$

and the same statement holds if ni_H is replaced by $\mathrm{ni}_H^\natural$.

That Theorem 8.2.1 holds if ni_H is replaced with $\mathrm{ni}_H^\natural$ follows from the fact that the Galois action preserves the monodromy group. If X is a finite set of components and $\sigma \in \Gamma_K$, we write Theorem 8.2.1 under the form $\sigma.\mathrm{ni}(X) = \mathrm{ni}(\sigma.X)$, where $\sigma.X$ is a shorthand for $\{\sigma.x \mid x \in X\}$.

8.2.2. **Permuting components**

In [Cau12, Proposition 2.10] and [Cau16, Théorème 3.8], Cau applies Theorem 8.2.1 in situations where he shows $\mathrm{ni}(x_1, \dots, x_n) = \{x_1 \cdots x_n\}$. We introduce a different condition that is later shown to imply $\mathrm{ni}^\natural(x_1, \dots, x_n) = \{x_1 \cdots x_n\}$ (Theorem 8.2.3 (i)):

Definition 8.2.2. Two components $x, y \in \mathrm{Comp}(G)$ of respective monodromy groups $H_1 = \langle x \rangle$ and $H_2 = \langle y \rangle$ are *permuting* if $H_1 H_2 = \langle H_1, H_2 \rangle$.

This terminology comes from the fact that subgroups H_1, H_2 of a group G are classically called *permuting* when H_1H_2 is a subgroup of G. Two elements of $\mathrm{Comp}(G)$ are permuting exactly when their monodromy groups are permuting subgroups of G. This condition is neither stronger nor weaker than the completeness conditions considered by Cau. In Subsection 8.2.5, we give a condition that generalizes both Definition 8.2.2 and the hypothesis of [Cau12, Proposition 2.10].

Note that $x, y \in \mathrm{Comp}(G)$ are permuting whenever $\langle x \rangle$ or $\langle y \rangle$ is normal in $\langle x, y \rangle$, and in particular when one monodromy group contains the other. Cases of interest are $\langle x \rangle = \langle y \rangle$ as well as $\langle x \rangle = G$ or $\langle y \rangle = G$. Moreover, if x, y are permuting and $\sigma \in \Gamma_K$, then $\sigma.x$ and $\sigma.y$ are permuting.

We now prove Theorem 8.2.3, whose third point is Theorem 8.1.2 (i):

Theorem 8.2.3. *Let $x, y \in \mathrm{Comp}(G)$ be permuting components. Then:*

(i) $\mathrm{ni}^\natural(x, y) = \{xy\}$.

(ii) For all $\sigma \in \Gamma_K$ we have $\sigma.(xy) = (\sigma.x)(\sigma.y)$.

(iii) If x and y are defined over K, then xy is defined over K.

Proof. (i) Let $\gamma, \gamma' \in H$ such that $\left\langle x^\gamma y^{\gamma'} \right\rangle = H$. We show $x^\gamma y^{\gamma'} = xy$. We use Proposition 3.3.11 (v) to reduce to the case $\gamma = 1$: indeed, we have $x^\gamma y^{\gamma'} = xy^{\gamma^{-1}\gamma'}$ since $\gamma^{-1} \in \left\langle x^\gamma y^{\gamma'} \right\rangle = H$. Write $\gamma' = \gamma_1\gamma_2$ with $\gamma_i \in H_i$. We have:

$$\begin{aligned} xy &= xy^{\gamma_2} && \text{by Proposition 3.3.11 (v), because } \gamma_2 \in \langle y \rangle \\ &= x(y^{\gamma_2})^{\gamma_1} && \text{by Proposition 3.3.11 (v), because } \gamma_1 \in \langle x \rangle \\ &= xy^{\gamma_1\gamma_2} \\ &= xy^{\gamma'}. \end{aligned}$$

(ii) Let $\sigma \in \Gamma_K$. By Theorem 8.2.1, the component $\sigma.(xy)$ belongs to the set $\mathrm{ni}^\natural(\sigma.x, \sigma.y)$ and thus it is equal to $(\sigma.x)(\sigma.y)$, by point (i) applied to the permuting components $\sigma.x$ and $\sigma.y$.

(iii) Follows from point (ii).

□

A noteworthy corollary of Theorem 8.2.3 (iii) is the following:

Corollary 8.2.4. *If x is a component defined over K, then so is x^n for all $n \geq 0$.*

Remark 8.2.5. To deduce Theorem 8.2.3 (iii) from Theorem 8.2.3 (i), one can use Theorem 8.4.5 instead of Theorem 8.2.1.

8.2.3. **Applications and examples**

In this subsection, we give two applications of Theorem 8.2.3: these are Example 8.2.6, which improves the minimal number of branch points needed to find components defined over $\mathbb{Q}$ in the case of semi-direct products of symmetric groups, and Corollary 8.2.7, which implies the existence of an operation similar to the field norm for components of Hurwitz spaces : by gluing a component with all its Galois conjugates, one obtains a component defined over K with the same monodromy group, but with a larger degree.

Example 8.2.6. Theorem 8.2.3 implies a slightly stronger version of [Cau12, Théorème 3.5]. Indeed, let $G = H_1 \ltimes H_2$ be a semi-direct product of groups. Assume that for $i = 1, 2$ there is a *rigid* (cf. [Cau12, Definition 2.4]) r_i-tuple $\underline{c_i}$ of $\mathbb{Q}$-rational conjugacy classes of H_i. Then for $i = 1, 2$ there is a unique component $m_i \in \mathrm{Comp}(G)$ such that $\langle m_i \rangle = H_i$ and the (H_i, H_i)-multidiscriminant of m_i counts the appearances of a class in $\underline{c_i}$. By the rigidity hypothesis and the branch cycle lemma (Corollary 7.2.6), these components are defined over $\mathbb{Q}$. Cau's results led him to observe that (H_1, H_1, H_2, H_2) is a complete family of subgroups of G and therefore $m_1^2 m_2^2$ is defined over $\mathbb{Q}$. We obtain a slightly better result: since G is a semi-direct product of H_1 and H_2, the components m_1, m_2 are permuting and therefore the component $m_1 m_2$ is defined over K.

Assume G is a semi-direct product of symmetric groups: $G = \mathfrak{S}_n \ltimes \mathfrak{S}_m$. There are rigid $\mathbb{Q}$-rational triples of conjugacy classes of $\mathfrak{S}_n$ and $\mathfrak{S}_m$. The reasoning above shows that there is a component defined over $\mathbb{Q}$ of G-covers with six branch points, improving upon the twelve used by Cau and the thirty-two used by Dèbes and Emsalem.

We now prove Corollary 8.2.7, which can be perceived as the existence of a field norm for components. This result is a variant of [Cau12, Corollaire 1.1/Corollaire 3.4]: Cau shows that the concatenation of all components with a given size is defined over $\mathbb{Q}$; here we are more precise by restricting our attention on a single Galois orbit, leading to a smaller size for the product component.

Corollary 8.2.7. *Let $x \in \mathrm{Comp}(G)$ be a component, and $H = \langle x \rangle$. Let Γ_x be the subgroup of finite index of Γ_K consisting of elements $\sigma \in \Gamma_K$ such that $\sigma.x = x$. The following component, whose monodromy group is H, is defined over K:*

$$\mathrm{N}_K(x) = \prod_{\sigma \in \Gamma_K / \Gamma_x} \sigma.x.$$

Proof. Let $\Gamma_K.x$ be the set $\{\sigma.x \,|\, \sigma \in \Gamma_K/\Gamma_x\}$. Since all components of the form $\sigma.x$ have group H, repeated applications of Theorem 8.2.3 (i) show that:

$$\mathrm{ni}_H^\natural(\Gamma_K.x) = \{\mathrm{N}_K(x)\}. \tag{8.2.1}$$

Consider an automorphism $\sigma \in \Gamma_K$. The action of σ permutes $\Gamma_K.x$. Finally:

$$\begin{aligned}
\{\mathrm{N}_K(x)\} &= \mathrm{ni}_H^\natural(\Gamma_K.x) && \text{by Equation (8.2.1)} \\
&= \mathrm{ni}_H^\natural(\sigma.(\Gamma_K.x)) && \text{because } \sigma \text{ permutes } \Gamma_K.x \\
&= \sigma.\mathrm{ni}_H^\natural(\Gamma_K.x) && \text{by Theorem 8.2.1} \\
&= \sigma.\{\mathrm{N}_K(x)\} && \text{by Equation (8.2.1)} \\
&= \{\sigma.\mathrm{N}_K(x)\}
\end{aligned}$$

and thus $N_K(x)$ is defined over K. □

8.2.4. **Reduction of the Galois action to components of small size**

In this subsection we express the Galois action of Γ_K on components in terms of the action on components of small size (Proposition 8.2.8). Let $\psi(G)$ be the sum of the orders of the elements of G:

$$\psi(G) \stackrel{\mathrm{def}}{=} \sum_{g \in G} \mathrm{ord}(g).$$

Consider a n-tuple $\underline{g} = (g_1, \dots, g_n) \in G^n$, and let $H = \left\langle \underline{g} \right\rangle$. If $n > \psi(G)$, then there is an element $g \in G$ which appears at least $\mathrm{ord}(g) + 1$ times in the tuple $\underline{g}$. Usual braid manipulations allow one to move these occurrences of g to the beginning of the tuple. This shows that we have the following equality in $\mathrm{Comp}(G)$:

$$\underline{g} = (\underbrace{g, \dots, g}_{\mathrm{ord}(g)})y$$

for some $y \in \mathrm{Comp}(G)$ of group H. Note that $(g, \dots, g)$ and y are permuting components and that $\langle (g, \dots, g) \rangle = \langle g \rangle$ is abelian. We have:

$$\begin{aligned} \sigma.\underline{g} &= (\sigma.(g, \dots, g))\,(\sigma.y) && \text{by Theorem 8.2.3 (ii)} \\ &= \left(g^{\chi(\sigma^{-1})}, \dots, g^{\chi(\sigma^{-1})}\right)(\sigma.y) && \text{by the branch cycle lemma (Corollary 7.2.6 (i)).} \end{aligned}$$

We can iterate this factorization process until the size of y is smaller than $\psi(G)$: this shows that the Galois action on components is entirely determined by the cyclotomic character and the Galois action on components of small size. We turn this into a precise proposition:

Proposition 8.2.8. *Let $x \in \mathrm{Comp}(G)$ be a component and $H = \langle x \rangle$. There are elements $g_1, \dots, g_r \in H$ and a component $y \in \mathrm{Comp}(G)$ of group H with $\deg(y) \leq \psi(G)$ such that:*

$$x = \left(\prod_{i=1}^{r} (\underbrace{g_i, \dots, g_i}_{\mathrm{ord}(g_i)}) \right) y.$$

Moreover, once x is expressed under this form, the Galois action of an automorphism $\sigma \in \Gamma_K$ on x can be expressed in terms of the cyclotomic character χ and of the Galois action on components of size $\leq \psi(G)$:

$$\sigma.x = \left(\prod_{i=1}^{r} \left(\underbrace{g_i^{\chi(\sigma^{-1})}, \dots, g_i^{\chi(\sigma^{-1})}}_{\mathrm{ord}(g_i)} \right) \right) (\sigma.y).$$

Here is another example of this phenomenon. Let H be a subgroup of G and c a K-rational conjugation-invariant subset of H. Denote by $\mathcal{C}_{H,c}$ the set of components $x \in \mathrm{Comp}(G)$ such that $\langle x \rangle = H$ and all monodromy classes of x are contained in c. Then:

Proposition 8.2.9. *Assume every component $x \in \mathcal{C}_{H,c}$ of size $\leq 2\,|c|\,\psi(G)$ with a K-rational (H, c)-multidiscriminant is defined over K. Then, every component $x \in \mathcal{C}_{H,c}$ with a K-rational (H, c)-multidiscriminant is defined over K.*

Proof. We prove the result by induction. Consider a component $x \in \mathcal{C}_{H,c}$ of size $n > 2\,|c|\,\psi(G)$ with a K-rational (H, c)-multidiscriminant. Assume that every component in $\mathcal{C}_{H,c}$ of size $< n$ with a K-rational (H, c)-multidiscriminant is defined over K. Choose a tuple $\underline{g} \in c^n$ representing x. Since $n > 2\,|c|\,\psi(G)$, there is some $g \in c$ which appears at least $2\mathrm{ord}(g)\,|c| + 1$ times in $\underline{g}$.

Let $g_1, \dots, g_r$ be the elements obtained as $g^{\chi(\sigma)}$ for some $\sigma \in \Gamma_K$. By Corollary 7.2.6 (iii), the following component, whose group is the abelian group $\langle g \rangle$, is defined over K:

$$y \stackrel{\mathrm{def}}{=} (\underbrace{g_1, \dots, g_1}_{\mathrm{ord}(g)}, \underbrace{g_2, \dots, g_2}_{\mathrm{ord}(g)}, \dots, \underbrace{g_r, \dots, g_r}_{\mathrm{ord}(g)}).$$

In particular, the component y has a K-rational (H,c)-multidiscriminant by Corollary 7.2.6 (ii).

We want to show that there is a component z with $\langle z\rangle = H$ such that $x = yz$. For this, we apply the factorization lemma Lemma 4.4.8. Consider a conjugacy class γ of H which appears in y. Then:

— The conjugacy class γ is some $\chi(\sigma)$-th power of the conjugacy class of g, which appears at least $2\mathrm{ord}(g)\,|c|+1$ times in $\underline{g}$ because g itself does. Since x has a K-rational (H,c)-multidiscriminant, we have $\mu_{H,c}(x)(\gamma) \geq 2\mathrm{ord}(g)\,|c|+1$.

— The conjugacy class γ appears at most $\mathrm{ord}(g)\,|c|$ times in y since $\deg(y) \leq \mathrm{ord}(g)\,|c|$.

Finally:

$$\begin{aligned}\mu_{H,c}(x)(\gamma) &\geq 2\mathrm{ord}(g)\,|c|+1\\ &\geq \mathrm{ord}(g)(|\gamma|+|c|)\\ &= \mathrm{ord}(\gamma)\,|\gamma| + \mathrm{ord}(g)\,|c|\\ &\geq \mathrm{ord}(\gamma)\,|\gamma| + \mu_{H,c}(y)(\gamma).\end{aligned}$$

By Lemma 4.4.8, there exists $z \in \mathrm{Comp}(G)$ such that $x = yz$ and $\langle z\rangle = H$, and in particular $z \in \mathcal{C}_{H,c}$. Since $x = yz$ and y both have K-rational (H,c)-multidiscriminants, the component z has a K-rational (H,c)-multidiscriminant too. By the induction hypothesis, z is defined over K. Moreover $\langle y\rangle \subseteq H$ so y and z are permuting, and thus $x = yz$ is defined over K by Theorem 8.2.3 (iii). We conclude by induction. □

Remark 8.2.10. When we have discussed the lifting invariant in Section 8.3, it will appear that the hypothesis "with a K-rational (H,c)-multidiscriminant" in Proposition 8.2.9 can be replaced by the more precise necessary condition "whose (H,c)-lifting invariant is Γ_K-invariant". The proof of Proposition 8.2.9 can be reproduced identically except for the two following details:

— That γ appears at least $2\mathrm{ord}(g)\,|c|+1$ times in $\underline{g}$ follows from the fact that a component with a Γ_K-invariant (H,c)-lifting invariant also has a K-rational (H,c)-multidiscriminant. This follows directly from the definition of the Γ_K-action on lifting invariants in Subsection 8.3.2.

— To apply the induction hypothesis, we have to show that the component z obtained using the factorisation lemma has a Γ_K-invariant lifting invariant. At that point in the proof, we know that $x = yz$, and that x and y both have Γ_K-invariant lifting invariants. First notice that $x = yz$ implies:

$$\Pi_{H,c}(x) = \Pi_{H,c}(y)\Pi_{H,c}(z). \tag{8.2.2}$$

Now, consider an automorphism $\sigma \in \Gamma_K$. Theorem 8.3.4 together with the equality $x = yz$ imply:

$$\sigma.\Pi_{H,c}(x) = (\sigma.\Pi_{H,c}(y))(\sigma.\Pi_{H,c}(z))$$

i.e.:

$$\Pi_{H,c}(x) = \Pi_{H,c}(y)(\sigma.\Pi_{H,c}(z)). \tag{8.2.3}$$

Since the lifting invariant takes values in a group, Equation (8.2.2) and Equation (8.2.3) together imply $\Pi_{H,c}(z) = \sigma.\Pi_{H,c}(z)$. Hence the (H,c)-lifting invariant of z is Γ_K-invariant.

Remark 8.2.11. The constant $2\,|c|\,\psi(G)$ in Proposition 8.2.9 can be improved to:

$$\sum_{\gamma\in D} |\gamma| \left[\mathrm{ord}(\gamma)\Big(\,|\gamma| + \varphi\Big(\mathrm{ord}(\gamma)\Big)\Big) - 1\right]$$

where D is the set of conjugacy classes of H contained in c and φ is Euler's totient function.

Example 8.2.12. In the situation of Example 7.2.8, where G is the symmetric group $\mathfrak{S}_d$ and c is the set of transpositions in G, checking that all components of size $\leq \frac{1}{2}d^4$ are defined over $\mathbb{Q}$ would have been enough to prove that they are all defined over $\mathbb{Q}$.

8.2.5. **Generalized permuting components**

In this subsection, we prove Theorem 8.2.14, which generalizes both Theorem 8.2.3 and [Cau12, Proposition 2.10]. First, we introduce the following definition:

Definition: *Generalized permuting components*

Definition 8.2.13. Let $x_1,\dots,x_n \in \mathrm{Comp}(G)$ be components, let $H_i = \langle x_i\rangle$ and $H = \langle H_1,\dots,H_n\rangle$. The family $(x_1,\dots,x_n)$ is *permuting* when for all elements $\gamma_1,\dots,\gamma_n \in H$ and for all $i \in \{2,\dots,n\}$ we have:

$$\text{if } \left\langle H_1, H_2,\dots,H_{i-1}, H_i, H_{i+1}^{\gamma_{i+1}},\dots,H_n^{\gamma_n}\right\rangle = H,$$
$$\text{then } \left\langle H_1, H_2,\dots,H_{i-1}, H_{i+1}^{\gamma_{i+1}},\dots,H_n^{\gamma_n}\right\rangle H_i = H.$$

We now state and prove Theorem 8.2.14. Note that the case $n = 2$ gives back Theorem 8.2.3, and that the hypothesis of Theorem 8.2.14 is slightly weaker than the one required to apply Theorem 8.2.3 multiple times recursively:

Theorem 8.2.14. *Let $(x_1,\dots,x_n)$ be a permuting family of components. Then:*

(i) $\mathrm{ni}_H^{\natural}(x_1,\dots,x_n) = \{x_1\cdots x_n\}$.

(ii) For all automorphisms $\sigma \in \Gamma_K$, we have $\sigma.(x_1\cdots x_n) = (\sigma.x_1)\cdots(\sigma.x_n)$.

(iii) If $x_1,\dots,x_n$ are defined over K then $x_1\cdots x_n$ is defined over K.

Proof. We focus on proving point (i), from which points (ii) and (iii) follow like in the proof of Theorem 8.2.3. Let $\gamma_1,\dots,\gamma_n \in G$ such that $\langle \prod x_i^{\gamma_i}\rangle = H$. First we can assume $\gamma_1 = 1$ as in the proof of Theorem 8.2.3 (i). We proceed by induction. Assume we have shown:

$$x_1\cdots x_n = x_1x_2\cdots x_{i-1}x_i x_{i+1}^{\gamma_{i+1}}\cdots x_n^{\gamma_n}.$$

In particular, we have $\left\langle H_1, H_2,\dots,H_{i-1}, H_i, H_{i+1}^{\gamma_{i+1}},\dots,H_n^{\gamma_n}\right\rangle = H$. Since $(x_1,\dots,x_n)$ is permuting, we can write $\gamma_i = \gamma_i^{(1)}\gamma_i^{(2)}$ with $\gamma_i^{(1)} \in \left\langle H_1, H_2,\dots,H_{i-1}, H_{i+1}^{\gamma_{i+1}},\dots,H_n^{\gamma_n}\right\rangle$ and $\gamma_i^{(2)} \in H_i$. Therefore:

$$\begin{aligned}
x_1\cdots x_n &= x_1\cdots x_{i-1}x_i^{\gamma_i^{(2)}} x_{i+1}^{\gamma_{i+1}}\cdots x_n^{\gamma_n} && \text{by Proposition 3.3.11 (v), because } \gamma_i^{(2)} \in \langle x_i\rangle\\
&= x_1\cdots x_{i-1}\left(x_i^{\gamma_i^{(2)}}\right)^{\gamma_i^{(1)}} x_{i+1}^{\gamma_{i+1}}\cdots x_n^{\gamma_n} && \text{because } \gamma_i^{(1)} \in \left\langle x_1\cdots x_{i-1}, x_{i+1}^{\gamma_{i+1}}\cdots x_n^{\gamma_n}\right\rangle\\
&= x_1\cdots x_{i-1}x_i^{\gamma_i} x_{i+1}^{\gamma_{i+1}}\cdots x_n^{\gamma_n}
\end{aligned}$$

and we conclude by induction. □

We now give an application of Theorem 8.2.14:

Example 8.2.15. Let c be a K-rational conjugation-invariant set of G. Assume that c is *complete*, i.e. no proper subgroup of G intersects every conjugacy class contained in c (for example, Jordan's lemma implies that $c = G \setminus \{1\}$ is complete).

The following component (introduced in [EVW12, Paragraph 5.5]) is defined over K:

$$V = \prod_{g \in c} (\underbrace{g, \dots, g}_{\mathrm{ord}(g)}).$$

Indeed, consider an automorphism $\sigma \in \Gamma_K$. Since $\langle g \rangle$ is abelian, Corollary 7.2.6 (i) implies that $\sigma.(g, \dots, g) = (g^{\chi(\sigma^{-1})}, \dots, g^{\chi(\sigma^{-1})})$. The profinite integer $\chi(\sigma^{-1})$ is invertible and so the action of σ permutes the factors of V. Now:

$$\sigma.V = \sigma. \prod_{g \in c} (g, \dots, g) \in \mathrm{ni}^\natural(\{(g, \dots, g) \mid g \in c\}).$$

We want to apply Theorem 8.2.14 (i) to show that $\mathrm{ni}^\natural(\{(g, \dots, g) \mid g \in c\})$ is a singleton, from which $\sigma.V = V$ follows. Consider an element $g \in c$ and elements $\gamma_{g'} \in G$ for all $g' \in c \setminus \{g\}$, such that G is generated by g together with the elements $(g')^{\gamma_{g'}}$ for $g' \in c \setminus \{g\}$. We want to show $\left\langle (g')^{\gamma_{g'}} \text{ for } g' \in c \setminus \{g\} \right\rangle \langle g \rangle = G$. There are two distinct cases:

— If g is a central element of G, then this follows easily from, say, the fact that $\langle g \rangle$ is normal in G.

— If g is not a central element of G, then there is a $g' \in c \setminus \{g\}$ such that g and g' are conjugate. Therefore $\left\langle g'^{\gamma_{g'}} \text{ for } g' \in c \setminus \{g\} \right\rangle$ is a subgroup of G that intersects every conjugacy class contained in c, and therefore it equals G by the completeness assumption.

8.3. The lifting invariant approach

In this section, we use the lifting invariant of [EVW12; Woo21] to study Question 8.1.1. We give arithmetic applications (Subsection 8.3.1 and Subsection 8.3.2), including Theorem 8.3.1 (which is Theorem 8.1.2 (ii)).

8.3.1. The lifting invariant and fields of definition of glued components

In this subsection, we use Theorem 3.4.39 to prove Theorem 8.1.2 (ii). The proof also makes use of Theorem 8.2.1.

First, following Remark 3.4.41, we fix a constant M independent from (H, c) which satisfies the conclusion of Theorem 3.4.39. Theorem 3.4.39 implies that M-big components (Definition 3.4.40) are determined by their lifting invariant. We now prove Theorem 8.3.1, whose third point is Theorem 8.1.2 (ii):

Theorem 8.3.1. *Let $x_1, \dots, x_n \in \mathrm{Comp}(G)$ be components such that $x_1 \cdots x_n$ is M-big. Then:*

(i) $\mathrm{ni}^\natural(x_1, \dots, x_n) = \{x_1 \cdots x_n\}$.

(ii) For all automorphisms $\sigma \in \Gamma_K$, we have $\sigma.(x_1 \cdots x_n) = (\sigma.x_1) \cdots (\sigma.x_n)$.

(iii) If $x_1, \dots, x_n$ are defined over K, then $x_1 \cdots x_n$ is defined over K.

Proof. Let $H = \langle x_1 \cdots x_n \rangle$ and c be the smallest conjugation-invariant containing all elements of a tuple representing $x_1 \cdots x_n$. It follows from Proposition 3.4.43 and from the multiplicativity of $\Pi_{H,c}$ that all elements of $\mathrm{ni}^\sharp(x_1, \ldots, x_n)$ have the same (H,c)-lifting invariant. Moreover they are M-big and their group is H. By Theorem 3.4.39, they are thus equal to each other. This proves point (i). Points (ii) and (iii) follow from point (i) and from Theorem 8.2.1 like in the proof of Theorem 8.2.3. □

Theorem 8.3.1 (iii) coupled with Corollary 8.2.4 imply that if $x_1, \ldots, x_n$ are defined over K, and if $k \geq M$, then $(x_1 \cdots x_n)^k$ is defined over K.

8.3.2. **The Galois action on lifting invariants**

Let H be a subgroup of G, c be a K-rational conjugation-invariant subset of H which generates H, and D^* be the set of conjugacy classes of H contained in c. In this subsection, we define a Galois action of Γ_K on the set $U(H,c)$. Proposition 8.3.2 implies that this action effectively describes the effect on lifting invariants of the Galois action on $\mathrm{Comp}(G)$. This generalizes the branch cycle lemma (Corollary 7.2.6 (i)). Moreover, in Theorem 8.3.4, we show that the Galois action on lifting invariants of elements of $\mathrm{Comp}(G)$ is compatible with multiplication.

We use the notation from Subsection 3.5.2. Consider a Galois automorphism $\sigma \in \Gamma_K$. Since c is a K-rational subset, the $\chi(\sigma)$-th power operation defines a map $p_\sigma : D^* \to D^*$.

If $\gamma \in D^*$, choose an arbitrary element g_γ of γ and denote by $\widehat{g_\gamma}$ (resp. $\widehat{(g_\gamma)^{\chi(\sigma^{-1})}}$) the projection on S_c (cf. Theorem 3.4.45) of the element $[g_\gamma] \in U(H,c)$ (resp. $\left[(g_\gamma)^{\chi(\sigma^{-1})}\right] \in U(H,c)$). Define the following element of S_c, which can be checked to be independent from the choice of g_γ:

$$w(\gamma,\sigma) \overset{\text{def}}{=} \widehat{g_\gamma}^{-\chi(\sigma^{-1})} \widehat{(g_\gamma)^{\chi(\sigma^{-1})}}.$$

Importantly, the element $w(\gamma,\sigma)$ is central in S_c (its image in H is $(g_\gamma)^{-\chi(\sigma^{-1})}(g_\gamma)^{\chi(\sigma^{-1})}$, that is 1, and thus Proposition 3.4.42 applies).

Consider an element $v \in U(H,c)$, decomposed as (h,ψ) via the isomorphism $U(H,c) \simeq S_c \underset{H^{\mathrm{ab}}}{\times} \mathbb{Z}^{D^*}$ (cf. Theorem 3.4.45). We let:

$$\sigma.v = \left(h^{\chi(\sigma^{-1})} \prod_{\gamma \in D^*} w(\gamma,\sigma)^{\psi(c)} \quad , \quad \psi \circ p_\sigma \right).$$

This formula defines an action of Γ_K on the set $U(H,c)$. This construction is taken from [Woo21, Paragraph 4.1], and the following proposition follows from [Woo21, Paragraph 6.1]:

Proposition 8.3.2. *Let $x \in \mathrm{Comp}(H,c)$. Then $\Pi_{H,c}(\sigma.x) = \sigma.\Pi_{H,c}(x)$.*

By projection on $\mathbb{Z}^{D^*}$, Proposition 8.3.2 gives back the branch cycle lemma (Corollary 7.2.6 (i)). A consequence of Proposition 8.3.2 is the following necessary condition, which refines Corollary 7.2.6 (ii):

Corollary 8.3.3. *Let $x \in \mathrm{Comp}(H,c)$. If the component x is defined over K, then its (H,c)-lifting invariant is Γ_K-invariant.*

We now show that a product of Γ_K-invariant elements of $U_1(H,c)$ is Γ_K-invariant, and thus the lifting invariant cannot be used to detect negative answers to Question 8.1.1. This follows from the following fact:

Theorem 8.3.4. *The action of Γ_K on $U_1(H,c)$ is compatible with multiplication.*

Proof. Let $v, v' \in U_1(H,c)$, and decompose them as $v = (h, \psi)$, $v' = (h', \psi')$ with $h, h' \in H_2(H,c)$ and $\psi, \psi' \in \ker(\widetilde{\pi})$. We have $vv' = (hh', \psi + \psi')$. Let $\sigma \in \Gamma_K$. With notation as above, we have:

$$\begin{aligned}
\sigma.(vv') &= \left((hh')^{\chi(\sigma^{-1})} \prod_{\gamma \in D^*} w(\gamma,\sigma)^{(\psi+\psi')(c)} \quad , \quad (\psi+\psi') \circ p_\sigma \right) \\
&= \left(h^{\chi(\sigma^{-1})} (h')^{\chi(\sigma^{-1})} \prod_{\gamma \in D^*} w(\gamma,\sigma)^{\psi(c)} w(\gamma,\sigma)^{\psi'(c)} \quad , \quad \psi \circ p_\sigma + \psi' \circ p_\sigma \right) \\
&= \left(\left(h^{\chi(\sigma^{-1})} \prod_{\gamma \in D^*} w(\gamma,\sigma)^{\psi(c)} \right) \left((h')^{\chi(\sigma^{-1})} \prod_{\gamma \in D^*} w(\gamma,\sigma)^{\psi'(c)} \right) \ , \ \psi \circ p_\sigma + \psi' \circ p_\sigma \right) \\
&= (\sigma.v)(\sigma.v').
\end{aligned}$$

□

We have used repeatedly that $H_2(H,c)$ is abelian in the final computation: this proof does not apply to arbitrary elements of $U(H,c)$. However, the same proof shows that $\sigma.(vv') = (\sigma.v)(\sigma.v')$ holds as soon as v and v' commute in $U(H,c)$.

Theorem 8.3.4 implies positive answers to Question 8.1.1 in situations where the lifting invariant is shown to characterize components. For example, Theorem 8.3.1 (iii) can be deduced from Theorem 3.4.39 by using Theorem 8.3.4 instead of Theorem 8.2.1.

8.4. The patching approach

In this section, we use patching results over complete valued fields to study the fields of definition of components obtained by gluing two components $x, y \in \mathrm{Comp}(G)$ defined over the number field K. The main result is Theorem 8.4.5, which is Theorem 8.1.2 (iii): if x, y are components defined over K, then $\mathrm{ni}^\natural(x,y)$ contains a component defined over K. We now give a sketch of the argument, which also serves as an outline of the section.

In Subsection 8.4.1, we construct infinitely many field extensions $K_1, K_2, \dots$ of K, pairwise linearly disjoint, over which the components x and y both have points (Lemma 8.4.1). This construction is done using Hilbert's irreducibility theorem (Theorem 7.1.10) repeatedly. For each $n \in \mathbb{N}$, denote by f_n (resp. g_n) a $K_n((X))$-point of x (resp. y) obtained from a K_n-point of x (resp. y). Note that $K_n((X))$ is a complete valued field for the (X)-adic valuation.

In Subsection 8.4.2, we prove that for each $n \in \mathbb{N}$, the cover obtained by patching the $K_n((X))$-G-covers f_n and g_n is a $K_n((X))$-G-cover which lies in a component $m_n \in \mathrm{ni}^\natural(x,y)$ (Lemma 8.4.2). In particular, the field of definition of the component m_n is included in $\overline{\mathbb{Q}} \cap K_n((X)) = K_n$.

Finally, we observe that at least two components $m_n, m_{n'}$ have to be equal because $\mathrm{ni}^\natural(x,y)$ is finite. Such a component $m_n = m_{n'}$ has its field of definition included in $K_n \cap K_{n'} = K$. In other words, we have found a component defined over K in $\mathrm{ni}^\natural(x,y)$: this is precisely Theorem 8.4.5. The detailed proof is the focus of Subsection 8.4.3.

Note that the results of this section rely crucially on the fact that number fields are *Hilbertian*.

8.4.1. **Constructing covers with linearly disjoint fields of definition**

Using Hilbert's irreducibility theorem (as stated in Theorem 7.1.10), we prove the Lemma 8.4.1, which is used in the proof of Theorem 8.4.5. This lemma allows us to construct points, in a given component, whose fields of definitions are linearly disjoint over the field of definition of that component. We now state and prove the lemma:

Lemma 8.4.1. *Let $L' \mid L$ be a finite Galois extension of number fields and S be an irreducible component of the Hurwitz scheme $\mathcal{H}^*(G,n)_L$ which is geometrically irreducible. Then there exists a field extension $\widetilde{L} \mid L$ such that $\widetilde{L}$ and L' are linearly disjoint over L, and an $\widetilde{L}$-point $f \in S(\widetilde{L})$.*

Proof. Since S is geometrically irreducible, its extension $S_{L'}$ is irreducible. The branch point morphism $S \to (\mathrm{Conf}_n)_L$ is finite étale. By Hilbert's irreducibility theorem (Theorem 7.1.10), there is a configuration $\underline{t} \in \mathrm{Conf}_n(L)$ such that the fiber $F \subset S(\overline{\mathbb{Q}})$ above $\underline{t}$ consists of a single Galois orbit.

Let f be any of the points in F and $\widetilde{L}$ be the smallest extension of L over which the point f is rational. Note that $\widetilde{L}L'$ is the smallest extension of L' over which the point f is rational. The fiber F is the $\mathrm{Gal}(\overline{\mathbb{Q}} \mid L')$-orbit of f, hence the degree of the extension $\widetilde{L}L' \mid L'$ is the cardinality of F. The same argument shows that the degree of the extension $\widetilde{L} \mid L$ is also equal to the cardinality of F. The equality $[\widetilde{L}L' : L'] = [\widetilde{L} : L]$ implies that L' and $\widetilde{L}$ are linearly disjoint over L. □

8.4.2. **Relating patching and gluing**

In this section, we prove Lemma 8.4.2, which is used in the proof of Theorem 8.4.5. The lemma contains all the results from Harbater's patching theory which we need for the proof.

Let $\mathcal{O}$ be a complete discrete valuation ring of characteristic zero and L its fraction field, which is a complete valued field. Since $\overline{\mathbb{Q}}$ is algebraically closed and $\overline{L}$ contains $\overline{\mathbb{Q}}$, extension of scalars induces a bijection between the connected components of $\mathcal{H}^*(G,n)_{\overline{\mathbb{Q}}}$ and those of $\mathcal{H}^*(G,n)_{\overline{L}}$. We denote by Φ_n this bijection. This lets us do the following slight terminological abuse: we say that a component $x \in \mathrm{Comp}(G)$ has an L-rational point if its extension $\Phi_{\deg(x)}(x)$ to $\overline{L}$ has an L-rational point.

Lemma 8.4.2. *Let $x_1, x_2 \in \mathrm{Comp}(G)$ be components which have L-rational points. Then there is a component $y \in \mathrm{ni}^{\natural}(x_1, x_2)$ which has an L-rational point.*

Proof.

— **Step 1: Setting things up**

For $i = 1, 2$, let $r_i = \deg(x_i)$, $G_i = \langle x_i \rangle$ and fix an L-model $f_i \in \mathcal{H}^*(G, r_i)(L)$ of an L-rational point of $\Phi_{r_i}(x_i)$. The point f_i corresponds to an L-G-cover with a marked L-point above ∞. In the cover f_i, keep only the geometrically connected component of the marked point, which is defined over L since the marked point is L-rational. This turns f_i into a geometrically connected L-G_i-cover with a marked L-point. The cover f_i belongs to the component x_i' of $\mathcal{H}^*(G_i, r_i)_L$ obtained by keeping only the component of the marked points in the covers of x_i, like in Subsection 7.2.4. Without loss of generality, we may assume $G = \langle G_1, G_2 \rangle$.

— **Step 2: Patching covers over L**

We use the algebraic patching results of [HV96]. First define:

$$\begin{aligned} L\{z\} &= \left\{ \textstyle\sum_{i\geq 0} a_i z^i \in L[[z]] \,\middle|\, a_i \underset{i\to\infty}{\to} 0 \right\} & Q_1 &= \mathrm{Frac}(L\{z\}) \\ L\{z^{-1}\} &= \left\{ \textstyle\sum_{i\geq 0} a_i z^{-i} \in L[[z^{-1}]] \,\middle|\, a_i \underset{i\to\infty}{\to} 0 \right\} & Q_2 &= \mathrm{Frac}(L\{z^{-1}\}) \\ L\{z,z^{-1}\} &= \left\{ \textstyle\sum_{i\in\mathbb{Z}} a_i z^i \in L[[z,z^{-1}]] \,\middle|\, a_i \underset{i\to\pm\infty}{\to} 0 \right\} & \widehat{Q} &= \mathrm{Frac}(L\{z,z^{-1}\}). \end{aligned}$$

Let also $Q_1' = Q_2$ and $Q_2' = Q_1$. From the point of view of rigid analytic geometry, Q_1 (resp. Q_2, and $\widehat{Q}$) is the algebra of analytic functions on the unit disk D_1 centered at 0 (resp. a disk D_2 centered at ∞, and the annulus $D_1 \cap D_2$):

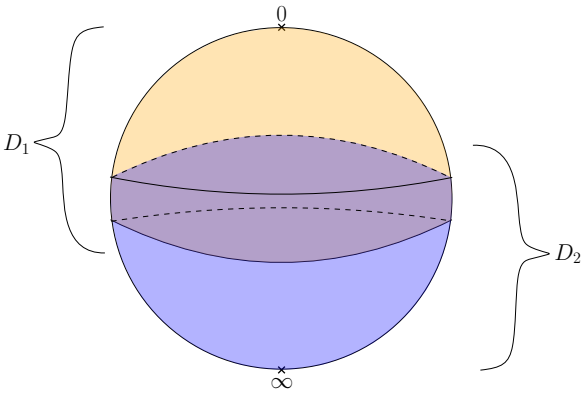


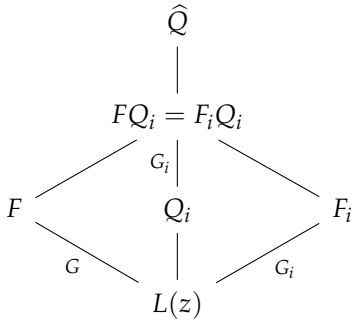
Figure 8.4.3.
The rigid analytic projective line

The marked points of the G-covers f_1, f_2 are L-points in an unramified fiber. Their existence ensures that the corresponding field extensions F_1, F_2 of $L(z)$ have an unramified prime of degree 1. By [HV96, Lemma 4.2], for $i = 1, 2$, we can then replace f_i by an isomorphic L-G_i-cover such that F_i is included in Q_i', and in particular the branch locus $\underline{t}_i \in \mathrm{Conf}_{r_i}(L)$ of f_i is included in a disk strictly smaller than D_i. [HV96, Proposition 4.3] implies that f_1 and f_2 can be patched into a geometrically connected L-G-cover f with an L-point.[7]

[7] If we are only interested in proving that there are components defined over K of small size, we do not really need to go further in the proof. In particular, no rigid analytic geometry is needed.

— **Step 3: Restriction of the patched cover f to disks**

Denote by F the field extension corresponding to f, i.e. the *compound* of F_1 and F_2 in the terminology of [HV96], which is included in $\widehat{Q}$. By [HV96, Lemma 3.6 (b)], we have the equalities $FQ_i = F_iQ_i$ (for $i = 1, 2$) inside $\widehat{Q}$. Moreover, the morphism $\mathrm{Gal}(FQ_i \mid Q_i) \to \mathrm{Gal}(F \mid L(z))$ corresponds to the inclusion $G_i \hookrightarrow G$. We sum this up by the following diagram:



Geometrically, the equality $FQ_1 = F_1Q_1$ means that the cover f_1 is isomorphic to f as a rigid analytic cover when both are restricted to the unit disk D_1, and similarly for f_2 and f in restriction to D_2.

In consequence, the branch points of f are given by the configuration $\underline{t} = \underline{t}_1 \cup \underline{t}_2$. Let y be the component of $\mathcal{H}^*(G, r_1 + r_2)_{\overline{L}}$ containing f (seen as an $\overline{L}$-point). To show that the component y fits, it remains to check that $\Phi^{-1}_{r_1+r_2}(y) \in \mathrm{ni}(x_1, x_2)$.

— **Step 4: Admissibility of the special fiber $\overline{f}$ of the patched cover**

Since $\underline{t}_1$ and $\underline{t}_2$ are included in disks strictly smaller than D_1, D_2, each of the configurations $\underline{t}_1, \underline{t}_2$ maps to a single element $\overline{a_1}, \overline{a_2}$ modulo the maximal ideal of $\mathcal{O}$, with $\overline{a_1} \neq \overline{a_2}$. The projective line $\mathbb{P}^1_L$ marked by $\underline{t} = \underline{t}_1 \cup \underline{t}_2$ has a semistable model $\widetilde{P}_{\underline{t}}$ over $\mathcal{O}$, whose special fiber $\overline{P}_{\underline{t}}$ is a "comb" with two teeth T_1, T_2, one for each coset $\overline{a_1}, \overline{a_2}$. For $i = 1, 2$, the points of the configuration $\underline{t}_i$ extend to sections which specialize to r_i distinct nonsingular points of the tooth T_i.

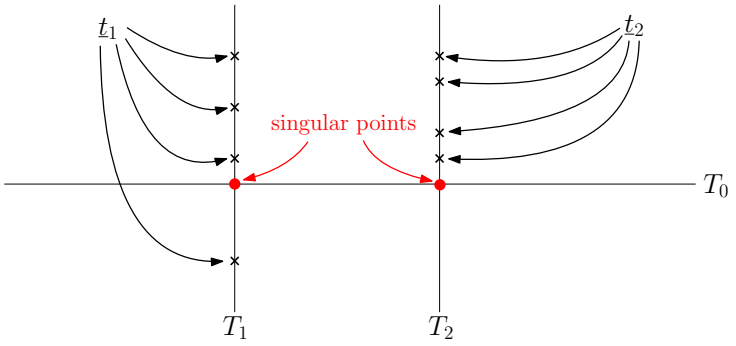


Figure 8.4.4.
The comb with two teeth $\overline{P}_{\underline{t}}$

The cover f, branched at $\underline{t}$, extends to a cover $\widetilde{f}$ of the semistable model $\widetilde{P}_{\underline{t}}$, which is ramified along the sections of the points in $\underline{t}$. The special fiber $\overline{f}$ of $\widetilde{f}$ is a cover of the comb which lies on the "boundary" of the component y in the sense of the Wewers' compactification, see [DE06, Paragraph 1.2] or [Cau12, Paragraph 3.3.1].

To prove that the special fiber $\overline{f}$ of $\widetilde{f}$ is unramified at the singular points of the comb, we follow [DE06, Paragraph 2.3] closely. The restriction of f to D_1 extends to a cover (namely, f_1) of the rigid projective line which has no branch points outside D_1. By the arguments of [DE06, Proposition 2.3, (ii)⇒(i)⇒(iii)], the restricted cover $f_{|D_1}$ is trivial above the annulus ∂D_1. The same holds for $f_{|D_2}$. Hence, $\overline{f}$ is unramified at the singular points of the comb.

We conclude that $\overline{f}$ is a cover of the comb $\overline{P}_{\underline{t}}$ unramified at the singular points, whose restriction to the i-th tooth is isomorphic to the cover f_i – which belongs to the component x_i'.

— **Step 5: Conclusion**

The conclusion of Step 4 implies that $\overline{f}$ is a Δ-admissible cover in the sense of [Cau12, Definition 3.7], where:

$$\Delta = \Big(G, (G_1, G_2), (x_1', x_2')\Big)$$

is the degenerescence structure associated to (x_1', x_2'). By [Cau12, Proposition 3.9], the component of f is a Δ-component, which in our terminology means that $\Phi^{-1}_{r_1+r_2}(y) \in \mathrm{ni}(x_1, x_2)$ as we noted in Subsection 8.2.1. This concludes the proof.

□

8.4.3. **Proof of the theorem**

We finally prove Theorem 8.4.5, which is Theorem 8.1.2 (iii). For this, we use Lemmas 8.4.1 and 8.4.2, and we follow the outline of the proof given at the beginning of this section.

Theorem 8.4.5. *Let $x, y \in \mathrm{Comp}(G)$ be components defined over K. Then $\mathrm{ni}^\natural(x,y)$ contains a component defined over K.*

Proof. Let $r_1 = \deg(x)$, $r_2 = \deg(y)$. Since the components x, y are defined over K, we fix $\begin{cases} \text{a } K\text{-model } X \subseteq \mathcal{H}^*(G,r_1)_K \text{ of } x \\ \text{a } K\text{-model } Y \subseteq \mathcal{H}^*(G,r_2)_K \text{ of } y \end{cases}$. Note that X and Y are geometrically irreducible. The proof consists of three steps:

1. First, we inductively construct two sequences of marked G-covers $(f_n)_{n\geq 1}$ and $(g_n)_{n\geq 1}$, as well as a sequence (K_n) of field extensions of K such that:

   — K_n is linearly disjoint with the Galois closure of $K_1 \cdots K_{n-1}$ over K.

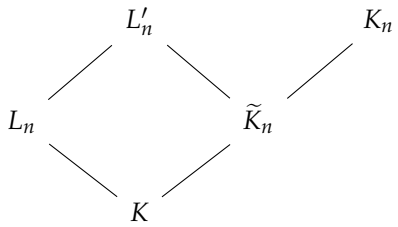
   — f_n and g_n are K_n-points of X and Y respectively.

   For f_1 and g_1, choose arbitrary $\overline{\mathbb{Q}}$-points of X and Y respectively, and let K_1 be the smallest extension of K over which they are both rational.

   Assume we have constructed $K_1, \ldots, K_{n-1}$ and $f_1, g_1, \ldots, f_{n-1}, g_{n-1}$. Let L_n be the Galois closure of $K_1 \cdots K_{n-1}$ over K.

   Apply Lemma 8.4.1 with $L = K$, $L' = L_n$ and $S = X$. This yields a field extension $\widetilde{K}_n$ of K such that $\widetilde{K}_n$ and L_n are linearly disjoint over K, and a $\widetilde{K}_n$-point f_n of X. Let L_n' be the Galois closure of $L_n\widetilde{K}_n$. Apply once again Lemma 8.4.1 with $L = \widetilde{K}_n$, $L' = L_n'$ and $S = Y_{\widetilde{K}_n}$. This yields a field extension K_n of $\widetilde{K}_n$ such that K_n and L_n' are linearly disjoint over $\widetilde{K}_n$, and a K_n-point g_n of Y. Finally, replace the $\widetilde{K}_n$-point f_n by f_n seen as a K_n-point.

   The inclusions between the fields introduced above are summed up by the following diagram:



   By construction, we have $f_n \in X(K_n)$ and $g_n \in Y(K_n)$. Now:

$$K_n \cap L_n = K_n \cap \left(L_n' \cap L_n\right) = \left(K_n \cap L_n'\right) \cap L_n = \widetilde{K}_n \cap L_n = K.$$

   Since $L_n \mid K$ is Galois, this is enough to conclude that K_n and L_n are linearly disjoint over K. We have verified that the constructed sequences (f_n), (g_n), (K_n) satisfy the desired properties.

2. Next, we show that for each n there is a component $z_n \in \mathrm{ni}^\natural(x,y)$ defined over K_n.

   Denote by $\widetilde{f}_n$ (resp. $\widetilde{g}_n$) the $K_n((X))$-point of X (resp. Y) obtained by seeing $f_n \in X(K_n)$ (resp. $g_n \in Y(K_n)$) as a $K_n((X))$-point. Since $F = K_n((X))$ is a complete

valued field, Lemma 8.4.2 implies that there is a component $z_n \in \mathrm{ni}^\natural(x,y)$ which has a $K_n((X))$-rational point. In particular, the field of definition of z_n is included in $K_n((X)) \cap \overline{\mathbb{Q}} = K_n$.

We have established that there is a component $z_n \in \mathrm{ni}^\natural(x,y)$ defined over K_n for all n.

3. Finally, since $\mathrm{ni}^\natural(x,y)$ is finite, there must be distinct integers n, n' such that $z_n = z_{n'}$. Fix such n, n'. Then, the field of definition of z_n is included in $K_n \cap K_{n'} = K$.

   This concludes the proof: there is a component $z_n \in \mathrm{ni}^\natural(x,y)$ defined over K.

□

8.4.4. **Applications of Theorem 8.4.5**

In this subsection, we give applications of Theorem 8.4.5: we show that this patching result for components of Hurwitz spaces defined over number fields implies the existence of components defined over $\mathbb{Q}$ with few branch points for many groups of interest. A first example is the following:

Example 8.4.6. The Mathieu group M_{23} is the only sporadic simple group not known to be a Galois group over $\mathbb{Q}$. In [Cau16, Exemple 3.12], a component defined over $\mathbb{Q}$ of connected M_{23}-covers with 15 branch points is constructed. Theorem 8.4.5 improves upon this result. The group M_{23} is generated by two conjugate elements a, a^γ of order 3. Using GAP:

```
a := (1, 22, 14) (2, 13, 9) (3, 8, 6) (7, 16, 21) (10, 18, 19) (11, 23, 12);
b := (2, 4, 16) (3, 5, 7) (6, 11, 12) (8, 9, 14) (10, 21, 20) (15, 18, 17);
StructureDescription(Group(a, b)); # Output: "M23"
IsConjugate(Group(a, b), a, b); # Output: true
```

By the conclusions of Example 7.2.7, the component $x = (a, a^{-1})$ and its conjugate x^γ are defined over $\mathbb{Q}$. By Theorem 8.4.5, there are elements $\gamma_1, \gamma_2 \in M_{23}$ such that $x^{\gamma_1} x^{\gamma_2 \gamma}$ is a component defined over $\mathbb{Q}$ of connected M_{23}-covers with four branch points. The same is true of the component $x x^{\widetilde{\gamma}}$ where $\widetilde{\gamma} = \gamma_1^{-1}\gamma_2\gamma$. However, we know little about $\widetilde{\gamma} \in M_{23}$. There are many pairs of generators of M_{23} with orders in $\{2,3,4,6\}$, and consequently a lot of similar examples may be found.

A second example, which is very similar, is the following:

Example 8.4.7. Similarly, the group $G = \mathrm{PSL}_2(16) \rtimes \mathbb{Z}/2\mathbb{Z}$ (labeled "17T7" on the Klüners-Malle database and on LMFDB), which is the transitive group of least degree not known yet to be a Galois group over $\mathbb{Q}$, is generated by two conjugate elements a, b of order 6:

```
a := (1, 11, 5, 13, 14, 17) (3, 15, 7, 12, 8, 6) (9, 10, 16);
b := (1, 2, 15, 12, 8, 5) (3, 14, 11, 4, 9, 6) (7, 10, 17);
StructureDescription(Group(a, b)); # Output: "PSL(2,16) : C2"
```

Like in Example 8.4.6, we conclude by Theorem 8.4.5 that there is a component defined over $\mathbb{Q}$ of connected G-covers with 4 branch points.

These two groups belong to a large family of examples: the same holds for any group generated by two elements with orders in $\{2,3,4,6\}$. More generally:

Proposition 8.4.8. *Let G be a group and $X = \{g_1, \dots, g_n\}$ be a generating set of G. For each $i \geq 2$, let $m(i)$ be the number of elements of X of order i. Then, there is a component defined over $\mathbb{Q}$ of connected G-covers whose number of branch points is $2m(2) + \sum_{i\geq 3} \varphi(i)m(i)$, where φ is Euler's totient function.*

Proof. For each $i \in \{1, \dots, n\}$, let $\underline{g}_i$ be the following tuple:

— If $\mathrm{ord}(g_i) = 2$, then:

$$\underline{g}_i = (g_i, g_i).$$

— Otherwise, $\underline{g}_i = (g_i^{k_1}, g_i^{k_2}, \dots, g_i^{k_{\varphi(\mathrm{ord}(g_i))}})$ where $\{k_1, \dots, k_{\varphi(\mathrm{ord}(g_i))}\}$ is the set of integers of $\{1, \dots, \mathrm{ord}(g_i)\}$ coprime to $\mathrm{ord}(g_i)$.

Then $\pi\underline{g}_i = 1$ so the tuple $\underline{g}_i$ defines a component whose group is the abelian group $\langle g_i \rangle$. Moreover this component is easily checked to be defined over $\mathbb{Q}$ using Corollary 7.2.6 (iii). Now apply Theorem 8.4.5 multiple times: some component of the form:

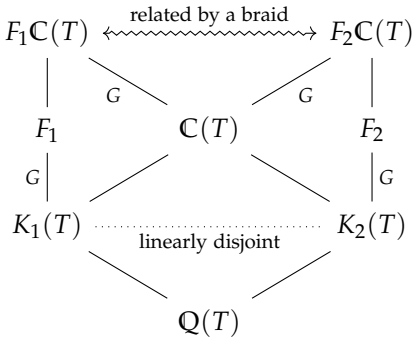
$$\prod_{i=1}^{n} \underline{g}_i^{h_i}$$

is defined over $\mathbb{Q}$ and has monodromy group $\langle g_1, \dots, g_n \rangle = G$. The number of branch points of the covers this component contains is:

$$\sum_{i=1}^{n} \left|\underline{g}_i\right| = 2m(2) + \sum_{i\geq 3} \varphi(i)m(i).$$

□

Note also that, using Lemma 8.4.1, the following can be deduced from the existence of a component x of group G defined over $\mathbb{Q}$: there are two connected G-covers, defined over two linearly disjoint Galois number fields K_1, K_2, which belong to this component:



8.5. A little extra: arithmetic factorization lemmas

This section presents results not contained in [Seg23]. We explore the possibility of obtaining factorization results similar to Lemma 4.4.8, but where we can assure that z is defined over K. This problem is a variant of Question 8.1.1 where we focus on stability by "division" instead of multiplication. This could be applied to the question of counting components defined over K.

We first recall the factorization lemma Lemma 4.4.8 under a slightly rewritten form:

Lemma: *The factorization lemma*

Lemma 8.5.1. *Let $x, y \in \mathrm{Comp}(G)$ and $H = \langle y \rangle$. Assume that $\langle x \rangle \subseteq H$ and that for all $\gamma \in D_H(x)$, we have:*

$$\mu_{H,H}(y)(\gamma) \geq |\gamma| \operatorname{ord}(\gamma) + \mu_{H,H}(x)(\gamma).$$

Then there exists a component $z \in \mathrm{Comp}(G)$ such that $y = xz$ and $\langle z \rangle = H$.

We obtain two arithmetic versions of Lemma 8.5.1: they are Lemma 8.5.2 and Lemma 8.5.3. In both cases, the proof works because the component z of Lemma 8.5.1 is shown to be uniquely defined, and thus equal to its conjugates because we are in one of the situations when Question 8.1.1 has a positive answer.

Let M be as in Remark 3.4.41, i.e. such that every M-big component (Definition 3.4.40) is characterized by its lifting invariant. A first arithmetic version of Lemma 8.5.1, whose proof uses the lifting invariant and the results of Section 8.3, is the following:

Lemma 8.5.2. *Let $x, y \in \mathrm{Comp}(G)$ be components defined over K and $H = \langle y \rangle$. Assume that $\langle x \rangle \subseteq H$ and that for all $\gamma \in D_H(y)$, we have:*

$$\mu_{H,H}(y)(\gamma) \geq M + \mu_{H,H}(x)(\gamma).$$

Then there exists a component $z \in \mathrm{Comp}(G)$ defined over K such that $y = xz$ and $\langle z \rangle = H$.

Proof. Let c be the union of all conjugacy classes $\gamma \in D_H(y)$. Note that for all $\gamma \in D_H(y)$, we have $\mu_{H,H}\left(\Pi_{H,c}(y)\Pi_{H,c}(x)^{-1}\right) \geq M$. By Theorem 3.4.39, there is a unique component $z \in \mathrm{Comp}(G)$ of group H whose (H,c)-lifting invariant is $\Pi_{H,c}(y)\Pi_{H,c}(x)^{-1}$. We show that z is defined over K. Since z is uniquely determined by its lifting invariant, it suffices to prove that $\Pi_{H,c}(z)$ is Γ_K-invariant. For all $\sigma \in \Gamma_K$, we have:

$$\begin{aligned}
\sigma.\Pi_{H,c}(z) &= \sigma.\left(\Pi_{H,c}(y)\Pi_{H,c}(x)^{-1}\right) \\
&= \left(\sigma.\Pi_{H,c}(y)\right)\left(\sigma.\Pi_{H,c}(x)\right)^{-1} && \text{by Theorem 8.3.4} \\
&= \Pi_{H,c}(y)\Pi_{H,c}(x)^{-1} && \text{by Corollary 8.3.3} \\
&= \Pi_{H,c}(z).
\end{aligned}$$

This concludes the proof. □

We give a second arithmetic factorization lemma, inspired by arguments of [EVW16]. This one uses the results from Section 8.2:

Lemma 8.5.3. *Let $x, y \in \mathrm{Comp}(G)$ be components defined over K and $H = \langle y \rangle$. Assume that $\langle x \rangle \subseteq H$. Let α be a nonnegative real number[8] such that:*

$$\mu_{H,H}(y) \geq \left(\frac{\deg(y)}{\deg(x)} - \alpha\right) \mu_{H,H}(x).$$

There exists an integer $N(x,\alpha)$, depending[9] only on x and α, such that if $\deg(y) \geq N(x,\alpha)$, then there is a component $z \in \mathrm{Comp}(G)$ defined over K such that $y = xz$ and $\langle z \rangle = H$.

[8] The smaller α is, the better the result. For example if the (H,H)-multidiscriminant of y is a multiple of that of x, we can take $\alpha = 0$.

[9] When x is fixed, the integer obtained in the proof increases with α, and tends to $+\infty$ when $\alpha \to +\infty$ – it is bounded below by $\deg(x)\alpha$.

Proof. Let $r = \deg(x)$. For $n \in \mathbb{N}$, let F_n be the (finite) set of components of size n, of group H, and whose (H,H)-multidiscriminant is at least $(\frac{n}{r} - \alpha)\mu_{H,H}(x)$. By definition of α, the component y belongs to $F_{\deg(y)}$. Lemma 8.5.1 implies that multiplication by x induces a surjection $F_{n-r} \to F_n$ when n is larger than:

$$N_0 \stackrel{\text{def}}{=} r\left(1 + \alpha + \max_{\gamma \in D_H(x)} \frac{|\gamma| \operatorname{ord}(\gamma)}{\mu_{H,H}(x)(\gamma)}\right).$$

Let $k \in \{0, \dots, r-1\}$. Since the sets F_{N_0+k+rn} are finite, their cardinality cannot decrease infinitely often, hence this cardinality stops getting smaller after some threshold. Take the maximum threshold for the various classes modulo r to obtain an integer $N(x, \alpha)$ such that if $n \geq N(x, \alpha)$, then multiplication by x induces a bijection $F_{n-r} \to F_n$. If y has size at least $N(x, \alpha)$, this implies that there is a *unique* z of group H such that $y = xz$. Let $\sigma \in \Gamma_K$. The components x and z are permuting and thus Theorem 8.2.3 (ii) implies $y = x(\sigma.z)$. By uniqueness of z, this implies $z = \sigma.z$ for all $\sigma \in \Gamma_K$. Hence z is defined over K, which concludes the proof. □

Example 8.5.4. Let c be a conjugacy class of G. Let $x \in \mathrm{Comp}(G, c)$ be a component defined over K. Assume $y \in \mathrm{Comp}(G)$ is a component defined over K of group G, represented by a n-tuple of elements of G of product one, all in c except for one. We have $\mu_{G,G}(y)(c) = \deg y - 1$. Provided that:

$$n \geq N\left(x, \frac{1}{\deg(x)}\right),$$

we can factorize y as xz, with z a component defined over K of product one. This bound does not seem so far compared to $N(x, 0)$ (although numerical evidence lacks): Lemma 8.5.3 is robust to the presence of a few elements in y whose conjugacy classes do not appear in x. This is an important difference with Lemma 8.5.2, where nothing can be said if some class appears less than M times in y.

Appendice A

Glossaire

A.1. Lexique

7-Γ-**V-EQUIVALENCE.** *Équivalence 7-Γ-V.* — Définition 6.2.4.

ALGEBRAIC COVER. *Revêtement algébrique.* — Définition 7.1.3.

ARTIN BRAID GROUP. *Groupe des tresses d'Artin.* — Définition 2.4.1.

BRAID GROUP. *Groupe des tresses.* — Définition 2.3.10.

BRAID GROUP ACTION (ON TUPLES). *Action des tresses (sur les uplets).* — Proposition 3.3.6.

BRANCH CYCLE DESCRIPTION. *Description des cycles de branchement.* — Définition 2.3.28.

BRANCH POINT. *Point de branchement.* — Définition 2.3.13.

BRANCHED / RAMIFIED COVER. *Revêtement ramifié / branché.* — Définition 2.3.13.

BRANCHED MARKED *G*-**COVER.** *G-revêtement ramifié marqué.* — Définition 2.3.15.

CONCATENATION OF TUPLES. *Concaténation de uplets.* — Définition 1.4.7.

CONFIGURATION. *Configuration.* — Définition 2.3.8.

CONFIGURATION DEFINED OVER *K***.** *Configuration définie sur K.* — Définition 7.1.1.

CONFIGURATION SPACE (ALGEBRAIC). *Espace des configurations (algébrique).* — Définition 7.1.2.

CONFIGURATION SPACE (TOPOLOGICAL). *Espace des configurations (topologique).* — Définition 2.3.8.

CONNECTED COVERING MAP. *Revêtement connexe.* — Définition 2.2.5.

COVERING MAP. *Revêtement topologique.* — Définition 2.2.1.

DEFINED OVER *K* **(COMPONENT).** *Définie sur K (composante).* — Définition 7.2.2.

DEFINED OVER *K* **(COVER).** *Défini sur K (revêtement).* — Définition 7.1.13.

D-**GENERATED SUBGROUP.** *Sous-groupe D-engendré.* — Définition 3.2.20.

EXTENSION OF SCALARS. *Extension des scalaires.* — Définition 1.4.9.

FACTOR FAMILY. *Famille de facteurs.* — Définition 5.5.4.

FACTORED SPLITTER. *Déliteur factorisé.* — Définition 5.5.7.

FIBER. *Fibre.* — Définition 2.2.2.

FIELD OF DEFINITION. *Corps de définition.* — Définition 7.1.13.

FIELD OF DEFINITION (COMPONENT). *Corps de définition (composante).* — Définition 7.2.2.

FREE FAMILY OF SUBGROUPS. *Famille libre de sous-groupes.* — Définition 5.5.2.

GALOIS COVERING MAP. *Revêtement galoisien.* — Définition 2.2.6.

G-**COVER (TOPOLOGICAL).** *G-revêtement topologique.* — Définition 2.2.10.

GEOMETRIC POINT. *Point géométrique.* — Définition 1.4.10.

GLUING OF MARKED *G*-**COVERS.** *Recollement de G-revêtements marqués.* — Définition 2.4.18.

GROUP OF A TUPLE. *Groupe d'un uplet.* — Définition 1.4.5.

HILBERT'S IRREDUCIBILITY THEOREM. *Théorème d'irréductibilité de Hilbert.* — Sous-section 7.1.3.

HURWITZ SPACE OF MARKED *G*-**COVERS (TOPOLOGICAL).** *Espace de Hurwitz topologique des G-revêtements marqués.* — Définition 3.2.4.

HURWITZ SPACE OF UNMARKED *G*-**COVERS (TOPOLOGICAL).** *Espace de Hurwitz topologique des G-revêtements non-marqués.* — Définition 3.2.12.

HURWITZ SPACE WITH CONSTRAINED MONODROMY. *Espace de Hurwitz avec monodromie contrainte.* — Définition 3.2.15.

IRRELEVANT IDEAL. *Idéal irrelevant.* — Définition 3.4.21.

k-*G*-**COVER.** *k-G-revêtement.* — Définition 7.1.4.

k-*G*-**COVER WITH A MARKED** *k*-**POINT.** *k-G-revêtement muni d'un k-point marqué.* — Définition 7.1.6.

L′-**POINT.** *L′-point.* — Définition 1.4.10.

LIFTING INVARIANT. *Lifting invariant.* — Définition 3.4.38.

LIKELY MAP. *Bon candidat.* — Définition 4.4.3.

LOCAL MONODROMY ELEMENT. *Élément local de monodromie.* — Définition 2.3.28.

MARKED COVERING MAP. *Revêtement marqué.* — Définition 2.2.9.

MARKED *G*-**COVER.** *G-revêtement marqué.* — Définition 2.2.13.

MARKED *k*-*G*-**COVER.** *k-G-revêtement marqué.* — Définition 7.1.5.

M-**BIG COMPONENT.** *Composante M-vaste.* — Définition 3.4.40.

MOCK BRANCH POINT. *Point de branchement factice.* — Définition 2.3.27.

MONODROMY CLASS. *Classe de monodromie.* — Définition 2.3.25.

MONODROMY GROUP. *Groupe de monodromie.* — Définition 2.2.18.

MONODROMY MORPHISM. *Morphisme de monodromie.* — Définition 2.2.17.

MONOID OF COMPONENTS. *Monoïde des composantes.* — Définitions 3.4.1 et 3.4.4.

MORPHISM OF *G*-**COVERS.** *Morphisme de G-revêtements.* — Définition 2.2.12.

MORPHISM OF COVERS. *Morphisme de revêtements.* — Définition 2.2.4.

MULTIDISCRIMINANT (OF A MARKED *G*-**COVER).** *Multidiscriminant (d'un G-revêtement marqué).* — Définition 2.3.29.

MULTIDISCRIMINANT (OF A TUPLE). *Multidiscriminant (d'un uplet).* — Définition 1.4.6.

NON-FACTORIZABLE COMPONENT. *Composante non-factorisable.* — Définition 3.4.14.

NON-SPLITTING PROPERTY. *Hypothèse de non-délitement.* — Définition 4.2.2.

ORDERED CONFIGURATION. *Configuration ordonnée.* — Définition 2.3.4.

PERMUTING COMPONENTS. *Composantes permutantes.* — Définitions 8.2.2 et 8.2.13.

PRODUCT OF A FREE FAMILY OF SUBGROUPS. *Produit d'une famille libre de sous-groupes.* — Définition 5.5.3.

PRODUCT OF A TUPLE. *Produit d'un uplet.* — Définition 1.4.4.

PURE BRAID GROUP. *Groupe des tresses pures.* — Définition 2.3.10.

RATIONAL POINT. *Point rationnel.* — Définition 1.4.11.

REALLY LIKELY MAP. *Très bon candidat.* — Définition 4.5.4.

RING OF COMPONENTS. *Anneau des composantes.* — Définition 3.4.12.

SIZE OF A TUPLE. *Taille d'un uplet.* — Définition 1.4.3.

(NON-)SPLITTER. *(Non-)déliteur.* — Définition 4.2.4.

SPLITTING NUMBER. *Nombre de délitement.* — Définition 4.2.3.

TOPOLOGICAL BOUQUET. *Bouquet topologique.* — Définition 2.3.19.

WEIGHTED SPAN. *Sous-espace « à poids » engendré par des vecteurs.* — Définition 5.5.12.

A.2. Index des notations

Pour les notations introduites dans le chapitre 1, voir la section 1.4.

Symbole	Description	Référence
$O^\sharp\left(n^\zeta\right)$	A function that is $O(n^\zeta)$ and not $o(n^\zeta)$	Definition 1.4.1
$X_{L'}$	The extension of scalars of X to L'	Definition 1.4.9
$X(L')$	The set of L'-points of the scheme X	Definition 1.4.10
$\star[\gamma]$	Point d'arrivée de l'unique chemin relevant γ et débutant au point $\star$	Proposition 2.2.14
(P)Conf$_{n,X}$	Espace des configurations de n points (ordonnés si P) distincts de $X \setminus \{t_0\}$	Définitions 2.3.4 et 2.3.8
(P)B$_{n,X}$	Groupe des tresses (pures si P) de X	Définition 2.3.10
BCD$_{\underline{\gamma}}(p,\star)$	Description des cycles de branchement du G-revêtement marqué $(p,\star)$ pour le bouquet $\underline{\gamma}$	Définition 2.3.28
$\mu_{H,c}(p,\star)$	(H,c)-multidiscriminant du G-revêtement marqué $(p,\star)$	Définition 2.3.29
B$_n$	Groupe des tresses d'Artin	Définition 2.4.1
(C)(P)Hur$_X^{(*)}(G,n)$	Espace de Hurwitz des G-revêtements (marqués si $*$) (connexes si C) de X ramifiés en n points (ordonnés si P)	Définitions 3.2.1, 3.2.2, 3.2.4, 3.2.11 et 3.2.12
TΓ	Isomorphisme de transport le long d'un chemin Γ dans Conf$_n$	Lemme 3.2.7
Hur$_X^*(G,D,\xi)$	Espace de Hurwitz des G-revêtements ramifiés de X, marqués, avec $\xi(\gamma)$ éléments de monodromie dans chaque $\gamma \in D$.	Définition 3.2.15

ConjInv	Catégorie des triplets (H, D, ξ), où les éléments de D sont des parties disjointes du groupe H, invariantes par conjugaison, et $\xi : D \to \{0, 1, \dots\}$.	Définition 3.2.18
$\mathrm{Sub}_{G,D}$	Ensemble des sous-groupes D-engendrés de G	Définition 3.2.20
$\sim$	Relation d'équivalence des n-uplets modulo l'action du groupe des tresses B_n	Proposition 3.3.6
$\mathrm{Comp}_X(G)$, $\mathrm{Comp}_X(H, c)$, $\mathrm{Comp}_X(G, D, \xi)$	Monoïdes des composantes de G-revêtements marqués de X	Définitions 3.4.1, 3.4.4 et 3.4.10
$R_X(G)$, $R_X(H, c)$, $R_X(G, D, \xi)$	Anneaux des composantes de G-revêtements marqués de X	Définition 3.4.12
$\widetilde{\pi}$	Le morphisme $\mathbb{Z}^{D^*} \to G^{\mathrm{ab}}$ qui permet de retrouver l'image de $\pi\underline{g}$ dans G^{ab} à partir du (G, c)-multidiscriminant de $\underline{g}$	Définition 3.4.32
$U(G, c)$	Groupe dans lequel le *lifting invariant* prend ses valeurs	Définition 3.4.37
$\Omega(D)$	The splitting number	Definition 4.2.3
$\gamma_\xi(H)$	Subset of Spec $R(G, \xi)(k)$ associated to the subgroup H	Definition 5.1.2
Conf_n	Espace des configurations (algébrique)	Sous-section 7.1.1
$(\mathcal{C})\mathcal{H}^{(*)}(G, n)$	$\mathbb{Q}$-schéma de Hurwitz des G-revêtements (marqués si $*$) (géométriquement irréductibles si $\mathcal{C}$) de $\mathbb{P}^1$, ramifiés en n points, non-ramifiés au dessus du point à l'infini.	Sous-section 7.2.1

Appendice B

Ma thèse racontée aux non-mathématicien·ne·s

Organisation du chapitre

Mise en garde : Les notes dans la marge sont généralement des précisions techniques dont on ne recommande pas la lecture au public non-mathématicien. (Elles ont avant tout pour fonction de protéger l'auteur des châtiments qu'il mérite pour les simplifications, évidemment douloureuses, qu'il a décidées)

Petite convention : quand un mot apparaît pour la première fois et qu'il est *en italique*, cela signifie qu'il est attendu que vous ne l'ayez jamais rencontré, et que les phrases qui suivent donnent une description rapide de la façon à laquelle il faut penser à l'objet correspondant.

B.1. Équations polynomiales : géométrie et arithmétique

Dès l'Antiquité, notre espèce s'est intéressée à la résolution d'*équations* : au lieu d'évaluer une expression en fonction de ses paramètres, on cherche quelle valeur attribuer aux paramètres (qu'on appelle alors *inconnues* ou *indéterminées*) pour que l'expression prenne une valeur donnée. C'est une forme de « calcul à l'envers ».

Parmi les équations, on trouve les *équations polynomiales*[1]. Ce sont les équations qu'on peut écrire en utilisant des nombres entiers (1, 2, 157, -39, 0, ...) et des fractions d'entiers (des *nombres rationnels*, comme $5/7$ ou $-4/11$), des multiplications, des additions et soustractions, et des inconnues qu'on représente par des lettres (x, y, z, ...). On peut élever ces inconnues au carré, au cube, et ainsi de suite (par exemple, $x^4 = x \times x \times x \times x$). Voici un exemple d'équation polynomiale :

$$(x-3)^2 + (y-1)^2 = 25.$$

Une *solution* de cette équation est donnée par deux nombres x et y qui satisfont l'égalité. Par exemple, si on fixe la valeur de x à 0 et celle de y à 5, on a :

$$(x-3)^2 + (y-1)^2 = (-3)^2 + 4^2 = 9 + 16 = 25.$$

Ainsi, « $x = 0$ et $y = 5$ » est une solution de l'équation ci-dessus.

Étant donnée une équation polynomiale, on peut la considérer de plusieurs points de vue :

— On peut s'intéresser à ses solutions au sens large[2]. En les considérant toutes, on obtient un objet géométrique, qu'on appelle *variété*.

  Dans l'exemple ci-dessus, il s'agit des points (x, y) du plan qui satisfont l'égalité $(x-3)^2 + (y-1)^2 = 25$: c'est un cercle, de centre $(3, 1)$ et de rayon 5.

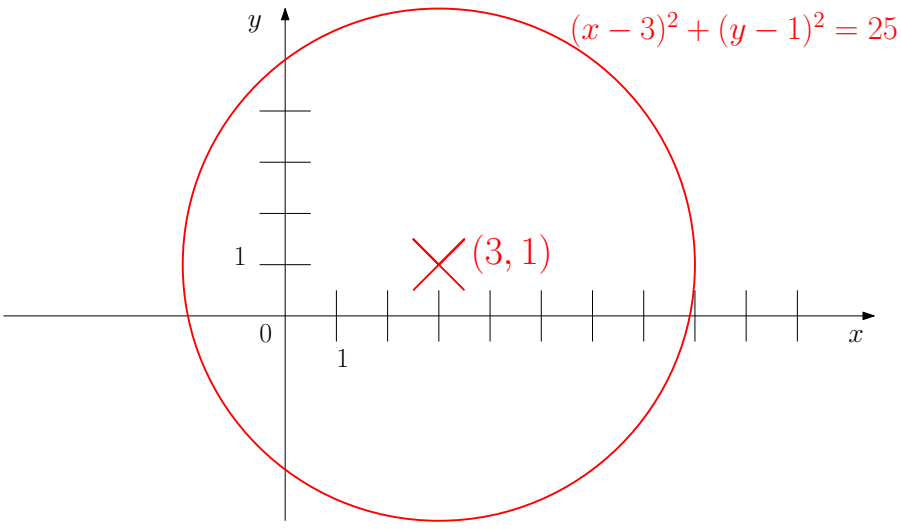


Figure B.1.1. La variété associée à l'équation $(x-3)^2 + (y-1)^2 = 25$

  Quand on décrit la forme de la variété associée, on dit qu'on s'intéresse aux propriétés *géométriques* de l'équation.

— On peut s'intéresser à des solutions particulières. Par exemple, on regarde les solutions qui sont des entiers ou des nombres rationnels (des fractions).

  On parle parfois d'*équations diophantiennes*, du nom du mathématicien grec Diophante, qui vivait au troisième siècle : la recherche de solutions en nombres entiers ou rationnels est un problème très ancien. Cette question a trouvé au cours du siècle dernier un rôle central en *cryptographie* : il est si compliqué de trouver des solutions à ces équations qu'on peut exploiter cette complexité afin de sécuriser des transactions bancaires !

[1] « à coefficients rationnels », mais toutes nos équations seront implicitement de ce type sauf mention explicite du contraire

[2] Comprendre : les solutions complexes (ou, en première approximation, réelles)

Chercher des solutions en nombres rationnels revient à chercher, sur l'objet géométrique précédent (la *variété*), des points dont toutes les coordonnées sont rationnelles. Trouver de tels points particuliers, les *points rationnels*, est un problème très difficile.

Quand on regarde les points rationnels (ou entiers) d'une variété, on dit qu'on s'intéresse aux propriétés *arithmétiques* de l'équation.

Revenons à l'exemple de l'équation du cercle. Trouver les points rationnels du cercle revient essentiellement à lister les *triplets pythagoriciens*, à savoir les nombres entiers a, b et c qui sont les côtés d'un triangle rectangle (comme 3, 4 et 5, puisque $3^2 + 4^2 = 5^2$). La méthode générale pour construire de tels triplets était déjà connue de Pythagore, qui vivait au sixième siècle avant notre ère : les propriétés arithmétiques de l'équation du cercle sont bien comprises.

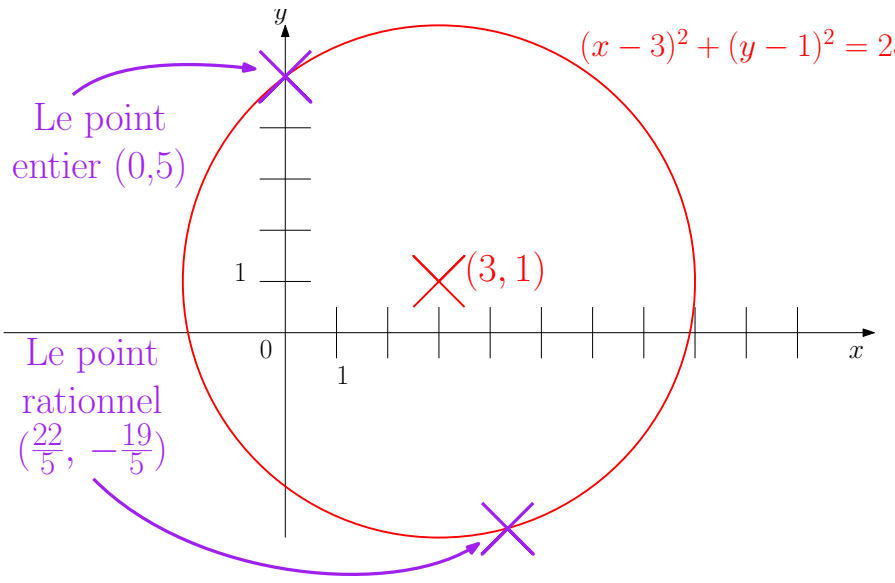


Figure B.1.2. Deux solutions rationnelles de $(x-3)^2+(y-1)^2=25$

Pour des équations plus compliquées, on ne sait souvent rien dire. Par exemple, il a fallu attendre 1995 pour que le mathématicien anglais Andrew Wiles démontre que l'équation suivante, qui est visuellement « à peine plus générale » que celle de Pythagore (on a simplement remplacé 2 par un entier arbitraire $n \geq 3$) n'a aucune solution pour laquelle a, b et c sont des entiers non nuls :

$$a^n + b^n = c^n.$$

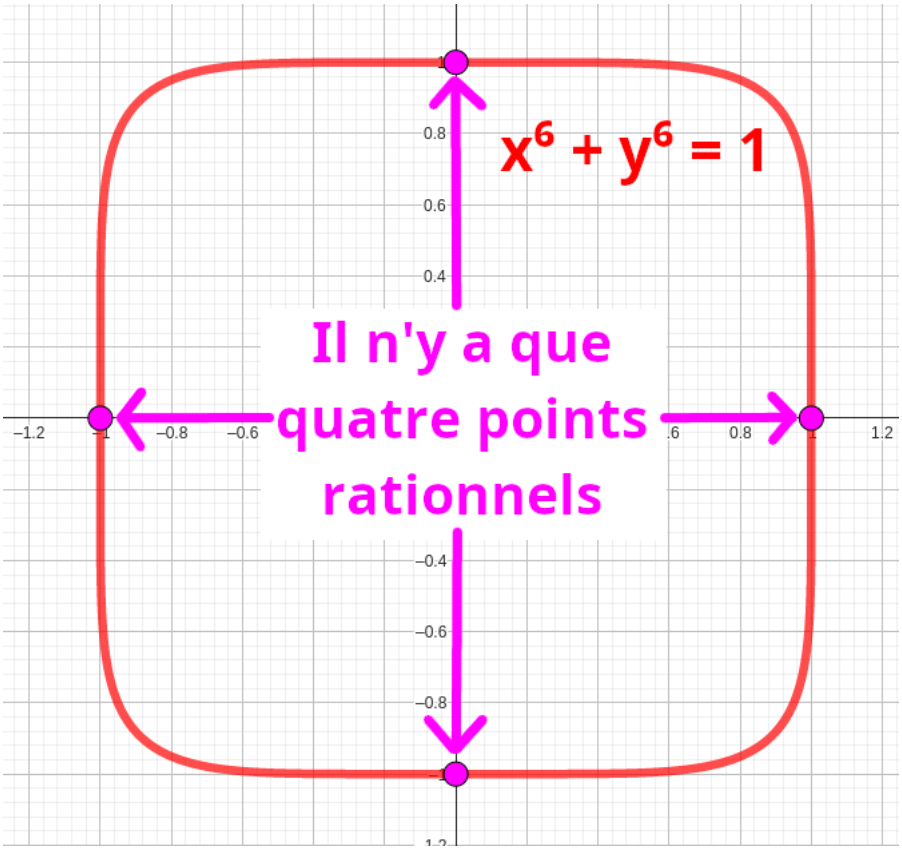


Figure B.1.3.
La variété correspondant à l'équation $x^6 + y^6 = 1$ (un carré aux coins arrondis) n'a pas de points rationnels non-triviaux : c'est le cas $n = 6$ du grand théorème de Fermat

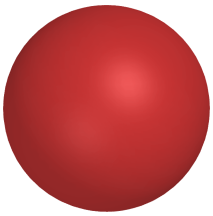
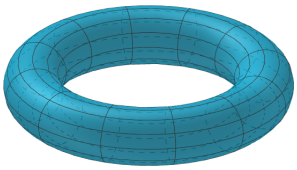
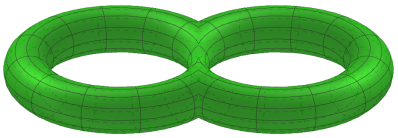
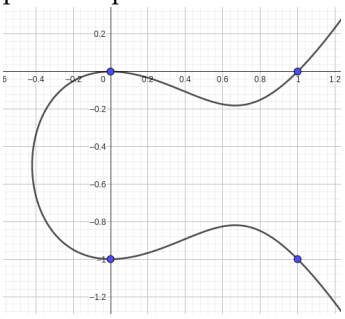
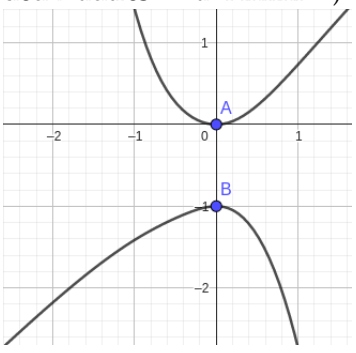
La *géométrie arithmétique* est l'étude des liens entre les propriétés géométriques et les propriétés arithmétiques d'une équation polynomiale. En général, l'étude géométrique est plus aisée que l'obtention d'informations arithmétiques : l'existence d'un point rationnel est, en général, un problème très difficile !

Pour donner une idée du type de liens attendus, voici deux exemples de résultats de géométrie arithmétique :

— **Premier exemple :** Si la variété correspondant à une certaine équation à deux indéterminées définit une surface[3] qui a au moins deux trous (un donut n'a qu'un trou, mais deux donuts collés ensemble forment une surface avec deux trous), alors elle ne possède qu'un nombre fini de points rationnels.

Si vous voulez en savoir plus, le tableau suivant résume les différentes situations qui sont couvertes par le théorème, en donnant quelques exemples :

[3] Nous disons ici « surface », mais le terme mathématique est en fait « courbe », c'est-à-dire « variété de dimension 1 ». Cela est dû à la différence entre nombres réels et complexes : quand on dessine les solutions réelles comme on l'a fait précédemment, on dessine en fait une « tranche » de la variété qui, prise tout entière, a une dimension deux fois plus grande. À l'œil, les courbes ressemblent donc plutôt à des surfaces quand on les

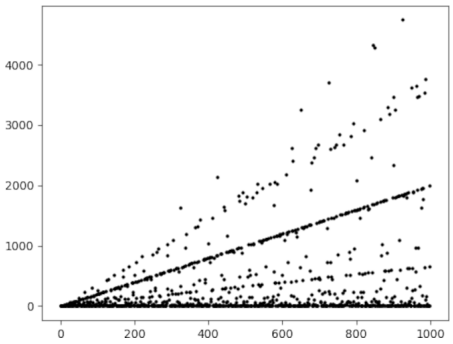
Genre (« nombre de trous ») de la variété	0	1	≥ 2
Situation géométrique typique	La sphère : 	Le donut (ou *tore*) : 	Le tore à 2 trous : 
Degré typique des équations	1 ou 2	3	≥ 4
Nombres possibles de points rationnels	• Soit aucun • Soit une infinité	• Soit aucun • Soit un nombre fini ≥ 1 (courbe elliptique de rang 0) • Soit une infinité (courbe elliptique de rang ≥ 1)	• Soit aucun • Soit un nombre fini
Exemples	• $x^2 + y^2 = -1$ Il n'y a pas de points rationnels puisqu'il n'y a même pas de points réels : le membre de gauche est toujours positif lorsque x et y sont réels, et n'est donc pas égal à -1. • $x^2 + y^2 = 1$ Les points réels forment un cercle de centre $(0,0)$ et de rayon 1, qui a une infinité de points rationnels.	• $3x^3 + 4y^3 + 5 = 0$ Il n'y a pas de points rationnels. • $y^2 + y = x^3 - x^2$ Il y a quatre points rationnels, plus un point « à l'infini » :  • $y^2 + y = x^3 + x^2$ Il y a une infinité de points rationnels.	• $y^2 + x^6 + 3x^4 + 4x^2 = -2$ Courbe de genre 2. Il n'y a pas de points rationnels car il n'y a pas de points réels. • $y^2 + (x^3 + 1)y = x^4 + x^2$ Courbe de genre 2. Il y a deux points rationnels (et deux autres « à l'infini ») : 

Ce résultat, qui relie géométrie et arithmétique d'une manière particulièrement frappante, a été démontré en 1983 par le mathématicien allemand Gerd Faltings.

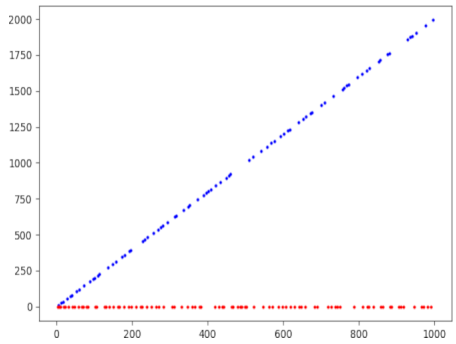
— **Deuxième exemple :** L'ensemble des nombres rationnels étant infini, il n'est pas toujours facile de donner un sens au fait de compter les solutions d'une équation. À la place, on peut regarder les solutions dans un système de nombres qui est de taille finie. Il faut imaginer un système de nombres qui généralise « l'arithmétique de l'horloge » : 4 heures après 22h, il n'est pas 26h mais 2h. On peut donc considérer que $22 + 4 = 2$, et que $24 = 0$. Cette façon de calculer permet de faire de l'arithmétique avec une quantité finie de nombres, et de regarder les solutions d'une équation dans cet ensemble fini. Par exemple, sur une horloge avec 13 heures par jour, c'est-à-dire en considérant que $13 = 0$, l'équation :

$$x^2 + y^2 = 0$$

admet la solution $x = 5$ et $y = 1$, puisque $5^2 + 1^2 = 26 = 2 \times 13 = 2 \times 0 = 0$. Toute équation a un nombre fini de solutions lorsqu'on la regarde sur une telle horloge : on se demande alors *combien* il y en a. Par exemple, dans le cas de l'équation $x^2 + y^2 = 0$, il y a 25 solutions sur une horloge à treize heures, et 193 sur une horloge à 97 heures. L'évolution du nombre de solutions pour les horloges ayant mille heures et moins est représentée sur les graphiques suivants :



Si on regarde toutes les tailles d'horloge, il y a du « bruit ».



La situation est un peu plus claire si on ne regarde que les horloges dont le nombre d'heures est un nombre premier.

Un théorème difficile dit qu'on peut estimer avec grande précision le nombre de solutions d'une équation dans un système de nombres qui est fini mais très grand[4] à partir de données complètement géométriques, qu'on appelle « nombres de Betti », et qui généralisent en quelque sorte le « nombre de trous » dont on a parlé précédemment.

C'est là une forme des *conjectures de Weil*, proposées par le mathématicien français André Weil en 1949. Ces conjectures ont été au cœur des mathématiques de la deuxième moitié du vingtième siècle. Elles ont finalement été démontrées par étapes, entre 1960 et 1974, par les mathématiciens Bernard Dwork (américain), Alexandre Grothendieck (français) et Pierre Deligne (belge).

[4] On regarde en fait le comportement du nombre de solutions à valeurs dans un *corps fini* $\mathbb{F}_q$, lorsque q devient grand. Si q n'est pas un nombre premier ($q = p^r$ avec $r > 1$) l'arithmétique de l'horloge n'est pas une bonne façon de comprendre $\mathbb{F}_q$.

B.2. Équations en une indéterminée : la révolution galoisienne

Parmi les équations polynomiales, une classe importante est celle des équations ne faisant intervenir qu'une seule inconnue. Une telle équation peut toujours s'écrire sous la forme :

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

On dit que l'entier n, la plus grosse puissance qui apparaît dans l'équation, est le *degré* de l'équation. Ici, et bien qu'on les désigne par des lettres, les nombres $a_{n-1}, \ldots, a_0$ ne sont pas des inconnues, ce sont des nombres fixés qu'on appelle *coefficients* de l'équation. On les écrit ainsi afin de donner la forme la plus générale possible d'une équation : chaque liste de nombres par laquelle on substituera $a_{n-1}, \ldots, a_0$ donnera lieu à *une* équation. Dans cette section, le mot *équation* signifie « équation polynomiale en une indéterminée ».

Géométriquement, la variété définie par une équation de degré n est de peu d'intérêt, il s'agit simplement d'un ensemble de n points[5] (qui peuvent se superposer) : autrement dit, la variété associée est de dimension nulle.

La *résolution* des équations, dans ce cas, consiste à exprimer les solutions (ou, au moins, l'une d'entre elles) en fonction des coefficients. La complexité de la résolution augmente visiblement avec le degré :

[5] Ici, les « points » sont des nombres complexes. Le fait qu'il y en ait bien n n'est déjà pas évident : il s'agit du *théorème fondamental de l'algèbre*, démontré au dix-huitième siècle.

— Pour les équations de degré 1, qui sont de la forme :

$$x + a_0 = 0,$$

la solution est donnée par $-a_0$. En particulier, cette solution est toujours rationnelle.

— La résolution des équations de degré 2 remonte aux mathématiques babyloniennes du dix-huitième siècle avant notre ère. Étant donnée une équation du second degré :

$$x^2 + a_1 x + a_0 = 0,$$

les solutions sont de la forme :

$$\frac{-a_1 + \delta}{2}$$

où δ est une racine carrée du nombre $a_1^2 - 4a_0$. La rationalité de ces solutions dépend de si $a_1^2 - 4a_0$ est le carré d'un nombre rationnel ou non : ce cas illustre la nécessité, dans certains cas, « d'élargir » le système de nombres dans lequel on fait les calculs pour résoudre des équations.

— La résolution des équations de degré 3 et 4 remonte au seizième siècle, et est due aux mathématiciens italiens Niccolò Tartaglia et Ludovico Ferrari. Comme dans le cas des équations de degré 2, il est nécessaire, pour exprimer les solutions, d'extraire des racines (carrées ou cubiques) de quantités obtenues à partir des coefficients.

On pourrait croire que le schéma se poursuit pour les degrés supérieurs : quitte à extraire des racines de quantités formées à partir des coefficients, on peut exprimer les solutions d'une équation en fonction de ses coefficients. Cependant, au début du dix-neuvième siècle, le mathématicien norvégien Niels Abel démontre que pour les équations de degré cinq et plus, aucune telle méthode de résolution ne fonctionne.

Le jeune mathématicien français Évariste Galois, jetant une lumière nouvelle sur les résultats d'Abel, met alors en évidence un principe important : la difficulté à résoudre une équation est liée aux « symétries » qui existent entre ses solutions.

Il introduit pour cela la notion de *groupe de symétries*[6] d'une équation, qu'on nommera aussi *groupe de Galois*[7]. L'existence de symétries entre les différentes solutions d'une équation sont liées au fait que, dans certaines situations, deux d'entre elles peuvent être indistinguables, c'est-à-dire que toute équation (à coefficients rationnels) satisfaite par l'une est aussi satisfaite par l'autre[8] :

— Si, par exemple, une équation polynomiale a une solution rationnelle $\frac{a}{b}$, alors celle-ci est bien distinguable des autres puisqu'elle satisfait l'équation $ax - b = 0$ que ne satisfont pas les autres solutions. Cela entraîne que le groupe des symétries va « fixer » la solution rationnelle (elle va rester à sa place quelle que soit la symétrie considérée).

— Dans l'autre direction, si nous prenons les deux racines carrées d'un nombre rationnel non nul qui n'est pas le carré d'un nombre rationnel (par exemple, 2), alors il n'y a pas de manière de les distinguer[9] : toute équation satisfaite par l'une est automatiquement satisfaite par l'autre. Il existe ainsi une symétrie qui permute les deux racines carrées.

Galois ayant introduit cette idée de symétries entre solutions, le résultat d'Abel prend un sens nouveau, plus géométrique : dans certaines circonstances (liées notamment au degré), il y a des symétries si nombreuses et complexes entre les solutions d'une équation qu'aucune formule simple, qui ne ferait intervenir que les coefficients, ne pourrait avoir les mêmes symétries. Cela redémontre l'impossibilité de résoudre les équations de degré cinq et plus.

Aparté : *L'auteur recommande chaudement le visionnage de la vidéo suivante (en anglais, sur la chaîne YouTube de « not all wrong ») pour une preuve du théorème d'Abel qui reprend un argument dû au mathématicien russe Vladimir Arnol'd, et dans laquelle la notion de symétrie entre solutions est illustrée de manière limpide (bien que le mot « groupe de Galois » soit soigneusement évité) :* `https://www.youtube.com/watch?v=BSHv9Elk1MU`.

On a dit qu'une solution rationnelle était fixée par toutes les symétries entre les solutions. On peut en fait montrer l'inverse : une solution qui est fixée par le groupe de Galois est une solution rationnelle. Cela donne une autre manière d'envisager la recherche de solutions rationnelles : au lieu de rester dans le monde des fractions et d'essayer d'y résoudre des équations, on regarde toutes les solutions, rationnelles ou non, et on essaie de démontrer que l'une d'entre elles n'est échangée avec une autre solution par aucune des symétries de l'équation.

B.3. Le problème de Galois inverse

En étudiant les symétries qui existent entre les solutions d'une équation polynomiale (à une seule inconnue), Galois a introduit un objet mathématique « abstrait », le *groupe*. La notion de groupe est un modèle mathématique de ce que peuvent être les symétries d'un objet, au sens le plus large. À chaque équation, Galois associe un groupe, le *groupe de Galois* de cette équation, qui tient compte de toutes les symétries qui existent entre ses solutions.

[6] Les groupes considérés seront nécessairement finis, excepté les groupes de Galois absolus. On n'entrera pas dans ces précisions pour fluidifier la narration.

[7] On ignore ici toute discussion sur le caractère galoisien des extensions : le groupe de Galois d'un polynôme est le groupe de Galois de son corps de décomposition.

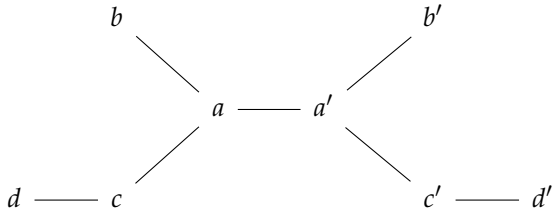
[8] Pour être complet, on doit aussi prendre en compte que deux *paires* de solutions peuvent être indistinguables, etc.

[9] Là encore, cela est vrai car nous travaillons avec des nombres complexes. Dans les nombres réels, on peut différencier les deux racines carrées d'un nombre réel positif puisque seule l'une d'entre elle possède une racine carrée.

Depuis Galois, les groupes ont pris une place importante au sein des mathématiques : pour à peu près tout objet mathématique, on peut considérer ses symétries (ou, plus pompeusement, ses *automorphismes*) et obtenir un groupe. Dans de nombreux contextes, on sait montrer que tout groupe est le groupe des symétries d'un objet concret :

— Par exemple, le mathématicien germano-chilien Roberto Frucht a démontré en 1939 que tout groupe fini est le groupe des automorphismes d'un graphe.

  On peut imaginer un graphe comme un réseau social. L'existence de symétries correspond alors à l'impossibilité de distinguer deux membres du réseau. Par exemple, deux membres qui ont des nombres d'amis distincts sont nécessairement distinguables (on peut les reconnaître en comptant leurs amis), et aucune symétrie ne peut donc les échanger. Pour un exemple plus intéressant, il existe une unique symétrie non-triviale du graphe suivant (celle qui échange a et a', b et b', c et c', d et d') :



  Le théorème de Frucht énonce alors que toutes les possibilités « théoriquement envisageables » de symétries sont en effet le groupe de symétries d'un graphe. (On propose de construire un graphe qui a exactement deux symétries non-triviales)

  Commentaire : *Si, dans le graphe ci-dessus, on ne peut pas distinguer a de a' et b de b', on peut bien distinguer la paire (a, b) (qui est connectée par une arête) de la paire (a, b') (qui ne l'est pas). Pour obtenir un graphe équivalent, on ne pourrait donc pas échanger les étiquettes des sommets a et a' sans également échanger celles de b et b'. Ces formes plus complexes de symétries (et d'absences de symétries, c'est-à-dire de capacité à distinguer entre eux non pas seulement des sommets, mais aussi certains ensembles de sommets) sont aussi prises en compte par le groupe des symétries d'un graphe. La même chose vaut pour les symétries dans le cas des équations polynomiales : certaines permutations des solutions sont possibles, d'autres non, et c'est cette information qui constitue le groupe de Galois proprement dit.*

— Similairement, dans le contexte des *revêtements ramifiés de la sphère*, objets géométriques qu'on reverra plus tard, on montre que tout groupe fini est le groupe des symétries d'un tel revêtement (Corollaire 2.4.17).

Ces résultats montrent en quelque sorte que la définition du *groupe* proposée par Galois est la bonne : elle n'est ni trop contraignante, ni trop peu, et elle prend précisément en compte la diversité des symétries qu'un objet peut effectivement avoir.

Le problème de Galois inverse est alors la question suivante : tout groupe fini est-il le groupe de Galois d'une équation polynomiale, dont les coefficients sont des nombres rationnels ? Au lieu de partir d'une équation et de déterminer son groupe de Galois, on part d'un groupe de symétries, et on tente de construire une équation dont les solutions ont exactement les symétries prescrites.

Rappelons que l'existence de symétries entre les solutions d'une équation est au cœur des difficultés qui existent à pouvoir la résoudre : de ce point de vue, une réponse négative au problème de Galois inverse serait curieuse, et entraînerait que certains des types théoriquement possibles d'obstacles à la résolution des équations ne surviennent en fait jamais.

En 2023, le problème de Galois inverse est toujours ouvert. Puisqu'une solution « uniforme » semble hors de portée, les mathématicien·ne·s réalisent divers groupes « un par un » pour y voir plus clair. On parle alors, lorsque G est un groupe, de résoudre le problème de Galois inverse *pour* G.

Le premier résultat important relatif au problème de Galois inverse est le *théorème d'irréductibilité*, que le mathématicien allemand David Hilbert démontre en 1892 (Sous-section 7.1.3). Il énonce essentiellement, que, pour réaliser un groupe G comme groupe de symétries d'une équation à une indéterminée, il suffit de construire une équation avec autant d'indéterminées qu'on veut, et telle que G soit le groupe des symétries de la variété associée (plus précisément, les symétries qui préservent toutes les coordonnées sauf la première, mais nous n'insisterons pas sur ce point et nous parlerons simplement de symétries).[10]

[10] Nous passons sous silence, ce qui peut surprendre étant donné le nom du théorème, l'hypothèse d'irréductibilité.

Le théorème d'irréductibilité de Hilbert transforme le problème de Galois inverse en un problème portant sur des objets géométriques qui ne sont plus de dimension nulle (auquel cas les méthodes géométriques sont de peu d'intérêt), mais de dimension supérieure : il ouvre ainsi la voie à l'utilisation d'outils géométriques pour étudier ce problème d'arithmétique.

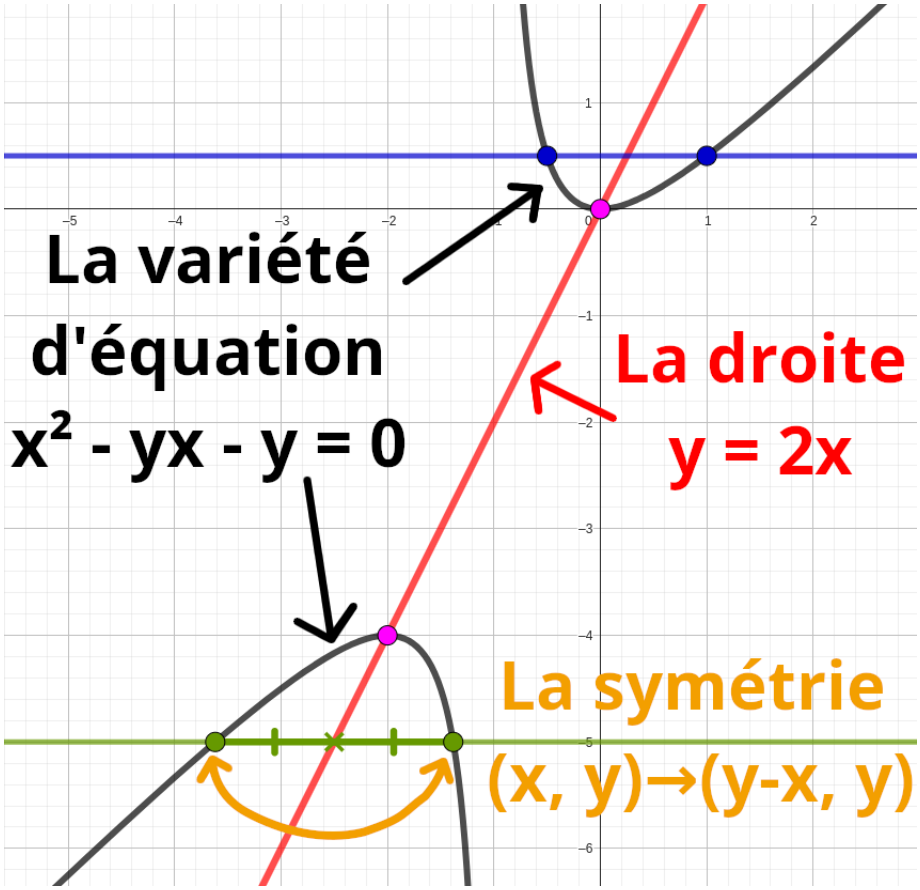
Nous détaillons un peu plus longuement le contenu de ce théorème dans l'encadré suivant :

Que dit le théorème de Hilbert ?

Considérons une équation polynomiale, par exemple l'équation :

$$x^2 - yx - y = 0.$$

Cette équation en deux indéterminées x et y définit une variété. Cette variété a exactement une symétrie non-triviale qui préserve la coordonnée y : c'est l'opération qui envoie un point (x, y) sur le point $(y - x, y)$:



Le théorème d'irréductibilité de Hilbert affirme que pour la plupart des nombres rationnels y_0, l'équation obtenue en attribuant la valeur y_0 à l'indéterminée y :

$$x^2 - y_0 x - y_0 = 0,$$

équation qui n'a *plus qu'une seule indéterminée* (à savoir x), a exactement les symétries décrites plus haut, à savoir les symétries de l'équation originale qui laissent inchangée la coordonnée y.
Dans l'exemple précédent, pour se retrouver dans le cas favorable, il suffit de trouver une « tranche » (c'est-à-dire l'intersection de la variété $x^2 - yx - y = 0$ avec une droite horizontale, comme la droite verte) qui est telle que :

— Il y ait le bon nombre de points. Il faut donc faire attention à éviter les deux points roses, obtenus pour $y = 0$ et $y = -4$.

— Les points en question ne soient pas rationnels. Par exemple, il faut éviter de choisir $y = \frac{1}{2}$ (en bleu sur le dessin) puisqu'alors les solutions de l'équation :

$$x^2 - \frac{1}{2}x - \frac{1}{2} = 0$$

sont les nombres rationnels $-\frac{1}{2}$ et 1. Lorsque les points sont rationnels, il n'y a aucune symétrie non-triviale et on ne retrouve donc pas la symétrie non-triviale qu'on avait identifiée sur la variété définie par l'équation $x^2 - yx - y = 0$.

Remarque : *Dans cet exemple, les valeurs problématiques de y sont exactement celles pour lesquelles $(y+2)^2 - 2^2$ est le carré d'un nombre rationnel. On peut lister ces valeurs en utilisant la description des triplets pythagoriciens.*

Le théorème de Hilbert dit que les nombres rationnels « problématiques », c'est-à-dire ceux tels que le groupe des symétries de l'équation change lorsqu'on remplace l'indéterminée y par leur valeur, sont exceptionnels. Si on attribue à une indéterminée y une valeur rationnelle prise au hasard, on va généralement obtenir une équation (avec une indéterminée de moins) ayant exactement autant de symétries que l'équation originale avait de symétries préservant l'indéterminée y.

B.4. Revêtements et espaces de Hurwitz

Au tournant du vingtième siècle, l'approche initiale considérée par Hilbert et la mathématicienne allemande Emmy Noether consistait à appliquer le théorème d'irréductibilité de Hilbert avec un nombre assez important d'indéterminées. En 1984, le mathématicien américain David Saltman a mis en évidence que leur stratégie envisagée était trop optimiste.

Une approche légèrement différente se concentre sur les équations à *deux* indéterminées, qu'on appellera *revêtements ramifiés de la sphère*.[11]

Les revêtements ramifiés sont des objets géométriques qui ont été étudiés largement au cours du dix-neuvième siècle, notamment par le mathématicien allemand Bernard Riemann. Ils peuvent être définis de façon géométrique, sans référence à la théorie des équations polynomiales. Riemann démontra l'équivalence entre les deux définitions : tout revêtement ramifié est la variété associée à une certaine équation polynomiale à deux inconnues. Cependant, les équations obtenues ont généralement des coefficients compliqués, qui ne sont pas simplement des fractions d'entiers : il faut puiser dans des systèmes de nombres un peu plus grands.

Quand on s'intéresse à la théorie géométrique des revêtements, on montre que tout groupe est le groupe des symétries[12] d'un revêtement ramifié de la sphère. En appliquant le théorème d'irréductibilité de Hilbert, on résout ainsi une forme « faible » du problème de Galois inverse : étant donné un groupe de symétries, il existe une équation dont les solutions ont les symétries prescrites, mais dont les coefficients ne sont cependant pas nécessairement rationnels (par exemple, ils peuvent faire intervenir des racines carrées).

Tout l'enjeu consiste alors à essayer de démontrer que, parmi les équations dont les solutions ont des symétries données, il en existe au moins une dont les coefficients soient rationnels : cela résoudrait le problème de Galois pour le groupe en question.

Dès le dix-neuvième siècle, les mathématiciens allemands Adolf Hurwitz, Jacob Lüroth et Alfred Clebsch avaient étudié un objet géométrique, l'*espace de Hurwitz*[13], dont les points correspondent aux revêtements ramifiés de la sphère qui ont un groupe de symétries donné, qu'on fixe à l'avance.

Autrement dit, on peut étudier la géométrie d'un objet dont les points sont les équations en deux indéterminées qui ont des symétries données. **Les équations**

[11] Ici, et contrairement à ce qu'on a fait dans le reste du manuscrit, on suppose sans le dire tout revêtement connexe. Le mot *revêtement* désigne donc les revêtements ramifiés et géométriquement connexes de la droite projective.

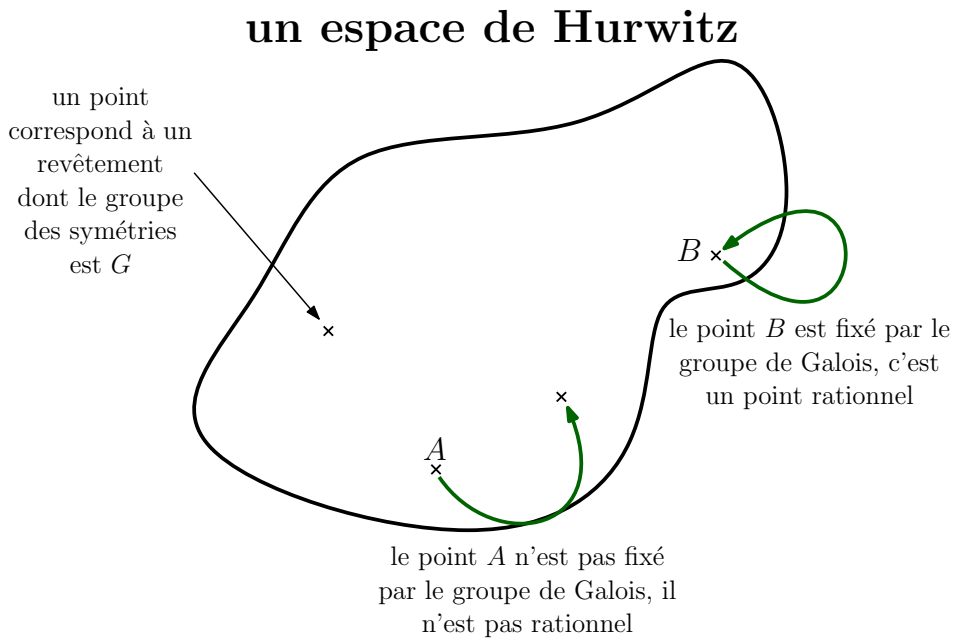
[12] Ici et dans la suite, il faut vraiment penser aux symétries *du revêtement*, c'est-à-dire celles qui préservent la première coordonnée. On n'insiste pas sur ce point.

[13] Bien qu'elle soit centrale, on passe sous silence la question des points de branchements et de leur nombre.

deviennent les *points* d'un espace géométrique qui est lui-même défini par des équations ! On peut dès lors avoir une approche de géomètre : par exemple, quand on se déplace sur l'espace de Hurwitz, on assiste à la déformation progressive d'un revêtement en un autre.

Montrer que, parmi les équations en deux indéterminées dont les symétries forment un groupe donné, il en existe une dont les coefficients soient rationnels – ce qui résout le problème de Galois inverse pour ce groupe – revient alors essentiellement à trouver des points rationnels sur l'espace de Hurwitz.

Comme dans le cas des équations en une indéterminée, cela revient à trouver sur l'espace de Hurwitz des points qui sont fixés par le groupe de Galois[14] :



[14] Il s'agit en fait ici de l'action du « groupe de Galois absolu » du corps des nombres rationnels.

Figure B.4.1.
Le problème de Galois inverse est lié à la recherche de points rationnels sur les espaces de Hurwitz

Cette approche du problème, développée depuis les années 1980 notamment par les mathématiciens John Thompson (américain), Michael Fried (américain) et Helmut Völklein (allemand), a permis la réalisation de nombreux groupes : c'est une voie riche et, encore aujourd'hui, pleine de promesses.

B.5. Mon travail

L'illustration précédente (Figure B.4.1), censée représenter un espace de Hurwitz, masque une partie de la complexité de ces espaces : en réalité, ils ne sont généralement pas « d'un seul tenant », mais sont formés de nombreuses *composantes* :

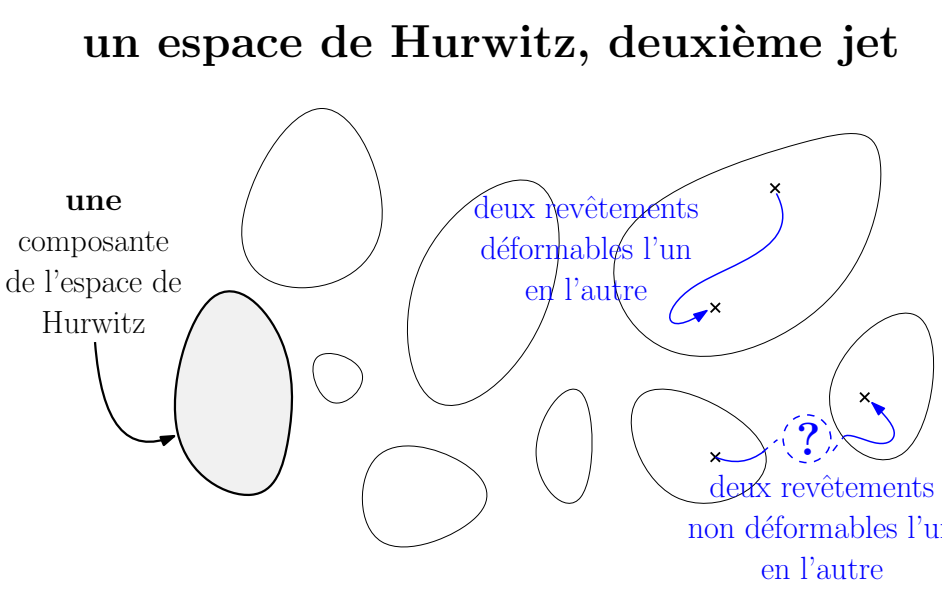
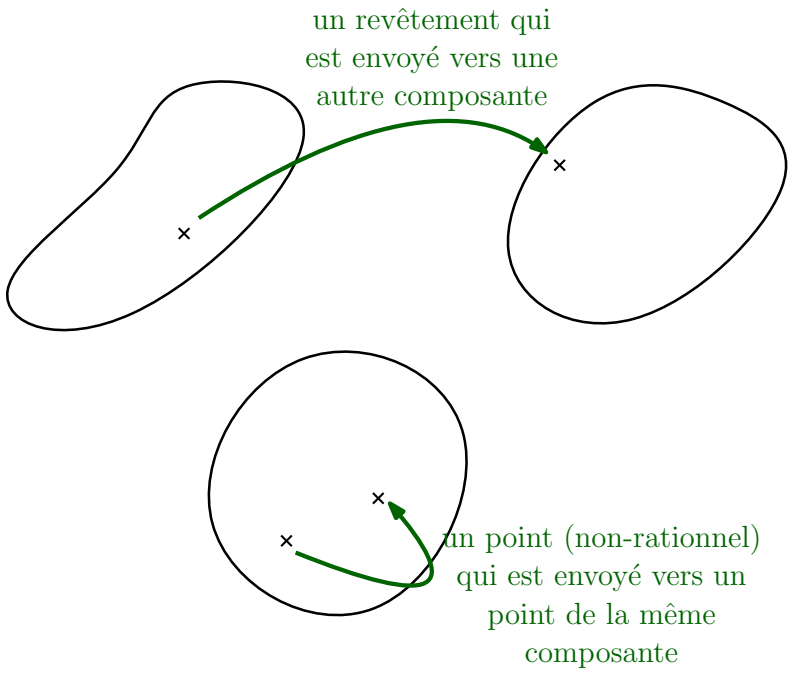


Figure B.5.1.
Un espace de Hurwitz n'est pas nécessairement en un seul morceau

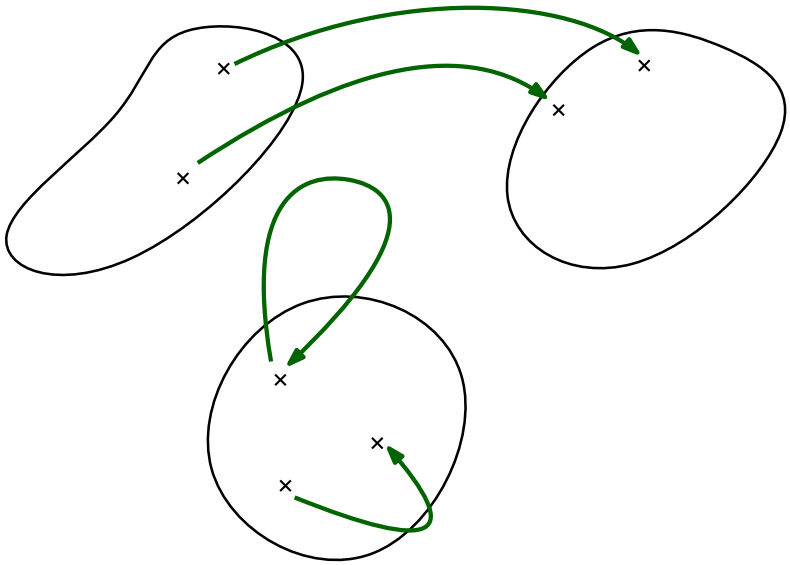
Autrement dit, étant donné deux revêtements dont le groupe des symétries est un groupe fixé G, il peut arriver qu'il soit possible de déformer l'un en l'autre (ils sont alors dans la même composante), mais il se peut aussi que ce soit impossible.

> Dans les chapitres 4 à 6, je *compte* ces composantes. Il s'agit d'une étude géométrique des espaces de Hurwitz, qui n'utilise aucun outil proprement arithmétique. Cependant, suivant la philosophie générale de la géométrie arithmétique, la connaissance de la géométrie de ces espaces est reliée aux questions arithmétiques (ici, la question de *compter les équations ayant des symétries prescrites*).

Étant donné un revêtement, rien n'assure a priori que l'action du groupe de Galois envoie ce revêtement vers un revêtement qui se trouve dans la même composante :



Une propriété intéressante est la suivante : lorsque deux revêtements se trouvent dans une même composante, le groupe de Galois les envoie nécessairement vers des revêtements qui se trouvent eux aussi dans une même composante :



Cela signifie qu'on peut parler d'une action du groupe de Galois sur les *composantes* elles-mêmes, en oubliant les revêtements :

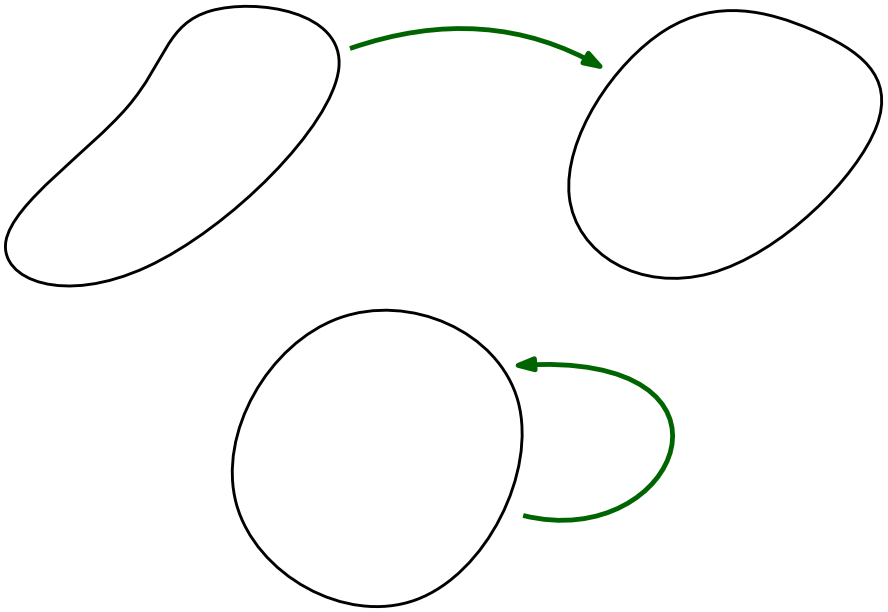


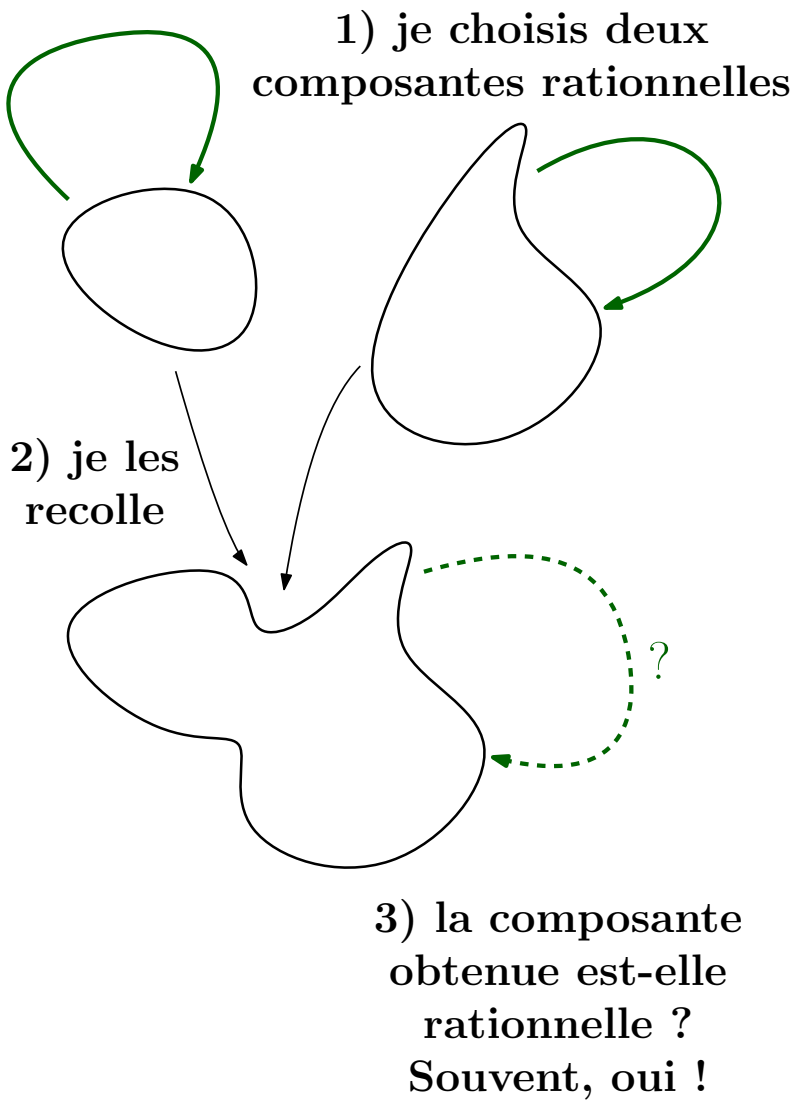
Figure B.5.2.
L'action du groupe de Galois sur les composantes

Remarquons la chose suivante : si une composante contient un point rationnel, alors elle est nécessairement fixée par le groupe de Galois (comme la composante du bas de notre exemple). On dira d'une telle composante qu'elle est *rationnelle*[15].

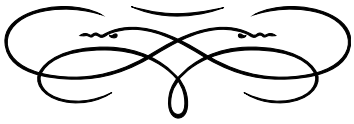
[15] Cela correspond à la notion de *composante définie sur* $\mathbb{Q}$ dans le manuscrit.

Sachant que nous cherchons des points rationnels sur les espaces de Hurwitz, on pose une question plus simple : existe-t-il toujours des composantes rationnelles ? Comment peut-on en construire ?

Dans le chapitre 8, je montre qu'il est possible de construire des composantes rationnelles d'espaces de Hurwitz en « recollant » des composantes rationnelles d'espaces de Hurwitz correspondant à des groupes de symétries plus petits.



Bibliographie



[Belo3] Paolo Bellingeri. *On presentation of Surface Braid Groups*. 2003. arXiv: math/0110129 [math.GT].

[Bia22] Andrea Bianchi. *Partially multiplicative quandles and simplicial Hurwitz spaces*. 2022. arXiv: 2106.09425 [math.AT].

[BM23] Andrea Bianchi and Jeremy Miller. *Polynomial stability of the homology of Hurwitz spaces*. 2023. arXiv: 2303.11194 [math.AT].

[BSFP14] Lior Bary-Soroker, Arno Fehm, and Sebastian Petersen. "On Varieties of Hilbert Type". In: *Ann. Inst. Fourier, Grenoble* 64.5 (2014), pp. 1893–1901. URL: http://www.numdam.org/item/10.5802/aif.2899.pdf.

[Cado4] Anna Cadoret. "Théorie de Galois inverse et arithmétique des espaces de Hurwitz". PhD thesis. Université Lille 1, 2004. URL: https://www.theses.fr/2004LIL10117.

[Cau12] Orlando Cau. "Delta-composantes des espaces de modules de revêtements". fr. In: *Journal de Théorie des Nombres de Bordeaux* 24.3 (2012), pp. 557–582. DOI: 10.5802/jtnb.811. URL: http://www.numdam.org/articles/10.5802/jtnb.811/.

[Cau16] Orlando Cau. "Delta-composantes des modules de revêtements : corps de définition". In: *Bull. Soc. math. France* 144.2 (2016), pp. 145–162. URL: https://smf.emath.fr/system/files/2017-08/smf_bull_144_145-162.pdf.

[DD97] Pierre Dèbes and Jean-Claude Douai. "Algebraic covers : field of moduli versus field of definition". In: *Annales scientifiques de l'École Normale Supérieure* 30.3 (1997), pp. 303–338.

[DE06] Pierre Dèbes and Michel Emsalem. "Harbater-Mumford Components and Towers of Moduli Spaces". In: *Journal of the Institute of Mathematics of Jussieu* 5 (2006), pp. 351 –371.

[EGA2] Alexandre Grothendieck. *Éléments de géométrie algébrique (rédigés avec la collaboration de Jean Dieudonné) : II. Étude globale élémentaire de quelques classes de morphismes*. Publications Mathématiques de l'IHÉS (Tome 8), 1961, pp. 5–222. URL: http://www.numdam.org/item/PMIHES_1961__8__5_0.pdf.

[ETW17] Jordan S. Ellenberg, TriThang Tran, and Craig Westerland. *Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and Malle's conjecture for function fields (first version)*. 2017. arXiv: 1701.04541v1 [math.NT].

[ETW23] Jordan S. Ellenberg, TriThang Tran, and Craig Westerland. *Fox-Neuwirth-Fuks cells, quantum shuffle algebras, and Malle's conjecture for function fields (second version)*. 2023. arXiv: 1701.04541v2 [math.NT].

[EVW12] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. *Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields, II*. **retracted preprint**. 2012. arXiv: 1212.0923v1 [math.NT].

[EVW16] Jordan S. Ellenberg, Akshay Venkatesh, and Craig Westerland. "Homological stability for Hurwitz spaces and the Cohen-Lenstra conjecture over function fields". In: *Annals of Mathematics* 183.3 (2016), pp. 729–786. URL: https://www.jstor.org/stable/24735176.

[FJ08] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer Berlin, Heidelberg, 2008. URL: https://link.springer.com/book/10.1007/978-3-540-77270-5.

[FN62a] Edward Fadell and Lee Neuwirth. "Configuration Spaces". In: *Mathematica Scandinavica* 10 (1962), 111–118. DOI: 10.7146/math.scand.a-10517. URL: https://www.mscand.dk/article/view/10517.

[FN62b] Ralph Fox and Lee Neuwirth. "The Braid Groups". In: *Mathematica Scandinavica* 10 (1962), 119–126. DOI: 10.7146/math.scand.a-10518. URL: https://www.mscand.dk/article/view/10518.

[Fri77] Michael D. Fried. "Fields of definition of function fields and Hurwitz families—groups as Galois groups". In: *Communications in Algebra* 5.1 (1977), pp. 17–82. ISSN: 0092-7872. DOI: 10.1080/00927877708822158.

[Fri95] Michael D. Fried. "Introduction to modular towers: Generalizing dihedral group–modular curve connections". In: *Recent Developments in the Inverse Galois Problem (Seattle, WA, 1993)*. Ed. by RI Amer. Math. Soc. Providence. Vol. 186. Contemp. Math. 1995, 111–171.

[FV91] Michael D. Fried and Helmut Völklein. "The inverse Galois problem and rational points on moduli spaces". In: *Math. Ann.* 290.4 (1991), pp. 771–800. ISSN: 0025-5831. DOI: 10.1007/BF01459271.

[Har03] David Harbater. "Patching and Galois theory". In: *MSRI Publication series* 41 (2003), pp. 313–424.

[Har77] Robin Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52. New York: Springer-Verlag, 1977. ISBN: 0-387-90244-9.

[Hos20] Timothy Hosgood. *An introduction to varieties in weighted projective space*. 2020. arXiv: 1604.02441 [math.AG].

[Hur91] Adolf Hurwitz. "Über Riemann'sche Flächen mit gegebenen Verzweigungspunkten". In: *Mathematische Annalen* 39 (1891), pp. 1–61. URL: http://eudml.org/doc/157563.

[HV96] Dan Haran and Helmut Völklein. "Galois groups over complete valued fields". In: *Israel Journal of Mathematics* 93 (1996), pp. 9–27. ISSN: 0021-2172. DOI: 10.1007/BF02761092.

[Hä22] Frank Häfner. *Braid orbits and the Mathieu group M_{23} as Galois group*. 2022. arXiv: 2202.08222 [math.NT].

[Lan20] Aaron Landesman. *Invariance of the fundamental group under base change between algebraically closed fields*. 2020. arXiv: 2005.09690 [math.AG].

[Liu95] Qing Liu. "Tout groupe fini est un groupe de Galois sur $\mathbb{Q}_p(T)$". In: *Recent developments in the Inverse Galois Problem*. Ed. by M. D. Fried. Vol. 186. Contemporary Mathematics. American Mathematical Society, 1995, pp. 261–265.

[Mar02] David Marker. *Model Theory: An Introduction*. Springer New York, NY, 2002. ISBN: 978-0-387-98760-6. DOI: 10.1007/b98860.

[RW06] Matthieu Romagny and Stefan Wewers. "Hurwitz Spaces". In: *Séminaire et Congrès* 13 (2006), pp. 313–341.

[Seg22] Béranger Seguin. *The Geometry of Rings of Components of Hurwitz Spaces*. 2022. arXiv: 2210.12793 [math.NT].

[Seg23] Béranger Seguin. *Fields of Definition of Components of Hurwitz Spaces*. 2023. arXiv: 2303.05903 [math.NT].

[Ser56] Jean-Pierre Serre. "Géométrie algébrique et géométrie analytique". In: *Annales de l'Institut Fourier* 6 (1956), pp. 1–42. ISSN: 0373-0956. DOI: 10.5802/aif.59. URL: http://www.numdam.org/article/AIF_1956__6__1_0.pdf.

[Stacks] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu. 2018.

[Sza09] Tamás Szamuely. *Galois Groups and Fundamental Groups*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2009. DOI: 10.1017/CBO9780511627064.

[Tie16] Jakob Frederik Tietz. "Homological Stability for Hurwitz Spaces". PhD thesis. Fakultät für Mathematik und Physik der Gottfried Wilhelm Leibniz Universität Hannover, 2016. URL: https://www.repo.uni-hannover.de/bitstream/handle/123456789/8928/863980716.pdf.

[Völ96] Helmut Völklein. *Groups as Galois groups*. Vol. 53. Cambridge Studies in Advanced Mathematics. An introduction. Cambridge University Press, Cambridge, 1996, pp. xviii+248. ISBN: 0-521-56280-5. DOI: 10.1017/CBO9780511471117.

[Wil19] Lucas Williams. *Configuration Spaces for the Working Undergraduate*. 2019. arXiv: 1911.11186 [math.HO].

[Woo21] Melanie Wood. "An algebraic lifting invariant of Ellenberg, Venkatesh, and Westerland". In: *Research in the Mathematical Sciences* 8 (June 2021). DOI: 10.1007/s40687-021-00259-2. URL: https://math.berkeley.edu/~mmwood/Publications/lifting.pdf.