Courbes très spéciales mais en aucun cas génériques

Emmanuel Hallouin

Mémoire écrit pour l'obtention d'une :

HABILITATION À DIRIGER DES RECHERCHES

Courbes très spéciales mais en aucun cas génériques

Présentée par :

Emmanuel Hallouin

Au vu des rapports écrits par :

Karim Belabas	Professeur, Université Bordeaux 1
David Kohel	Professeur, Université Aix-Marseille
Jürgen Klüners	Professeur, Université Paderborn

Soutenue le 12 novembre 2013, devant le Jury composé de :

Karim Belabas	Professeur, Université Bordeaux 1	rapporteur
Gerhard Frey	Professeur, Université Duisbourg et Essen	examinateur
Carlo Gasbarri	Professeur, Université Strasbourg	examinateur
David Kohel	Professeur, Université Aix-Marseille	rapporteur
Stéphane Lamy	Professeur, Université Toulouse 3	examinateur
Marc Perret	Professeur, Université Toulouse 2	parrain
Mark Spivakovsky	Directeur de Recherche, Université Toulouse 3	examinateur

Table des matières

Remerciements

La décision de soutenir une HDR a relevé, chez moi, d'un long processus de maturation. Il a d'abord fallu que je me départisse d'une autre HDR, remontant à l'époque de mes premiers pas dans la recherche, et consistant à avoir l'Habitude de Dénigrer mes Recherches. Ce temps long a eu le mérite de me laisser le loisir de faire de belles rencontres professionnelles que je souhaite évoquer ici en guise de remerciements.

Je me sens bien au département de Mathématiques et Informatique du Mirail dont je souhaite remercier les membres dans leur ensemble. Plus particulièrement, j'ai toujours plaisir à partager un repas, un café, un enseignement, une responsabilité administrative, voire parfois une idée... avec Claudie Chabriac, Sophie Ebersold, Frédéric Ferraty, Ollivier Haemmerlé, Nathalie Hernandez, Pascal Sarda, Caroline Thierry, Cassia Trojahn Dos Santos. Peut-être n'aurais-je jamais franchi le pas de l'HDR sans les encouragements bienveillants et insistants de plusieurs de ces collègues (ils se reconnaîtront sans peine). Manque à l'appel Julien Labetaa en la personne de qui je tiens bien plus qu'un collègue, puisqu'au fil des années, il s'est imposé comme un de mes amis les plus chers.

Un grand merci aussi aux nombreux étudiants que j'ai eu le privilège de côtoyer au cours de mes divers enseignements. C'est en grande partie à leur contact que je capte l'énergie nécessaire à la réflexion mathématique. Une pensée aussi aux thésards Tony Ezome, Alain Couvreur et Robin Guilbot qui m'ont témoigné leur confiance en venant régulièrement me poser des questions.

Ma première équipe de recherche était le GRIMM-algo. Cette époque fut exaltante et les liens que j'y ai tissés sont indéfectibles. Il est évident que mon parcours scientifique après la thèse doit énormément à Jean-Marc Couveignes. Ce fut un privilège de pouvoir partager au quotidien sa vision si singulière et profonde des mathématiques. J'en garde un souvenir ému et je lui suis très reconnaissant. Mon premier co-auteur, Emmanuel Riboulet-Deyris, avec qui j'ai pu découvrir la beauté des espaces de Hurwitz a su apporter les bruns de fantaisie et d'extravagance qui le caractérisent si bien ; quel luxe d'avoir pu apprendre à ses côtés ! Christian Maire a eu l'excellente idée de me proposer une collaboration sur un sujet dont ni l'un ni l'autre n'étions spécialistes, l'arithmétique des quaternions. Le bout de chemin que nous avons tracé ensemble, à cette occasion, a été riche d'enseignements et rebondissements. Christian était de surcroît un collègue dont j'appréciais particulièrement partager le quotidien.

Ces trois derniers ont quitté Toulouse mais il reste encore deux rescapés de cette époque qui comptent parmi mes collègues les plus proches. Déjà quinze ans de «co-loc» dans un bureau rendu exigu par l'encombrement de livres avec Thierry Henocq. Pas le soupçon d'une anicroche à déplorer. J'adore profiter de sa finesse d'esprit et échanger sur des sujets aussi divers que les mathématiques, l'enseignement, l'université, la politique, la vie et... la musique.

Et puis Marc Perret ! C'est peu dire que nous nous sommes rapprochés ces dix dernières années. Confronter mon point de vue algébrique (parfois poussif) à sa vision géométrique (parfois lumineuse) est un plaisir sans cesse renouvelé. Il peut arriver que la confrontation vire à la chamaillerie, mais c'est pour mieux en rire une heure après.

Depuis la disparition du GRIMM, j'ai intégré l'IMT dont je salue l'ensemble des membres. Accaparé par le Mirail, je regrette parfois de ne pas y passer plus de temps, afin de plus profiter

de Guillaume Chèze, Thomas Dedieu, Stéphane Lamy, Eric Lombardi. Merci aussi à Bin Zhang sans qui j'aurais sûrement eu beaucoup de mal à installer la distribution debian/linux sur mes ordinateurs portables successifs et à Dominique Barrère et Isabelle Nicolas pour leur disponibilité à la bibliothèque.

Il est aussi important de pouvoir s'extirper de temps en temps de son quotidien pour apporter un nouveau souffle à la réflexion. C'est l'une des raisons d'être des congrès. Tels les films, j'ai une certaine préférence pour ceux que l'on peut qualifier d'intimistes. À ce titre, j'ai eu la chance de pouvoir régulièrement participer aux «Petits groupes de travail en algèbre effective» organisés, en petit comité, par Henri Lombardi au CIRM ; merci à lui !

Dans une version encore plus intimiste, les petites retraites que nous avons planifiées durant toutes ces années avec Claude Quitté, en dehors de tout système, et avec pour seul objectif de faire partager à l'autre ses derniers engouements mathématiques m'ont à chaque fois procuré beaucoup de plaisirs et fait énormément de bien. Encore merci Claude Quitté !

En ce qui concerne l'HDR proprement dite, merci à Michèle Antonin et à Jocelyne Picard pour leurs soutiens administratif et logistique. Du point de vue scientifique, le choix des rapporteurs est évidemment une des étapes cruciales d'une HDR. Karim Belabas, Jürgen Klüners et David Kohel m'ont fait l'honneur d'accepter la tâche de rapporter mon travail. Un grand merci à eux ! Je remercie aussi chaleureusement Gerhard Frey, Carlo Gasbarri, Stéphane Lamy, Marc Perret, Mark Spivakovsky qui ont bien voulu se joindre à deux de mes rapporteurs pour former mon jury.

Les mathématiques ayant bien des fois débordées dans ma vie privée, qu'il me soit permis une petite intrusion à caractère strictement privé dans ce morceau de vie professionnelle. Je tiens à saluer mes amis, mes parents et bien sûr Corinne et Lola, «mes gonzesses, celles que j'suis avec, mes princesses, celles que j'suis leurs mec et père»...

Enfin merci à Nanni Moretti qui, au prix d'un bilan carbone personnel catastrophique, ne cesse d'arpenter mon fond d'écran sur son inoubliable Vespa, depuis la sortie de son non moins inoubliable «Journal intime»...

Introduction

Si j'ai toujours été sensible à la beauté des exemples en mathématiques, je n'avais pas conscience, avant de rédiger ce mémoire, que cet intérêt pour les exemples relevait chez moi de l'obsession [1] ! Oui, la majeure partie de mes travaux de recherches réside dans le calcul ou l'explicitation d'exemples. Selon moi, l'un des critère de beauté d'un exemple en mathématique est son caractère explicite et les exemples rejoignent ainsi l'autre spécificité des mathématiques que j'affectionne, à savoir leur aspect explicite, voire algorithmique.

Cela étant, les exemples qui m'ont préoccupés sont tous issus de la théorie des nombres. Plus particulièrement, il s'agit, pour la plupart des exemples, de courbes ou de revêtements de courbes possédant des propriétés spéciales pour ce qui est de leur groupe de Galois, ou de leur module, ou de leur corps de définition, ou encore de leur nombre de points quand elles sont définies sur un corps fini. Hormis la fascination pour les exemples, le fil conducteur de mon travail reste donc l'arithmétique des courbes au sens large.

La vérité, c'est que ce ne sont pas les exemples en eux-mêmes qui m'intéressent mais plutôt ce qu'ils révèlent ou illustrent comme phénomène. C'est aussi par le biais d'exemples, que j'ai appris et compris ce que je sais des mathématiques.

L'illustration [2] la plus frappante de cette façon d'aborder les mathématiques réside dans mes travaux sur les espaces de Hurwitz. Les théories des espaces de modules et plus particulièrement des espaces de Hurwitz relèvent de constructions assez éthérées, rarement explicites au premier abord. Il s'est passé trente ans entre l'une des premières apparitions des espaces de Hurwitz dans un article de Fulton et la proposition de méthode pour les calculer due à Jean-Marc Couveignes. C'est en développant cette méthode de calcul sur des exemples conséquents que je me suis familiarisé avec les espaces de Hurwitz. Le fait nouveau — et qui m'a permis d'être publié — d'être parvenu à produire des polynômes à groupe de Galois imposé avec la contrainte supplémentaire d'être totalement réel n'est finalement pas le plus important pour ce qui me concerne.

Le dernier exemple [3] en date de théorie que j'ai pu appréhender par le biais d'un exemple est celle des champs et des gerbes. J'ai bien évidemment eu l'occasion d'écouter des séminaires où il était question de champs ; j'ai même essayé de lire un peu de littérature sur le sujet. Mais en vain. C'est à nouveau un exemple assez simple mais non trivial qui m'a permis de forcer les portes de ce domaine et de mieux comprendre les ressorts algébriques sous-jacents à un champ. L'exemple en question est celui du champ, puis éventuellement de la gerbe, des «modèles» (au sens large) d'une variété. Avec Jean-Marc Couveignes, nous avons dû avoir recours à ce champ afin d'établir des résultats de stabilité de propriétés de modules ou de définition lors de constructions géométriques. Ces dernières ont pour but de passer d'une obstruction globale à la descente dans la catégorie des revêtements de courbes au même type d'obstruction mais dans la catégorie des courbes projectives lisses. Le point de vue que nous avons choisi pour aborder ces questions d'obstructions s'inscrit donc encore dans une démarche basée sur des exemples explicites. Notre approche se distingue ainsi de l'approche cohomologique qui a eu certains succès mais qui ne

1. Assurément, si je suivais une analyse, il faudrait que j'évoque cette obsession avec mon analyste, ce qui ne manquerait pas de sel pour quelqu'un qui se considère plutôt comme un algébriste.
2. J'aurais pu dire exemple, mais depuis que cette obsession s'est révélée à moi, j'essaye de me soigner.
3. La rechute me guette déjà !

s'est pas révélée source de beaucoup d'exemples.

Le seul aspect de mon travail qui relève, certes de la «dimension 1», mais pas stricto sensu de l'arithmétique des courbes est la collaboration avec Christian Maire sur l'étude de la simplification dans les algèbres de quaternions totalement définies sur un corps de nombres. Mais, c'était sans compter sur la théorie des courbes de Shimura qui est venue de façon inattendue (pour moi) jeter un pont entre le monde des espaces de Hurwitz et le monde des quaternions. Toujours est-il que la raison pour laquelle nous nous sommes intéressés à ces algèbres n'avait rien à voir avec les courbes au départ. Il s'agit encore d'exemples, mais l'enjeu n'est plus d'en détricoter un en particulier mais plutôt de dresser la liste exhaustive de tous les exemples d'ordre d'Eichler dans une algèbre de quaternions totalement définie sur un corps de nombres qui possèdent la propriété de simplification. La finitude de cet ensemble est un résultat de Vignéras. Cela m'a permis de me familiariser avec un autre aspect des mathématiques explicites, à savoir la tabulation de famille d'objets, les objets étant en l'occurrence des corps de nombres dans ce travail.

Enfin, à ma grande surprise, mon travail le plus récent, en collaboration avec Marc Perret, est parti du constat que dans l'étude de l'asymptotique des tours de courbes sur un corps fini, il y a pléthore d'exemples, mais assez peu d'études d'ordre général[4]. La démarche est donc presque inverse de celle prédominant à mes premiers travaux et consistant à me fixer des contraintes et à essayer de calculer un objet les satisfaisant. Au contraire nous sommes ici partis des nombreux exemples de bonnes tours asymptotiques (en général dues à Garcia et Stichtenoth plus certains co-auteurs) et nous essayons de mieux comprendre les raisons pour lesquelles une tour est asymptotiquement bonne ou pas. Nous nous sommes, pour l'instant, restreint au cadre des tours dites récursives et avons introduit un graphe facilitant leur étude et permettant de montrer une de leurs spécificités. Ce dernier travail m'a aussi procuré une petite satisfaction personnelle : j'ai pu ré-investir une partie de ma thèse sur le calcul de clôtures intégrales en dimension 1. Comme si un cycle commençait à se fermer dans ma modeste vie mathématique...

Organisation du mémoire. — Il comporte six chapitres répartis comme suit.

Le premier constitue une notice bibliographique sur ma vie d'enseignant-chercheur. J'y évoque mes principales activités administrative, d'enseignement et de recherche depuis ma nomination comme maître de conférences à Toulouse.

Le second est dédié à mes activités d'enseignement. Comme c'est une partie de mon métier que j'affectionne particulièrement, je tenais à ce que cette activité soit évoquée un peu en détail ici.

Enfin, le cœur du mémoire est regroupé dans les quatre derniers chapitres où sont décrits les quatre axes de recherche que j'ai développés depuis ma thèse. Pour chacun des thèmes abordés, outre le résumé des principaux résultats, j'ai choisi de raconter parfois certains à-côtés, parfois un bref état de l'art, ou encore parfois les derniers développements du sujet. Enfin chaque thème se termine par un volet «perspectives» constituant autant de pistes de recherches pour le futur.

4. Trop d'exemples tue l'exemple.

Chapitre 1

Curriculum Vitae

Ce chapitre est une notice bibliographique sur ma vie d'enseignant-chercheur principalement depuis la thèse.

Après les renseignements administratifs d'usage (§ 1.1) et un bref rappel de mon cursus universitaire (§ 1.2), je décris le contexte universitaire et scientifique dans lequel j'ai évolué depuis ma nomination comme maître de conférences à l'Université Toulouse 2 (§ 1.3).

Ensuite, j'évoque les responsabilités administratives qui m'ont été confiées (§ 1.4).

Enfin, je décris sommairement les deux activités principales au cœur de mon métier, à savoir l'enseignement (§ 1.5) et la recherche (§ 1.6). Je reviens en détails sur ces travaux dans le reste du mémoire.

1.1 Situation individuelle

Nom : Hallouin

Prénom : Emmanuel

Né le : 25 juin 1971 à Poitiers

Nationalité : française

Situation actuelle : Maître de Conférences à l'Université Toulouse 2

Laboratoire : Institut de Mathématiques de Toulouse (IMT)

Adresse personnelle :
1, rue Delacroix
31000 Toulouse
Tél : 05 34 42 97 59

Adresse professionnelle :
Université Toulouse 2
5, allées Antonio Machado
31058 Toulouse cedex 09
Tél : 05 61 50 48 93

e-mail : `hallouin@univ-tlse2.fr`

web : `http://www.math.univ-toulouse.fr/~hallouin/`

1.2 Formation initiale

1991-1992	Licence de Mathématiques pures (mention TB)	
1992-1993	Maîtrise de Mathématiques pures (mention B)	
1993-1994	D.E.A de Mathématiques pures (mention B)	
	Agrégation de Mathématiques (103-ème sur 415)	
1995-1998	Thèse	
	Directeur :	Claude Quitté
	Lieu :	Université de Poitiers
	Titre :	«Calcul de fermetures intégrales en dimension 1 et factorisation.»
	Soutenue le :	7 décembre 1998
	Mention :	Très honorable
	Président :	Pierre Torasso, Pr., Université de Poitiers
	Rapporteurs :	Jean-Marc Couveignes, Pr., Université de Toulouse 2
		David Ford, Pr., Univserité Concordia Montreal
	Examinateurs :	Dominique Duval, Pr., Univserité de Limoges
		Annie Page, Pr., Université de Poitiers

1.3 Notice bibliographique à partir de la thèse

J'ai commencé ma thèse sous la direction de Claude Quitté à l'Université de Poitiers en septembre 1995. Après avis favorables des rapporteurs David Ford et Jean-Marc Couveignes, je l'ai soutenu le 7 décembre 1998 ; elle s'intitule «Calculs de clôtures intégrales en dimension 1 et factorisation». J'ai ensuite été recruté Maître de Conférences à l'Université Toulouse 2 (UT2, l'Université de Lettres & Sciences Humaines et Sociales) en septembre 1999 et je continue à occuper ce poste aujourd'hui.

Un an avant mon arrivée à l'UT2, Jean-Marc Couveignes y était recruté Professeur. Il a beaucoup œuvré pour mon recrutement à Toulouse 2 et a, en parallèle, monté un projet d'équipe d'accueil qui a été accepté. Le Groupe de Recherche en Informatique et Mathématiques du Mirail (GRIMM) est né juste avant ma nomination ; cette équipe d'accueil fédérait la majeure partie des scientifiques en poste à l'UT2 qui se répartissaient dans les sections CNU 25, 26, 27 et 61. Avec Jean-Marc Couveignes et Thierry Henocq nous formions la sous-équipe GRIMM/Algo dont la spécialité était la théorie algorithmique des nombres. Le début de la période GRIMM a été exaltante et c'est une grande chance d'avoir pu participer à son expansion durant les premières années. Cette époque a culminé avec les recrutements, en septembre 2002, de deux nouveaux Professeurs à l'UT2, Christian Maire et Marc Perret, pour renforcer la composante GRIMM/Algo. Nous disposions alors de moyens humains conséquents permettant une vie scientifique. Nous étions aussi aidés par des sources de financement confortables comme des contrats de veille technologique avec le CELAR (porteur Couveignes) et comme des financements type ACI (porteurs Couveignes puis Perret).

En septembre 2006, l'aventure du GRIMM s'interrompt brutalement. L'équipe a été dissoute et nos instances dirigeantes ont fortement recommandé à ses membres d'intégrer les deux gros laboratoires de Mathématiques et d'Informatique de Toulouse. Même si j'ai regretté la disparition du GRIMM, c'est sans état d'âme que j'ai demandé l'intégration à l'Institut de Mathématiques de Toulouse (IMT) dès l'officialisation de la disparition de l'équipe d'accueil. Cette intégration s'est bien passée et je dois reconnaître avoir été bien accueilli dans ma nouvelle équipe. J'ai désormais un bureau dans les locaux de l'IMT situés sur le campus de l'Université Toulouse 3 (UT3, l'Université des Sciences & Technologies) comme tout enseignant-chercheur. Je partage donc mon temps entre le département de Mathématiques-Informatique de l'UT2 et l'IMT à l'UT3.

Je vis assez bien cette dichotomie.

1.4 Responsabilités administratives

Depuis ma nomination comme maître de conférence, plusieurs responsabilités de type administratives m'ont été confiées. Je les détaille ici et n'y reviendrai plus.

Tout d'abord, je conçois mon métier comme une alternance de périodes durant lesquelles j'occupe des responsabilités collectives énergivores avec des périodes de quasi abstinence de responsabilités. D'un côté, la préservation de la collégialité nécessite un engagement de chacun, mais de l'autre la recherche exige aussi des périodes qui lui sont quasiment intégralement dédiées. D'autre part, de la même façon que je pense qu'un turnover est bénéfique pour ce qui est des enseignements, je crois qu'il en est de même pour les responsabilités collectives.

J'ai distingué deux types de responsabilités, celles d'ordre pédagogique — et donc au plus près de mon métier — et les autres que j'ai qualifiées de «collectives» car résultant de la gestion collégiale des universités.

1.4.1 Responsabilités d'ordre pédagogique

La principale responsabilité pédagogique dont j'ai eu la charge est celle de (co-)responsable de la licence MIASHS pendant huit ans.

Licence MIASHS [2000-2008]. — Entre 2000 et 2008, j'ai été co-responsable de la licence MIASHS (ex MASS). Ce type de responsabilité regroupe un certains nombre de tâches. Des tâches purement organisationnelles allant de la l'organisation de la réunion d'accueil des étudiants, à la confection des emplois du temps et à la répartition des services. Des tâches plus spécifiquement pédagogiques à l'occasion de la rédaction des demandes d'habilitation (j'ai participé à trois vagues d'habilitation). Il s'agit de concevoir les programmes, de répartir les enseignements en Unité d'Enseignements (UE) et d'essayer de se conformer à la maquette générale des diplômes fixée à l'UT2. Ce dernier point a nécessité un certain nombre d'entrevues avec le VP CEVU ; en effet la licence MIASHS relevant du domaine Sciences & Technologies, elle ne rentre pas dans le cadre général d'une licence du domaine Lettres & Sciences Humaines (elle comporte beaucoup plus d'heures).

Toujours du point de vue plus organisationnel, j'ai été amené à gérer plusieurs situations de crise. L'Université du Mirail est réputée pour ses blocages du campus lors de mouvements étudiants. En tant que responsables de filières, durant ces périodes troubles, nous nous donnions pour objectif de garder le contact avec les étudiants ; ce ne fut pas toujours chose aisée. En 2001, l'explosion de l'usine AZF à Toulouse est intervenue une petite semaine après la rentrée universitaire. Le campus du Mirail étant en grande partie dévasté, nous avons dû organiser la délocalisation de toute la licence sur d'autres sites.

Enfin en tant que responsable, on peut essayer d'influer sur le cours des choses et de faire progresser la filière. Je suis par exemple assez fier d'avoir imposé, avec mes collègues co-responsables, la règle des quatre ans selon laquelle un enseignant qui a assuré le même enseignement pendant quatre ans n'est plus prioritaire pour cet enseignement. Dans la filière MIASHS, cela a eu le résultat escompté : les enseignements de mathématiques tournent désormais régulièrement, créant le mouvement nécessaire pour une plus forte émulsion.

Les mathématiques en ICE [2010-]. — Depuis maintenant trois ans, je suis superviseur des enseignements de mathématiques dans la filière L3 MIASHS-Info et du Master ICE. Je reconnais que cette tâche n'est pas très pesante. Cela consiste essentiellement à trouver des intervenants pour une centaine d'heures.

1.4.2 Responsabilités collectives

La principale responsabilité collective que j'ai occupée est celle de co-directeur adjoint du département de Mathématiques-Informatique du Mirail durant un an et demi.

Directeur adjoint du département de Mathématiques-Informatique de l'Université Toulouse 2 [2011-2012]. — En Janvier 2011, Caroline Thierry, la directrice adjointe du Département Mathématiques-Informatique du Mirail souhaite se retirer pour raisons personnelles. Le directeur, Ollivier Haemmerlé, me propose de la remplacer. J'accepte mais en binôme avec mon proche collègue Thierry Henocq. Je suis plus particulièrement en charge du budget. Ce dernier est assez conséquent grâce à la taxe professionnelle, et au fait que la formation ICE est en alternance. C'est ma première réelle confrontation avec les règles de gestion des finances publiques. J'apprends énormément. Je suis aussi quelques dossiers de très près, comme celui de l'instauration de la formation C2i au sein de l'UT2. C'est l'occasion de nombreuses tractations avec les services centraux, notamment les VP Moyens et CEVU. Je prends un certain plaisir à faire pencher certains arbitrages en notre faveur.

Enfin quelques autres responsabilités, plus anecdotiques en terme d'investissement, mais qui me tiennent néanmoins à cœur.

Conseil du département de Mathématiques-Informatique du Mirail [2000-]. — Peu après ma nomination à l'UT2, j'ai été élu au conseil du Département Mathématiques-Informatique du Mirail. Je le suis sans discontinuer depuis. J'ai assisté à la quasi totalité des conseils de département, m'y exprimant très régulièrement.

Membre du conseil de bibliothèque de l'IMT. — Amoureux des livres (de mathématiques mais pas seulement), les questions relatives à la documentation m'ont toujours intéressées. Quand l'équipe GRIMM existait encore, il se trouve que notre relative aisance financière nous permettait d'apporter une modeste contribution au budget de la bibliothèque de l'IMT. Cela nous semblait logique dans la mesure où tous les chercheurs en mathématiques de cette équipe utilisaient les ressources documentaires de cette bibliothèque. En retour, il a été proposé qu'un membre de GRIMM intègre le conseil de la bibliothèque. Je me suis proposé. J'y suis resté quand bien même l'équipe GRIMM a disparu.

GDR. — Je suis responsable du nœud toulousain du GDR «Structuration de la théorie des nombres» (GDR 2251) dirigé par Emmanuel Royer

1.5 Activités d'enseignements

Depuis ma nomination maître de conférences à l'UT2, mes enseignements se répartissent entre quatre types de formations selon la proportion (approximative) suivante :

Licence MIASHS (Mathématiques Informatique Appliquées et Sciences Humaines et Sociales)	UT2	50%
Master ICE (Informatique Collaborative pour l'Entreprise)	UT2	30%
Licence de Psychologie	UT2	5%
Master Mathématiques pour l'enseignement des mathématiques et préparations aux concours	UT3	15%

Je décris plus précisément le cadre de ces différents enseignements dans le chapitre 2.

1.6 Activités de recherche

Mon domaine de recherche est la théorie algorithmique des nombres et des corps de fonctions. En maîtrise Claude Quitté, que j'ai comme enseignant en TD d'algèbre, me sensibilise avec les aspects explicites des mathématiques. Je suis immédiatement séduit et attiré par ce type de mathématiques, d'où mon choix de faire une thèse dans le domaine du calcul formel sous la direction de Claude Quitté. Durant la thèse, je dévie progressivement et légèrement du calcul formel vers la théorie algorithmique des nombres. Je prends conscience que l'avènement des ordinateurs a permis aux mathématiques de revêtir un caractère expérimental que j'apprécie. D'autre part, les préoccupations explicites permettent de désacraliser des notions ou concepts mathématiques subtils. De façon anecdotique j'aime à raconter que j'ai appris ce qu'est le genre d'un corps de fonctions, en thèse, en lisant le code source du langage de calcul formel Axiom. Plus sérieusement, c'est par le biais de calculs d'exemples plus ou moins explicites que je suis parvenu à me familiariser avec certains concepts mathématiques, comme par exemple les espaces de modules, les algèbres de quaternions, la théorie des champs et des gerbes.

J'espère que mon goût pour les mathématiques explicites transparaît dans mon travail.

1.6.1 Bref descriptif des travaux

Plus précisément, je peux dégager quatre axes de réflexions. Je reviens sur ces quatre thèmes en détail dans les chapitres 3, 4, 5, 6, mais voici brièvement de quoi il s'agit.

Anneaux d'entiers en dimension 1 [Hal01, HM06]. — Ma thèse porte sur le calcul de clôture intégrale en dimension 1. J'y revisite un algorithme de calcul de base d'entiers, appelé round4, et dû à Zassenhaus. J'ai dégagé le cadre général adéquat pour cet algorithme et montré le lien entre les calculs de base d'entiers locales, de factorisations des idéaux et de factorisations des polynômes à coefficients dans un anneau de valuation discrète complet.

Plus tard, je me suis à nouveau intéressé aux anneaux d'entiers en dimension 1 mais dans le monde non commutatif par l'intermédiaire des algèbres de quaternions. Avec Christian Maire nous avons énuméré tous les genres des ordres d'Eichler possédant la propriété de simplification dans une algèbre de quaternions totalement définie. Ce travail met un point final à une question soulevée par Vignéras en 1976.

Espaces de Hurwitz et problème inverse de Galois explicite [HRD03, Hal05, Hal09]. — A mon arrivée à Toulouse, je me suis intéressé à certains aspects du problème inverse de Galois. Depuis un article fondateur de Fried et Völklein, on connaissait le lien entre ce problème inverse et celui de trouver des points rationnels dans des espaces de Hurwitz. Ces espaces sont des espaces de modules de revêtements de la droite projective. Après qu'ils aient été intensément étudiés du point de vue théorique, Couveignes proposait une nouvelle méthode pour calculer ces espaces ainsi que les familles associées. Je me suis attaché à mettre en œuvre cette méthode sur des exemples conséquents. Trois articles témoignent de ce versant de mon travail.

Avec Emmanuel Riboulet-Deyris (alors étudiant en thèse sous la direction de Couveignes), nous avons calculé la famille des revêtements de groupe de Galois S_n, ramifiés en quatre points avec inertie fixée. Cette famille était connue pour avoir des éléments possédant des fibres totalement réelles. Nous en déduisons des exemples de polynômes à coefficients rationnels, totalement réels, et de groupe de Galois S_n. C'est le premier exemple conséquent de famille de revêtements calculée par déformation d'un de ses éléments dégénérés.

Dans la même mouvance, je me suis intéressé à la famille des revêtements de degré 9, de groupe de Galois $\mathrm{PSL}_2(\mathbb{F}_8)$ avec inertie fixée. Cette famille était elle aussi connue pour contenir des éléments possédant des fibres totalement réelles.

En écoutant un exposé d'Elkies, j'ai réalisé que les deux mondes précédents, celui des espaces de modules de courbes et celui des algèbres de quaternions, sont deux pierres d'achoppement

des courbes de Shimura. M'appuyant sur l'exemple précédent, j'ai calculé un modèle explicite du modèle canonique d'une certaine courbe de Shimura, allongeant ainsi la liste des modèles explicites calculés par Elkies.

Obstructions à la descente [CH11]. — Grâce à l'étude des espaces de Hurwitz, j'ai été sensibilisé aux questions de corps des modules et de définitions des revêtements de courbes. Il se pose assez naturellement la question de savoir si ces deux corps coïncident. La réponse à la question est non en général et si tel est le cas, on dit qu'il y a une obstruction à la descente. L'étude de ces obstructions dans le cadre des revêtements fait l'objet de nombreuses publications dans les années 1990-2000 (cf. Harbater, Coombes, Fried, Dèbes, Douai, Couveignes, etc...). La zoologie des obstructions dans la catégorie des revêtements est maintenant assez complète.

Il n'y a évidemment pas lieu de restreindre cette question aux revêtements et la question de savoir si une courbe ou une variété est définie ou non sur son corps des modules est pertinente. Dans ces catégories, il faut reconnaître que le panel d'exemples est beaucoup plus restreint. L'objet de cette collaboration avec Couveignes a été de produire un exemple d'obstruction dite «globale» à la descente dans le cadre des courbes lisses absolument irréductibles sur les rationnels. L'idée a consisté à partir d'une telle obstruction dans la catégorie des revêtements et de proposer des constructions géométriques permettant de passer d'une catégorie à une autre.

Tours de corps de nombres ou de fonctions [HP08, HP13]. — Avec Perret, nous avons tenté de donner un critère cubique, à la Golod-Shafarevich, pour l'infinitude de la tour de corps de classes d'un corps de nombres. Nous n'avons pas atteint notre but initial, mais j'ai beaucoup appris scientifiquement à l'occasion de ce travail, notamment la cohomologie des corps de nombres.

Plus récemment et avec plus de succès, nous nous sommes intéressés aux tours récursives de corps de fonctions sur un corps fini conduisant à une minoration non triviale de la célèbre constante :

$$A(q) = \liminf_{g\to\infty} \frac{N_q(g)}{g} \qquad \text{où} \qquad N_q(g) = \max_{\substack{X/\mathbb{F}_q \text{ courbe, proj., lisse} \\ \text{genre de } X = g}} \sharp X(\mathbb{F}_q).$$

Si les exemples se font assez rares pour les obstructions du paragraphe précédent, dans cette mouvance là, les exemples fourmillent. Une majorité d'entre eux sont dûs à Garcia et Stichtenoth. Leur succès le plus frappant reste l'exemple de tour modérée conduisant à la preuve de l'égalité $A(q) = \sqrt{q} - 1$ pour q carré. Une telle tour est donnée par une correspondance sur une courbe dite de base. Par exemple, si la courbe de base est la droite projective, la donnée de la correspondance est équivalente à celle d'un polynôme bi-homogène. Notre but est de comprendre en profondeur les raisons pour lesquelles une tour est bonne. Pour cela, nous nous appuyons sur un graphe orienté inifini assez naturellement attaché à la tour. Mélangeant des résultats de géométrie des surfaces, de théorie des graphes et de théorie spectrale des matrices positives, nous sommes déjà parvenus à prouver une spécificité de ces tours récursives. Nous avons bon espoir de pouvoir aller plus loin dans cette direction.

1.6.2 Publications

Toutes mes publications sont accessibles sur ma page web, à l'adresse

`http://www.math.univ-toulouse.fr/~hallouin/eh-travaux.html`

On y distingue 6 publications dans des revues internationales, 1 proceeding [5] et 1 article soumis avec un premier rapport positif joint [8]

[1] Emmanuel Hallouin. «Computing local integral closures.», *J. of Symbolic Computation*, 32(3), 211–230, 2001.

[2] Emmanuel Hallouin & Emmanuel Riboulet-Deyris. «Computation of some moduli spaces of covers and explicit S_n and A_n regular $\mathbb{Q}(T)$-extensions with totally real fibers.», *Pacific J. Math.*, 211(1) :81–99, 2003.
[3] Emmanuel Hallouin. «Study and computation of a Hurwitz space and totally real $\mathrm{PSL}_2(\mathbb{F}_8)$-extensions of $\mathbb{Q}$.», *J. Algebra*, 292(1) :259–281, 2005.
[4] Emmanuel Hallouin & Christian Maire. «Cancellation in totally definite quaternion algebras.», *J. Reine Angew. Math.*, 595 :189–213, 2006.
[5] Emmanuel Hallouin & Marc Perret. «On generators of the group $\hat{H}^{-1}(\mathrm{Gal}(L/K), E_L)$ in some abelian p-extension L/K.», *Algebraic Geometry and its applications*, éditeurs : J.Chaumine, J.Hirschfeld, R.Rolland ; Series on Number Theory and its Applications Vol. 5, World Scientific, 2007.
[6] Emmanuel Hallouin. «Computation of a cover of Shimura curves using a Hurwitz space.», *J. Algebra*, 321(2) :558–566, 2009.
[7] Jean-Marc Couveignes & Emmanuel Hallouin. «Global descent obstructions for varieties.», *Algebra Number Theory*, 5(4) :431–463, 2011.
[8] Emmanuel Hallouin & Marc Perret. «Recursive towers of curves over finite fields using graph theory.», soumis, 2013.

Chapitre 2

Activités d'enseignements

J'aime enseigner. J'ai aimé dès mon stage d'agrégation et mon plaisir ne s'est pas du tout émoussé depuis. Je trouve que l'activité d'enseigner s'allie très bien avec celle de la recherche. La première activité est un échange, une transmission, la seconde est purement cérébrale, plus solitaire, presque monacale parfois. Je ne conçois pas de me livrer à l'une de ces activités sans l'autre.

Avant de décrire plus précisément les divers types d'enseignements que j'ai dispensés, je signale que la plupart des documents que je distribue aux étudiants sont accessibles sur ma page web :

`http://www.math.univ-toulouse.fr/~hallouin/`

2.1 Licence MIASHS (ex MASS)

Depuis mon arrivée à Toulouse, j'effectue la majeure partie de mon service d'enseignement (au moins 100 heures annuelles) dans la licence de Mathématiques Informatique appliquées et Sciences Humaines et Sociales (MIASHS, ex MASS). C'est une licence du domaine sciences et technologies donnant une solide formation en mathématiques et informatique doublée d'une ouverture vers une discipline de sciences humaines et sociales (d'où son ancrage à l'UT2 qui est une Université de Lettres et Sciences Humaines).

Le public est assez varié puisque nous recrutons des bacheliers S, mais aussi ES, et même beaucoup plus rarement L. Nous avons la chance de fonctionner avec des effectifs raisonnables pour un premier cycle universitaire. Je parviens donc assez vite à connaître tous les étudiants (je ne parle que de ceux qui viennent en cours). Il en résulte un contact assez privilégié et chaleureux avec ces étudiants et je prends beaucoup de plaisir à enseigner dans cette filière.

J'y dispense des cours et travaux dirigés de mathématiques standards pour un premier cycle universitaire. Tous ces enseignements sont proposés comme enseignement à distance via le Service d'Enseignement à Distance (SED) ; cela a nécessité un investissement important dans la rédaction de polycopiés de cours et de recueils d'exercices avec corrections. Depuis peu, j'essaye de diversifier les modes d'enseignement, alternant entre des séances de cours, des séances de cours en groupe, des séances de travaux dirigés classiques ou d'autres assistées d'ordinateurs. J'ai notamment utilisé la base d'exercices interactifs libres et gratuits WIMS. Je souhaite continuer dans cette voie là.

Comme je ne garde pas un enseignement plus de quatre ans, je suis intervenu dans une grande partie des Unités d'Enseignement de mathématiques des deux premières années. Voici le détail :

Licence MIASHS	Type d'enseignements	Contenu
1-ère année		
Algèbre 1-er semestre	Cours, TD, SED	Arithmétique des entiers et des polynômes, fractions rationnelles
Algèbre 2-ème semestre	Cours, TD, SED	Algèbre linéaire, applications linéaires, déterminants
2-ème année		
Algèbre 3-ème semestre	TD, SED	Réduction des endomorphismes, Espace euclidien, Isométries
Analyse 3-ème semestre	TD, SED	Espace vectoriel normé, suites, séries, suites de fonctions
Analyse 4-ème semestre	TD, SED	Séries entières, séries de fonctions, séries de Fourier, fonctions de plusieurs variables

2.2 Master ICE

L'autre versant des mes enseignements à l'UT2 (pour environ 60 heures) relève des mathématiques discrètes en L3 MIASHS, parcours informatique (ex IUP) ou en M1 Informatique collaborative pour l'entreprise (ICE). L'idée est d'initier des étudiants en informatique aux mathématiques utilisées dans le domaine des sciences de l'information.

Le public est majoritairement recruté dans les IUT d'informatique. Les étudiants sont donc très à l'aise avec la machine mais peuvent se montrer réfractaires aux mathématiques. Je m'amuse beaucoup à essayer de les convaincre de l'utilité de savoir ce qui se cache derrière certaines routines informatiques qu'ils utilisent au quotidien.

Plus précisément, j'enseigne les prémices de la cryptographie. Je fais le choix de désacraliser les notions mathématiques sous-jacentes pour ne pas trop effrayer les étudiants. Ayant à faire à un public très à l'aise avec l'environnement informatique, j'en profite pour utiliser les ordinateurs lors de ces enseignements grâce à WIMS une nouvelle fois, ou à Sage un système de calcul formel libre et gratuit basé sur python.

Voici le détail des notions que j'ai abordées.

	Type d'enseignements	Contenu
L3 MIASHS-Info		
Cryptographie I	Cours & TD	Corps finis, Protocole cryptographique à clé publique, El Gamal, Primalité
Master 1 ICE		
Cryptographie II	Cours & TD	$\mathbb{Z}/n\mathbb{Z}$, RSA, Factorisation des entiers

2.3 Masters de Mathématiques à l'UT3

Si j'éprouve une satisfaction sans faille dans les précédents enseignements, il me manquait cependant le contact avec un public d'étudiants en mathématiques plus avancés. C'est pourquoi, depuis maintenant cinq ans, je complète mon service avec quelques enseignements à l'Université Toulouse 3, l'Université des Sciences & Technologies (UT3). Je suis notamment intervenu dans la préparation à l'agrégation (pour l'option C et la préparation à l'oral d'algèbre) puis plus récemment en Master 1 Mathématiques pour l'Enseignement et l'Ingénierie (MEI). Les mathématiques

explicites étant encore sous représentées dans le cursus classique, j'oriente souvent mes interventions vers ce domaine. C'est un réel plaisir de révéler à des étudiants possédant déjà une certaine culture mathématique que les objets qu'ils connaissent se calculent et se manipulent parfois très bien grâce à l'ordinateur.

Enseignements dans les divers Masters de mathématiques de l'UT3.

	Type d'enseignements	**Contenu**
M1 MEI		
Modélisation	Cours, TD, TP	Arithmétique et cryptographie
AGREG		
Option C		Corps finis, Résidus quadratiques, Primalité, Arithmétique des entiers et des polynômes
Oral d'algèbre		Diverses leçons d'algèbre

2.4 Encadrement de mémoires

J'ai encadré deux mémoires de DEA :

• en 2002, celui de Guilhem Castagnos, «Analyse d'un algorithme de factorisation d'entiers à la meilleure complexité prouvée»

• en 2008, celui de Robin Guilbot, «Présentation d'un contre-exemple à la conjecture de Malle sur le nombre de corps de discriminant borné»

En 2010, j'ai encadré le mémoire de Sophie Albenge et Paul Grudzien, étudiants en Master 1 de «Mathématiques fondamentales et appliquées» à l'UT3, sur les algèbres de quaternions. Cela s'est fait à la demande de la première étudiante qui est venue me solliciter car je l'avais eu en...L1 MIASHS. La boucle était bouclée !

2.5 Et après ?

Comment j'ai commencé à le faire depuis deux ans en licence MIASHS, je souhaite continuer à diversifier les modes d'enseignements en licence. Dans l'enseignement des mathématiques en France, peut-être avons nous trop mis l'accent sur le cours et les séances d'exercices, au détriment des travaux de recherche sur documents et des expériences en mathématiques. Dans ma vie de chercheur, je passe mon temps à étudier dans des livres et articles et à faire des expériences sur ordinateur afin d'apprendre des mathématiques et d'essayer de comprendre des phénomènes. Ces deux activités sont précisément absentes des enseignements de mathématiques. Il ne faut donc pas s'étonner de se voir rétorquer «Ah bon il reste des choses à trouver en maths», quand on avoue en société faire de la recherche en mathématiques.

Enfin, assurément, le type d'enseignement que je n'ai pas encore osé dispenser est celui d'un *encadrement en thèse*.

Chapitre 3

Simplification dans les algèbres de quaternions totalement définies

Ce travail (cf. [HM06]) est né de la volonté commune à Christian Maire et à moi même de collaborer scientifiquement. Sur une suggestion de Jacques Martinet, nous avons choisi, pour entamer cette collaboration, d'achever un travail initié par M.-F.Vignéras en 1976, et consistant à dresser la liste de tous les ordres d'Eichler d'algèbres de quaternions totalement définies qui possèdent la propriété de simplification.

Une coïncidence incroyable a voulu qu'alors que j'étais en train d'écrire les premières lignes relatant ce travail pour ce mémoire, j'ai reçu un article de D. Smertnig ([Sme13]) expliquant pourquoi la dite liste est partiellement erronée. Cet article doit à ce jour suivre le processus de référencement et n'est donc pas encore paru. Je crois néanmoins pouvoir affirmer qu'il soulève bel et bien une erreur dans notre travail. Cette erreur figure déjà dans l'article originel de Vignéras (ce qui ne nous excuse en rien). Je vais donc expliquer quelle a été notre erreur et corriger la liste reprenant ainsi les arguments de Smertnig.

3.1 Simplification dans les algèbres centrales simples

Soit K un corps de nombres, dont on note A l'anneau des entiers, et soit $\mathcal{H}$ une algèbre centrale simple sur K. Une des premières spécificités du monde *non-commutatif* par rapport au monde *commutatif* provient du fait que l'ensemble des éléments de $\mathcal{H}$ entiers sur A n'est pas un sous-anneau (c'est très facile de s'en apercevoir dès l'exemple le plus simple d'algèbre centrale simple qu'est $M_n(K)$). Néanmoins, il existe des sous-anneaux constitués d'entiers et maximaux pour cette propriété ; on les appelle les ordres maximaux de $\mathcal{H}$. Ils sont peu ou prou le pendant des anneaux d'entiers des corps de nombres (le réel pendant se trouve être une classe un peu plus large d'ordres comme on le verra dans la suite).

Soit $\mathcal{O}$ un ordre maximal de $\mathcal{H}$. La question qui nous intéresse est de savoir si cette classe d'anneaux possède ou non la propriété de *simplification* : étant donnés M et N des $\mathcal{O}$-modules de type fini, a-t-on :

$$M \oplus \mathcal{O}^n \simeq N \oplus \mathcal{O}^n \qquad \Longrightarrow \qquad M \simeq N \ ?$$

La réponse est oui pour la quasi totalité des ordres d'une algèbre centrale simple sur un corps de nombres. C'est un résultat dû à Jacobinski [Jac68, Swa70] qui peut être considéré comme l'origine de ce travail.

Théorème 3.1 (de simplification de Jacobinski (1968)) *Les ordres maximaux d'une algèbre centrale simple sur un corps de nombres possèdent la propriété de simplification...sauf si cette algèbre est une* ***algèbre de quaternions totalement définie****.*

Depuis, la réputation des algèbres qui font exceptions dans cet énoncé n'est plus à faire. Après les travaux d'Eichler, on les appelle les algèbres qui *ne* satisfont *pas* la *condition d'Eichler*[1]. Ce sont les algèbres de quaternions ramifiées en toutes les places infinies de leur centre ; nécessairement, ce dernier est totalement réel puisqu'un plongement complexe n'est jamais ramifié dans une algèbre de quaternions. Ces algèbres de quaternions et leur arithmétique constituent le coeur de ce travail.

À peine dix ans après, Vignéras ([Vig76, Théorème 4]) montrait que les ordres des algèbres de quaternions totalement définies présentent une pathologie lourde du point de vue de la simplification dans le sens où *aucun* d'entre eux ne possède la propriété de simplification *sauf un nombre fini*.

Théorème 3.2 (Vignéras (1976)) *Il n'y a qu'un nombre fini d'ordres (à isomorphisme près) d'algèbres de quaternions totalement définies qui possèdent la propriété de simplification.*

Pour achever l'histoire, il restait à dresser la liste de tous les ordres possédant la propriété de simplification. Vignéras elle même (cf. loc. cit.) ébauchait cette liste en donnant les ordres possédant la propriété de simplification dans les algèbres de quaternions de centres $\mathbb{Q}$, ou un corps quadratique ou encore certains corps cubiques. Notre travail a consisté à compléter cette liste pour la rendre exhaustive.

3.2 Petit lexique d'arithmétique des quaternions

Durant ma thèse, j'ai étudié en profondeur les anneaux d'entiers d'un corps de nombres du point de vue explicite. Je croyais être au fait de la majeure partie des merveilles relevant de l'arithmétique des anneaux d'entiers (maximaux ou non) de dimension de Krull 1. C'était sans compter sur le monde non commutatif, qui même en dimension 1, révèle une richesse que je ne soupçonnais pas. C'est aussi un domaine semé d'embûches et d'écueils à éviter. Force est de constater que je n'y suis pas intégralement parvenu.

Soit $\mathcal{H}$ une algèbre de quaternions sur un corps de nombres K dont on note A l'anneau des entiers. Dans tout ce qui suit, la mention «localement» pour les ordres, modules ou idéaux est relative aux premiers (finis) de A.

On appelle *idéal fractionnaire* de $\mathcal{H}$ un sous-A-réseau complet de $\mathcal{H}$ (i.e. $I \otimes_A K \simeq \mathcal{H}$). Un *ordre* de $\mathcal{H}$ est un idéal fractionnaire qui est aussi un sous-anneau.

On dit que deux ordres sont du même *type* si et seulement s'ils sont isomorphes (en tant qu'anneaux) ce qui, d'après le théorème de Skolem-Noether, revient à dire qu'ils sont conjugués. S'ils ne sont que localement isomorphes, on dit qu'ils sont du même *genre* ; c'est équivalent au fait qu'ils aient même discriminant (réduit). On sait qu'il n'existe qu'un nombre fini de types d'ordres dans un genre donné.

Tout idéal I a un ordre à gauche $\mathcal{O}_l(I)$ et un ordre à droite $\mathcal{O}_r(I)$ respectivement définis par :

$$\mathcal{O}_l(I) = \{x \in \mathcal{H} \mid xI \subset I\} \qquad \text{et} \qquad \mathcal{O}_r(I) = \{x \in \mathcal{H} \mid Ix \subset I\}.$$

Dans la suite la mention *idéal à gauche de* $\mathcal{O}$ ou $\mathcal{O}$-idéal est réservée aux idéaux fractionnaires I de $\mathcal{H}$ tel que $\mathcal{O}_l(I) = \mathcal{O}$. Soit I un tel idéal. C'est en particulier un $\mathcal{O}$-module et on peut donc se poser la question de savoir s'il est :

- *libre*, i.e. de la forme $\mathcal{O}x$ avec $x \in \mathcal{H}$,
- ou *stablement libre*, i.e. s'il existe $n \geqslant 1$ tel que $I \oplus \mathcal{O}^n$ est libre, ce qui revient à vérifier que $I \oplus \mathcal{O}$ est libre,
- ou *projectif*, i.e. s'il existe J un autre $\mathcal{O}$-module tel que $I \oplus J$ soit libre,

1. La raison pour laquelle Eichler avait «posé sa condition» n'est pas éloignée de nos préoccupations.

— ou *localement libre*, i.e. si pour tout premier $\mathfrak{p}$ de A, le module $S_{\mathfrak{p}}^{-1}I$ est un $S_{\mathfrak{p}}^{-1}\mathcal{O}$-module libre (où $S_{\mathfrak{p}} = A \setminus \mathfrak{p}$).

On peut aussi définir une notion d'inversibilité pour les idéaux. Toutes ces notions sont loin d'être équivalentes.

Néanmoins, on va restreindre notre cadre aux cas d'anneaux pour lesquels certaines de ces notions sont équivalentes. Il s'agit des *ordres d'Eichler* maximaux en tous les premiers ramifiés et de niveau sans facteur carré, c'est-à-dire aux ordres dont le discriminant est sans facteur carré. Ce sont ces ordres qui constituent le bon pendant aux anneaux d'entiers d'un corps de nombres dans la mesure où ce sont les ordres héréditaires de $\mathcal{H}$: tous les idéaux d'un tel ordre sont projectifs. On peut de plus prouver que les notions projectifs, inversibles ou localement libres sont équivalentes. (cf.[Brz83, Proposition 1.1], [Kap69]). Bref, les ordres d'Eichler ont les mêmes qualités qu'un anneau de Dedekind, la commutativité en moins !

3.3 «Simplification» et «Équivalence entre Stablement libre et Libre»

Pour un ordre $\mathcal{O}$, on peut donc se poser deux problèmes : celui de savoir s'il possède la propriété de simplification, et celui de savoir si ses idéaux stablement libres sont libres. Des résultats généraux montrent qu'il suffit de se poser cette question pour les idéaux (autrement dit en «rang» un).

Le troisième paragraphe de l'article de Vignéras [Vig76], commence en disant qu'un ordre $\mathcal{O}$ possède la propriété de simplification si et seulement si tout $\mathcal{O}$-idéal stablement libre est libre. Nous avons répété ce fait au début du §1.4. de notre article. Il s'avère que c'est faux comme le remarque Smertnig [Sme13] dans sa note, exemple explicite à l'appui.

Une façon de s'en convaincre est d'introduire le pendant du groupe des classes d'idéaux d'un corps de nombres. À cause de la non-commutativité, on ne peut pas naïvement singer la définition du groupe des classes d'idéaux d'un anneau d'entiers. On note :

$$\mathcal{L}(\mathcal{O}) = \{I \text{ idéal fractionnaire de } \mathcal{H} \text{ vérifiant } \mathcal{O}_l(I) = \mathcal{O}\}$$

Cet ensemble est muni de deux relations d'équivalence, la relation d'*isomorphisme standard* entre $\mathcal{O}$-modules (à gauche) :

$$I \simeq J \qquad \Longleftrightarrow \qquad \exists h \in \mathcal{H} \mid I = Jh$$

et la relation d'*isomorphisme stable* entre $\mathcal{O}$-modules :

$$I \simeq_{\text{st.}} J \qquad \overset{\text{déf.}}{\Longleftrightarrow} \qquad \exists n \geqslant 0,\ I \oplus \mathcal{O}^n \simeq J \oplus \mathcal{O}^n \qquad \Longleftrightarrow \qquad I \oplus \mathcal{O} \simeq J \oplus \mathcal{O}$$

Évidemment, la première implique la seconde mais la réciproque est fausse en général. On désigne par $[I]$ la classe d'isomorphisme d'un idéal I et par $[I]_{\text{st.}}$ sa classe stable et on introduit les deux ensembles quotients de $\mathcal{L}(\mathcal{O})$ par les deux relations d'équivalence, notés respectivement $\mathcal{C}\ell(\mathcal{O})$ et $\mathcal{C}\ell_{\text{st.}}(\mathcal{O})$. On dispose d'une application *ensembliste* surjective entre ces deux ensembles quotients :

$$\begin{array}{rccc} \mu : & \mathcal{C}\ell(\mathcal{O}) & \longrightarrow & \mathcal{C}\ell_{\text{st.}}(\mathcal{O}) \\ & [I] & \longmapsto & [I]_{\text{st.}} \end{array}$$

C'est à dessin que j'ai insisté sur le caractère *ensembliste* de cette application. En effet, encore à cause de la non commutativité, l'ensemble $\mathcal{C}\ell(\mathcal{O})$ des classes d'isomorphisme des idéaux à gauche n'est pas muni d'une loi de groupe naturelle. En revanche, le second ensemble quotient $\mathcal{C}\ell_{\text{st.}}(\mathcal{O})$ peut lui être muni d'une loi de groupe. Cela résulte du fait que pour I et I' deux $\mathcal{O}$-idéaux à gauche, on peut montrer qu'il existe J un autre $\mathcal{O}$-idéal à gauche tel que $I \oplus I' = J \oplus \mathcal{O}$. Cela permet de définir la loi de groupe comme suit :

$$[I]_{\text{st.}} + [I']_{\text{st.}} \overset{\text{déf.}}{=} [J]_{\text{st.}}$$

L'ensemble de départ n'étant pas forcément un groupe, l'application μ n'est pas, a fortiori, un morphisme de groupes.

L'application μ est injective si et seulement si deux idéaux stablement isomorphes sont isomorphes :

$$[I \simeq_{\text{st.}} J \Rightarrow I \simeq J] \qquad \Longleftrightarrow \qquad [I \oplus \mathcal{O} \simeq J \oplus \mathcal{O} \Rightarrow I \simeq J]$$

ceci pour tous $I, J \in \mathcal{L}(\mathcal{O})$. Autrement dit :

$$\mu \text{ est injective} \qquad \Longleftrightarrow \qquad \mathcal{O} \text{ possède la } \textit{propriété de simplification.}$$

Malheureusement, l'application μ n'étant pas un morphisme de groupes, on ne peut pas mesurer son injectivité en étudiant son «noyau».

Les classes $[\mathcal{O}]$ et $[\mathcal{O}]_{\text{st.}}$ sont respectivement constituées des idéaux libres et des idéaux stablement libres. Evidemment, on a $\mu([\mathcal{O}]) = [\mathcal{O}]_{\text{st.}}$ et dans l'image réciproque du neutre $[\mathcal{O}]_{\text{st.}}$, on retrouve ni plus ni moins que les classes d'isomorphismes des $\mathcal{O}$-idéaux à gauche stablement libres, si bien que :

$$\mu^{-1}\left([\mathcal{O}]_{\text{st.}}\right) = \{[\mathcal{O}]\} \quad \Leftrightarrow \quad \text{tout } \mathcal{O}\text{-idéal } \textit{stablement libre} \text{ est } \textit{libre}$$

En tout état de cause, il n'est pas vrai, a priori, que pour qu'un ordre d'Eichler satisfasse la propriété de simplification, il suffise que les idéaux stablement libres soient libres comme nous le croyons avec Vignéras. Dans sa note, Smertnig montre même que c'est faux.

Une question reste en suspens : si le théorème de «simplification» de Vignéras ([Vig76, Théorème 3]) n'est plus un théorème de simplification, que caractérise-t-il ? En examinant la preuve, on s'aperçoit facilement que ce théorème permet en fait de vérifier si les idéaux stablement libres d'un ordre d'Eichler sont tous libres. Son énoncé corrigé devient donc (la preuve, quant à elle n'a pas besoin d'être modifiée) :

Théorème 3.3 (Vignéras (1976)) *Soit K un corps totalement réel, de degré n, dont on note A l'anneau des entiers. Soit $\mathcal{H}$ une algèbre de quaternions totalement définie sur K de discriminant D et soit $\mathcal{O}$ un ordre d'Eichler de niveau N, dont on note $\mathcal{W}$ le groupe des unités de norme 1. On pose :*

$$\Phi(D, N) = \prod_{\mathfrak{p}|D} (1 - N(\mathfrak{p})) \prod_{\mathfrak{q}|N} (1 + N(\mathfrak{q}))$$

Alors pour que les idéaux stablement libres de $\mathcal{O}$ soient tous libres, il faut et il suffit que :

$$|\mathcal{W}| \times [\mathcal{O}^* : \mathcal{W}A^*] \times \Phi(D, N) = \frac{(-4\pi^2)^n [A^{*+} : A^{*2}]}{\operatorname{disc}(K)^{\frac{3}{2}} \zeta_K(2)},$$

où A^* et $\mathcal{O}^*$ désignent les groupes des unités de A et $\mathcal{O}$, A^{*+} celui des unités de A totalement positives et où ζ_K est la fonction zeta de K.

Ce résultat n'en reste pas moins un outil très puissant pour vérifier si un ordre d'Eichler satisfait ou non la propriété de simplification. En effet, il suffit de l'associer à l'observation suivante due elle aussi à Smertnig :

Lemme 3.4 (Smertnig (2013)) *Soit $\mathcal{O}$ un ordre d'Eichler dans une algèbre de quaternions totalement définie $\mathcal{H}$. Alors sont équivalentes :*

(i) l'ordre $\mathcal{O}$ possède la propriété de simplification ;

(ii) tout ordre $\mathcal{O}'$ de même genre que $\mathcal{O}$ est tel que les idéaux stablement libres sont libres.

3.4 La liste complète. . .et corrigée

Du coup, les stratégies et techniques mises en oeuvre pour dresser la liste complète dans notre article restent opérationnelles et permettent bel et bien de dresser la liste complète. En voici les principales étapes. On commence par montrer que le degré du centre d'une algèbre de quaternions contenant un ordre qui possède la propriété de simplification ne peux pas dépasser six. Ensuite, pour chaque degré compris entre un et six, on majore le discriminant du centre. Enfin, on traite au cas par cas, les centres restant en s'appuyant sur une table des corps de nombres ordonnés par discriminants, dans les degrés considérés.

3.4.1 Utilisation des bornes d'Odlyzko

Pour les deux premières étapes, on utilise de façon cruciale les bornes d'Odlyzko ([Odl76]). Pour chaque degré n, on dispose de deux bornes $\mathrm{Od}_{\mathrm{t.r.}}(n)$ ou $\mathrm{Od}_{\mathrm{t.i.}}(n)$ qui minorent respectivement les (root)discriminants d'un corps de nombres totalement réel ou totalement imaginaire de degré n. D'autre part, ces bornes peuvent être affinées dès lors que l'on fait peser des contraintes autres que le degré et la signature sur les corps de nombres considérés. Par exemple, si on impose que le corps doive contenir un ou des premiers de petites normes, alors on est en mesure de donner des minorations explicites plus fines.

Grâce au théorème 3.3 de Vignéras, on vérifie facilement qu'une condition nécessaire à la simplification pour qu'un corps de nombres K totalement réel soit le centre d'une algèbre de quaternions totalement définie à simplification est que :

$$|\operatorname{disc}(K)|^{1/n} \leqslant \pi^{\frac{4}{3}} 2^{\frac{4}{3}-\frac{2}{3n}} \left(\frac{h^+}{h}\right)^{\frac{2}{3n}}$$

où n est le degré de K sur $\mathbb{Q}$ et où h et h^+ désignent respectivement les nombres de classes et de classes au sens restreint de K.

Du coup, en appliquant les bornes d'Odlyzko à K si $h^+ = h$ ou à son extension totalement imaginaire non ramifiée de degré $\frac{h^+}{h}$, on en déduit que le corps K peut être le centre d'une algèbre de quaternions totalement définie contenant un ordre possédant la propriété de simplification, seulement si :

$$\begin{cases} \mathrm{Od}_{\mathrm{t.r.}}(n) \leqslant \pi^{\frac{4}{3}} 2^{\frac{4}{3}-\frac{2}{3n}} & \text{si } h^+ = h \\ \mathrm{Od}_{\mathrm{t.i.}}(n) \leqslant \pi^{\frac{4}{3}} 2^{\frac{4}{3}-\frac{2}{3n}} \left(\frac{h^+}{h}\right)^{\frac{2}{3n}} & \text{si } h^+ > h \end{cases}$$

Cela permet déjà de prouver que $n \leqslant 8$. On se débarrasse des cas $n = 7$ et 8 en faisant intervenir les invariants de l'algèbre que sont $|\mathcal{W}|$ ou $\Phi(D, N)$ et en utilisant les minorations plus fines que l'on peut donner sous contraintes.

3.4.2 Passage en revue des cas restants

Au moment où nous avons entrepris ce travail, on ne disposait que de très peu de moyens de calculs pour ce qui concerne l'arithmétique des algèbres de quaternions. Nous avons donc fait en sorte de ramener la plupart des calculs dans le centre, voire dans une de ses extensions quadratiques se plongeant dans l'algèbre considérée. Ce faisant, grâce à `pari` et/ou `magma`, nous n'avons rencontré aucun obstacle calculatoire majeur. Nous avons pu passer en revue tous les cas restant. Pour ce faire nous avons fait usage des tables de corps de nombres dressées accessibles à l'adresse `http//megrez.math.u-bordeaux.fr/pub/numberfields/`. L'application du nouveau critère de simplification ne change guère la donne.

Depuis, plusieurs logiciels, tels `magma` et `sage`, proposent un nombre conséquent de fonctionnalités pour les algèbres de quaternions (la plupart des algorithmes sont dû à Voight [Voi09b, Voi09a, Voi06, Voi05]).

En tout état de cause, notre erreur ne pouvait pas nous conduire à oublier des éléments dans la liste des ordres possédant la propriété de simplification. En revanche, nous pouvions décréter qu'un ordre possède cette propriété sans que cela soit le cas. Dans un genre fixé, cette alternative ne pouvait se produire que dans un seul contexte :

— au moins un type d'ordre de ce genre est tel tous les idéaux stablement libres sont libres ;
— au moins un type d'ordre dans ce même genre possède un idéal stablement libre non libre ;
— le type d'ordre sur lequel nous avons vérifié le théorème 3.3 fait partie de la première catégorie.

Heureusement pour nous, cela ne s'est produit que dans un seul cas, celui du centre de degré 6.

Pour être complet sur cette histoire à rebondissement, j'ajoute que deux exemples d'ordre possédant la propriété de simplification nous avaient échappés. La raison de cet oubli est beaucoup moins profonde ; il s'agit d'une bête erreur de calcul, elle aussi soulevée par Smertnig. Voici la liste dûment corrigée.

Théorème 3.5 (H., Maire (2006) & Smertnig (2013)) *Les ordres d'Eichler d'une algèbre de quaternions totalement définie sur un corps de nombres de degré au moins* 3 *qui possèdent la propriété de simplification ont les invariants suivants,*

— *en degré* 5 *:*

Nb.	$\mathbf{K}$	$\operatorname{disc}\mathbf{K}$	$(\mathbf{d_1}, \mathbf{d_2})$
4	$x^5 - 5x^3 + 4x - 1$	38569	$(\mathfrak{p}_7, 1), (\mathfrak{p}_{13}, 1)$
3	$x^5 - 2x^4 - 3x^3 + 5x^2 + x - 1$	36497	$(\mathfrak{p}_3, 1)$
2	$x^5 - 5x^3 - x^2 + 3x + 1$	24217	$(\mathfrak{p}_5, 1)$

— *en degré* 4 *:*

Nb.	$\mathbf{K}$	$\operatorname{disc}\mathbf{K}$	$(\mathbf{d_1}, \mathbf{d_2})$
19	$x^4 - 2x^3 - 3x^2 + 4x + 1$	4752	$(\mathfrak{p}_4\mathfrak{p}_3, 1)$
16	$x^4 - 6x^2 - 4x + 2$	4352	$(\mathfrak{p}_2\mathfrak{p}_7, 1), (\mathfrak{p}_2\mathfrak{q}_7, 1)$
11	$x^4 - x^3 - 4x^2 + x + 2$	2777	$(1, 1), (1, \mathfrak{p}_2)$
8	$x^4 - 4x^2 + 1$	2304	$(\mathfrak{p}_2\mathfrak{p}_9, 1)$
5	$x^4 - 5x^2 + 5$	2000	$(\mathfrak{p}_4\mathfrak{p}_5, 1)$
4	$x^4 - 4x^2 - x + 1$	1957	$(1, 1), (1, \mathfrak{p}_3)$
2	$x^4 - x^3 - 4x^2 + 4x + 1$	1125	$(1, 1), (1, \mathfrak{p}_{59})$ *to* $(1, \mathfrak{s}_{59})$, $(1, \mathfrak{p}_{29})$ *to* $(1, \mathfrak{s}_{59})$, $(1, \mathfrak{p}_5), (1, \mathfrak{p}_9), (\mathfrak{p}_{16}\mathfrak{p}_5, 1)$
1	$x^4 - x^3 - 3x^2 + x + 1$	725	$(1, 1), (1, \mathfrak{p}_{11}), (1, \mathfrak{q}_{11}), (1, \mathfrak{p}_{19}), (1, \mathfrak{q}_{19}), (1, \mathfrak{p}_{29})$

— *en degré* 3 *:*

Nb.	**K**	disc **K**	$(\mathbf{d_1}, \mathbf{d_2})$
8	$x^3 - x^2 - 4x + 1$	321	$(\mathfrak{p}_3, 1)$
7	$x^3 - x^2 - 4x + 2$	316	$(\mathfrak{p}_2, 1), (\mathfrak{p}_2, \mathfrak{q}_2)$
6	$x^3 - x^2 - 4x + 3$	257	$(\mathfrak{p}_3, 1), (\mathfrak{p}_5, 1), (\mathfrak{p}_7, 1)$
5	$x^3 - 4x - 1$	229	$(\mathfrak{p}_2, 1), (\mathfrak{p}_4, 1), (\mathfrak{p}_7, 1)$
4	$x^3 - x^2 - 4x - 1$	169	$(\mathfrak{p}_5, 1), (\mathfrak{q}_5, 1), (\mathfrak{r}_5, 1),$ $(\mathfrak{p}_{13}, 1)$
3	$x^3 - x^2 - 3x + 1$	148	$(\mathfrak{p}_2, 1), (\mathfrak{p}_2, \mathfrak{p}_5), (\mathfrak{p}_{13}, 1)$ $(\mathfrak{p}_5, 1), (\mathfrak{p}_5, \mathfrak{p}_2)$
2	$x^3 - 3x - 1$	81	$(\mathfrak{p}_3, 1), (\mathfrak{p}_3, \mathfrak{p}_8),$ $(\mathfrak{p}_{19}, 1), (\mathfrak{q}_{19}, 1), (\mathfrak{r}_{19}, 1),$ $(\mathfrak{p}_{37}, 1), (\mathfrak{q}_{37}, 1), (\mathfrak{r}_{37}, 1)$
1	$x^3 - x^2 - 2x + 1$	49	$(\mathfrak{p}_8, 1), (\mathfrak{p}_7, 1),$ $(\mathfrak{p}_{13}, 1), (\mathfrak{q}_{13}, 1), (\mathfrak{r}_{13}, 1)$ $(\mathfrak{p}_{29}, 1), (\mathfrak{q}_{29}, 1), (\mathfrak{r}_{29}, 1)$ $(\mathfrak{p}_{43}, 1), (\mathfrak{q}_{43}, 1), (\mathfrak{r}_{43}, 1)$

Les mêmes tables en degrés 2 et 1 avaient déjà été remplies par Vignéras. Notons que D. Smertnig y a aussi décelé quelques erreurs.

3.5 Et après ?

Pour commencer, j'aimerais vérifier la liste une «dernière fois». Je ne l'ai pas fait à ce jour faute de temps. Comme je l'ai expliqué, compte tenu des nouvelles facilités de calculs dans les algèbres de quaternions, cela ne devrait pas poser énormément de problèmes.

Ce travail me laisse un petit goût amer à cause de l'erreur que nous avons commise mais aussi un goût d'inachevé. Le critère de simplification de Vigneras (qui s'est révélé être un critère d'équivalence entre les notions stablement libre et libre) n'est pas du tout explicite dans le sens où étant donné un ordre ne possédant pas la propriété de simplification (un ne figurant pas dans la liste exhaustive qui constitue notre résultat), je ne sais pas explicitement «confondre» cet ordre, c'est-à-dire construire explicitement un idéal violant la propriété de simplification ni même construire un idéal stablement libre qui n'est pas libre.

Dans le même ordre d'idées, dans la suite des travaux de Voight, beaucoup de questions d'ordre algorithmique se posent dans les algèbres de quaternions et plus généralement dans les algèbres centrales simples. Le point de vue de Voight est de privilégier les calculs locaux pour les globaliser ensuite. Comme en théorie algorithmique des nombres standard, cela nécessite souvent la factorisation de grands entiers. On aimerait un traitement plus «global». Je me suis, par exemple, intéressé — sans avoir conclu pour le moment — au problème du calcul des différents plongements (à conjugaison près) des anneaux d'entiers d'une extension quadratique du centre d'une algèbre de quaternions dans un de ses ordres maximaux. La raison pour laquelle j'ai privilégié ce problème-ci est le fait que dans le cas de l'algèbre de quaternions décomposée $M_2(K)$, on dispose d'une description on ne peut plus explicite d'un système de représentants des classes de conjugaison des différents plongements.

Chapitre 4

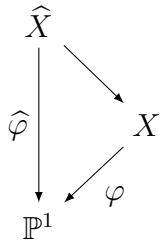
Calculs d'espaces et de familles de Hurwitz

Fraîchement nommé maître de conférences à Toulouse et sous l'impulsion de Jean-Marc Couveignes, je dévie un petit peu des mes travaux de thèse en m'intéressant à certains aspects du du *problème inverse de Galois*. Cela a donné lieu à trois articles, l'un en collaboration avec Emmanuel Riboulet-Deyris, alors en thèse avec J.-M. Couveignes [HRD03], et deux autres seuls [Hal05, Hal09].

Le problème inverse de Galois se décline de plusieurs points de vue. Celui privilégié ici est le point de vue dit «explicite» qui, étant donnés un corps k et un groupe G, consiste à construire un polynôme de $k[X]$ dont le groupe de Galois est G. On dit alors que l'on a *réalisé le groupe G sur k*. Pour ce qui nous concerne, le corps k est celui des rationnels, mais selon une stratégie maintenant éprouvée, pour aboutir à nos fins, on réalisera successivement le groupe G sur les corps $\mathbb{C}(x)$ puis $\mathbb{Q}(x)$. Si les groupes G réalisés sur $\mathbb{Q}$, l'étaient bien avant nos travaux, nous les avons réalisés sous une contrainte supplémentaire : les polynômes construits sont totalement réels. Enfin les techniques utilisées pour effectuer les calculs sont dues à Jean-Marc Couveignes [Cou99, Cou00] et s'appuient sur les espaces de Hurwitz sur lesquels nous revenons.

4.1 Revêtements de $\mathbb{P}^1$

L'objet central de ce travail est un revêtement de la droite projective. Étant donné k un corps de caractéristique zéro, on considère $\mathbb{P}^1$ la droite projective sur k. Un revêtement (ramifié) de $\mathbb{P}^1$ est la donnée d'une courbe algébrique X lisse absolument irréductible définie sur k et d'un morphisme fini $\varphi : X \to \mathbb{P}^1$ lui aussi défini sur k. À un tel revêtement, on associe sa clôture galoisienne qui est un revêtement galoisien et on a le diagramme :



Principaux invariants. — Les invariants sur lesquels nous allons nous concentrer sont les suivants :

- son degré, c'est-à-dire la dimension $[k(X) : k(\mathbb{P}^1)]$,
- son groupe de Galois $\mathrm{Aut}(\widehat{X}/\mathbb{P}^1)$ et l'action (dite de Galois dans la suite) de celui-ci sur ses classes (à gauche) modulo le sous-groupe $\mathrm{Aut}(\widehat{X}/X)$,
- ses points de branchement $b_1, \ldots, b_r \in \mathbb{P}^1$ et l'inertie $(C_1, \ldots, C_r)$ au-dessus de ces points (chaque C_i est la classe de conjugaison dans $\mathrm{Aut}(\widehat{X}/\mathbb{P}^1)$ d'un générateur du groupe d'inertie au-dessus du point de branchement b_i),

— ses fibres, ou encore ses spécialisations en un point de $\mathbb{P}^1$.

Le but est de calculer des modèles explicites de revêtements quand tout ou partie de ces invariants sont fixés à l'avance.

Diverses présentations sur $\mathbb{C}$. — Sur $\mathbb{C}$, un revêtement $X \to \mathbb{P}^1_{\mathbb{C}}$ de *courbes algébriques* ramifié en $b_1 \dots, b_r$ représente la version la plus riche d'une classe d'objets mathématiques admettant plusieurs descriptions équivalentes. C'est l'un des enseignements que l'on peut tirer du célèbre **théorème d'existence de Riemann** [Völ96, Dèb01b, Dèb01a] que l'on peut énoncer comme suit.

Théorème 4.1 (Existence de Riemann) *Soit $r \geqslant 3$ un entier et $b_1, \dots, b_r$ des éléments distincts de $\mathbb{P}^1_{\mathbb{C}}$. Il revient au même de se donner :*

*(i) un revêtement de courbes algébriques $\varphi : X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$, ramifié en $b_1, \dots, b_r$ à isomorphisme algébrique près (version **algébrique**) ;*

*(ii) un morphisme de surface de Riemann compacte $\varphi : X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$, ramifié en $b_1, \dots, b_r$ à isomorphisme analytique près (version **analytique**) ;*

*(iii) un revêtement topologique $\varphi : X \to \mathbb{P}^1_{\mathbb{C}} \setminus \{b_1, \dots, b_r\}$ à isomorphisme près (version **topologique**) ;*

*(iv) un $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{b_1, \dots, b_r\}, b_0)$-ensemble homogène à équivalence près (version **action du groupe fondamental**).*

où $b_0 \in \mathbb{P}^1_{\mathbb{C}}$ est un point base choisi en dehors des points de branchement.

> **Remarque.** — Si ces diverses descriptions sont bel et bien «mathématiquement» équivalentes, elles restent loin d'être «explicitement» équivalentes — et peut-être pas non plus «psychologiquement» équivalentes mais c'est une autre histoire. Un des enjeux de ce travail est précisément de passer d'une représentation à une autre de façon explicite.

La dernière présentation en terme de π_1-ensemble provient de l'action du groupe fondamental de la base $\mathbb{P}^1_{\mathbb{C}} \setminus \{b_1, \dots, b_r\}$ sur la fibre $\varphi^{-1}(b_0)$ d'un point base b_0, via le relèvement des lacets. Cette action est couramment dénommée *action de monodromie*. Elle fait apparaître un groupe fini, appelé *groupe de monodromie*, et défini comme l'image du π_1 dans le groupe des permutations de la fibre $\mathcal{S}_{\varphi^{-1}(b_0)}$. Le groupe de monodromie est défini à conjugaison près et est (anti [1])isomorphe au groupe de Galois version algébrique. De plus l'action de monodromie est équivalente à l'action de Galois rappelée plus haut.

Le groupe fondamental d'une sphère privée d'un certain nombre de points étant un groupe libre, on déduit facilement de la description en terme de π_1-ensemble que le problème inverse de Galois a une solution pour tout groupe fini G sur $\mathbb{C}(x)$. Il suffit de choisir r dépassant le cardinal d'un système de générateurs du groupe G.

C'est cette observation qui est à l'origine de la stratégie maintenant éprouvée consistant, pour réaliser un groupe de Galois sur $\mathbb{Q}$, à commencer à le réaliser sur $\mathbb{C}(x)$, puis à descendre à $\mathbb{Q}(x)$, puis à spécialiser le paramètre x en des valeurs adéquates. Cette façon de procéder a été couronnée de beaucoup de succès, tels ceux apportés par la rigidité (cf. [MM99, Völ96]). Les espaces de Hurwitz s'inscrivent pleinement dans cette démarche ci ; ils peuvent même être considérés comme un ultime développement de cette idée de départ.

Corps des modules et de définition. — Le théorème d'existence de Riemann nous a conduit à passer à $\mathbb{C}$. Néanmoins, étant en premier lieu concerné par l'arithmétique, on va vouloir redescendre à $\mathbb{Q}$. Cela nous amène à ajouter deux invariants à ceux pré-cités, le *corps des modules* et les *corps de définition*.

1. Le «anti» provient du fait qu'en général, on ne compose pas dans le même sens les automorphismes et les chemins.

Soit k un sous-corps de $\mathbb{C}$, $\overline{k}$ sa clôture algébrique, $\mathbb{P}^1_k$ la droite projective sur k et $\mathbb{P}^1_{\overline{k}}$ celle sur $\overline{k}$ provenant de l'extension de la base de $\mathbb{P}^1_k$ à $\overline{k}$. On considère $\varphi : X \to \mathbb{P}^1_{\overline{k}}$ un revêtement, où X désigne une courbe sur $\overline{k}$.

On dit que l extension de k et sous corps de $\overline{k}$ est un *corps de définition* de $\varphi : X \to \mathbb{P}^1_{\overline{k}}$ s'il existe X_l une courbe sur l et $\varphi_l : X_l \to \mathbb{P}^1_l$ un revêtement tel que $X_l \times_l \overline{k} = X_{\overline{k}}$ et $\varphi_l \times_l \overline{k} = \varphi_{\overline{k}}$. On dit aussi que φ_l est un l-modèle de φ.

On peut faire agir le groupe de Galois absolu $\mathrm{Gal}(\overline{k}/k)$ sur le revêtement φ défini sur $\overline{k}$ par conjugaison. Pour tout $\sigma \in \mathrm{Gal}(\overline{k}/k)$, le conjugué ${}^\sigma\varphi : {}^\sigma X \to \mathbb{P}^1_{\overline{k}}$ est encore un revêtement sur $\overline{k}$ et on est en mesure d'introduire le sous-groupe :

$$\Gamma = \{\sigma \in \mathrm{Gal}(\overline{k}/k) \mid {}^\sigma\varphi \simeq \varphi\} \subset \mathrm{Gal}(\overline{k}/k).$$

Le *corps des modules relativement à k* de φ est le corps fixe $\mathrm{Gal}(\overline{k}/k)^\Gamma$. C'est une extension finie de k qui est contenue dans tous les corps de définition de φ. S'il est lui même corps de définition, c'est donc le plus petit.

4.2 Espaces de Hurwitz et leurs variantes

Les espaces de Hurwitz, initiés par Hurwitz lui même, ont été utilisés par Fulton [Ful69] pour établir la connexité des espaces $\mathcal{M}_g$, puis ont été intensément étudiés par Fried, Völklein, Dèbes [Fri77, FV91, DF90, DF94], Coombes & Harbater [CH85], Wewers [Wew98] en particulier pour le lien étroit qu'ils entretiennent avec le problème inverse de Galois. Ce lien a été prouvé et mis en exergue par Fried et Völklein dans leur article fondateur de 1991 [FV91]. La description qui suit s'inspire fortement de cette référence mais aussi du livre de Völklein [Völ96] et du survey de Dèbes [Dèb01c] écrits sur le sujet.

Un espace de Hurwitz est l'espace des paramètres — ou des modules — d'une famille de revêtements de $\mathbb{P}^1$. L'idée est donc de ne pas considérer un revêtement seul, mais plutôt de les étudier en famille. Il s'agit bien entendu de familles à isomorphisme près. On distingue principalement deux types de classes d'isomorphisme de revêtements. Pour chacune de ces classes, il convient de décrire précisément les données inhérentes à la classe, la relation d'isomorphisme ainsi que le groupe d'automorphismes des objets.

Quelques notations relatives à la théorie des groupe Pour E un ensemble fini, on note $\mathcal{S}_E$ le groupe des permutations de E ; de façon usuelle, si $E = \{1, \dots, n\}$, on abrège par $\mathcal{S}_n$. Pour G un sous-groupe de $\mathcal{S}_E$, on note $Z_{\mathcal{S}_E}(G)$ le centralisateur et $N_{\mathcal{S}_E}(G)$ le normalisateur de G dans $\mathcal{S}_E$; ils sont respectivement définis par :

$$Z_{\mathcal{S}_E}(G) = \{\sigma \in \mathcal{S}_E \mid \sigma g = g\sigma,\ \forall g \in G\} \quad \text{et} \quad N_{\mathcal{S}_E}(G) = \{\sigma \in \mathcal{S}_E \mid \sigma G \sigma^{-1} = G\}.$$

Les revêtements purs. — On se fixe r un entier $\geqslant 3$, G un groupe fini, E un G-ensemble homogène avec action fidèle et $\mathbf{C} = (C_1, \dots, C_r)$ un r-uplet de classes de conjugaison (non triviales) de G. Il revient au même de supposer que G s'injecte dans $\mathcal{S}_E$ et que son image est un sous-groupe transitif.

Remarques.

1. Souvent $E = \{1, \dots, d\}$ mais parfois non comme on le verra dans le second exemple.

2. La donnée d'un G-ensemble homogène (à équivalence près) est équivalente à celle d'un sous-groupe U de G (à conjugaison près), la correspondance étant donnée dans un sens par $U \mapsto (G/U)_g$ avec action de G par multiplication à gauche et dans l'autre sens par $E \mapsto \mathrm{Stab}_G(x)$ où $x \in E$.

Un *revêtement pur* associé à ces données est un revêtement $\varphi : X \to \mathbb{P}^1$, de degré $\#E$, ramifié en (exactement) r points, avec inertie $C_1, \dots, C_r$ (sans ordre), tel que $\mathrm{Aut}(\widehat{X}/\mathbb{P}^1)$ est isomorphe à G, et tel que les actions de G sur E et de $\mathrm{Aut}(\widehat{X}/\mathbb{P}^1)$ sur les classes à gauche de $\mathrm{Aut}(\widehat{X}/\mathbb{P}^1)$ modulo $\mathrm{Aut}(\widehat{X}/X)$ sont équivalentes via cet isomorphisme.

Deux tels revêtements $\varphi : X \to \mathbb{P}^1$ et $\varphi' : X' \to \mathbb{P}^1$ sont isomorphes si et seulement s'il existe un isomorphisme $\iota : X \to X'$ tel que $\varphi = \varphi' \circ \iota$. Enfin le groupe d'automorphismes d'un objet est canoniquement isomorphe à $Z_{\mathcal{S}_E}(G)$

On désigne par $[\varphi]$ la dite classe d'isomorphisme et on désigne l'ensemble des classes d'isomorphisme des revêtements purs par :

$$\mathcal{H}_r(G)^{\mathrm{ab}} = \big\{[\varphi] \mid \varphi : X \to \mathbb{P}^1,\ \varphi \text{ pur de groupe de Galois } G, \text{ ramifiés en } r \text{ points}\big\}$$
$$\mathcal{H}_r(G, \mathbf{C})^{\mathrm{ab}} = \{[\varphi] \mid \text{ idem plus inertie } \mathbf{C}\}$$

Remarques.

1. Les notations choisies sont un tant soit peu abusives dans le sens où la notation $\mathcal{H}_r(G)^{\mathrm{ab}}$ dépend du groupe G mais aussi de sa représentation. Pour être rigoureux, il eut fallu noter l'espace absolu par $\mathcal{H}_r(G \hookrightarrow \mathcal{S}_E)^{\mathrm{ab}}$; par soucis de légèreté, je ne le ferai pas.

2. À ce titre, la notation de Fried & Volklein est mieux choisie puisqu'ils notent $\mathcal{H}_r(G, U)^{\mathrm{ab}}$ l'espace précédent, où U est un sous-groupe de G et où le G-ensemble homogène n'est rien d'autre que $(G/U)_g$.

Une fois fixés les points de branchement $b_1, \ldots, b_r \in \mathbb{P}^1$, sur $\mathbb{C}$, ces classes d'équivalence admettent une description très simple grâce à la version «action du groupe fondamental». Fixer de surcroît le groupe de Galois avec action revient à fixer le groupe de monodromie ainsi que l'action de monodromie. Cela revient en dernier lieu à se fixer une surjection de groupe fondamental $\pi_1(\mathbb{P}^1 \setminus \{b_1, \ldots, b_r\}, b_0)$ dans G, deux telles surjections donnant deux revêtements isomorphes si et seulement si elles sont conjuguées par un élément du normalisateur $N_{\mathcal{S}_E}(G)$. Une telle surjection est entièrement déterminée par l'image d'une *base homotopique* de $\mathbb{P}^1 \setminus \{b_1, \ldots, b_r\}$ constituée de r lacets dont le produit vaut 1. C'est pourquoi, on introduit, selon la terminologie de Fried, les *classes de Nielsen* :

$$\mathrm{Ni}_r(G) = \{(g_1, \ldots, g_r) \in (G \setminus \{1\})^r \mid G = \langle g_1, \ldots, g_r\rangle\,,\ g_1 \cdots g_r = 1\}$$
$$\mathrm{Ni}_r(G, \mathbf{C}) = \big\{(g_1, \ldots, g_r) \in G^r \mid G = \langle g_1, \ldots, g_r\rangle\,,\ g_1 \cdots g_r = 1,\ \exists \nu \in \mathcal{S}_r,\ g_i \in C_{\nu(i)}\big\}\,.$$

On pose :

$$\mathrm{ni}^{\mathrm{ab}}(G) = \mathrm{Ni}_r(G)/N_{\mathcal{S}_E}(G) \qquad \text{et} \qquad \mathrm{ni}^{\mathrm{ab}}(G, \mathbf{C}) = \mathrm{Ni}_r(G)/N_{\mathcal{S}_E}(G, \mathbf{C})$$

alors on a les correspondances bi-univoques suivantes :

$$\mathrm{ni}(G)^{\mathrm{ab}} \longleftrightarrow \big\{[\varphi] \in \mathcal{H}_r(G)^{\mathrm{ab}} \mid \varphi \text{ ramifié en } b_1, \ldots, b_r\big\}$$
$$\mathrm{ni}(G, \mathbf{C})^{\mathrm{ab}} \longleftrightarrow \big\{[\varphi] \in \mathcal{H}_r(G, \mathbf{C})^{\mathrm{ab}} \mid \varphi \text{ ramifié en } b_1, \ldots, b_r\big\}$$

Les* G*-revêtements. — On se fixe un entier $r \geqslant 3$, un groupe fini G et éventuellement un r-uplet $(C_1, \ldots, C_r)$ de classes de conjugaisons de G. Un revêtement associé à ces données s'appelle un G-*revêtement*[2] et c'est la donnée d'un couple (ψ, ϵ) où $\psi : Y \to \mathbb{P}^1$ désigne un revêtement galoisien et où $\epsilon : \mathrm{Aut}(Y/\mathbb{P}^1) \to G$ est un isomorphisme de groupes. Deux tels couples (X, ϵ) et (X', ϵ') sont dits isomorphes si et seulement s'il existe $\iota : Y \to Y'$ tel que :

$$\psi = \psi' \circ \iota \qquad \text{et} \qquad \epsilon(\sigma) = \epsilon'(\iota \circ \sigma \circ \iota^{-1}),\ \forall \sigma \in \mathrm{Aut}(Y/\mathbb{P}^1).$$

L'entier r est le nombre (exact) de points de branchement du revêtement, les classes de conjugaison $C_1, \ldots, C_r$ désignent les classes d'inertie sans ordre.

Il faut voir l'isomorphisme ϵ comme un étiquetage des automorphismes. Mécaniquement, cet étiquetage fait fondre le groupe d'automorphismes de l'objet considéré : au lieu de G groupe d'automorphismes de l'objet non étiqueté, le groupe d'automorphismes de l'objet étiqueté s'identifie à $Z(G)$ le centre de G.

2. Le G (droit) de l'appellation G-revêtement est là pour signifier que le groupe de Galois fait partie des données. Il n'a rien à voir avec le groupe G (mode mathématique) lui même. C'est un peu troublant mais cela fait partie du folklore.

On note $[\psi, \epsilon]$ la classe d'isomorphisme d'un G-revêtement et on désigne l'ensemble des classes d'isomorphisme par :

$$\mathcal{H}_r(G)^{\text{in}} = \Big\{[\psi,\epsilon] \mid \psi : Y \to \mathbb{P}^1,\ \text{Aut}(\psi) \xrightarrow{\epsilon} G,\ \psi \text{ ramifiés en } r \text{ points}\Big\}$$
$$\mathcal{H}_r(G,\mathbf{C})^{\text{in}} = \{[\psi,\epsilon] \mid \text{ idem plus inertie } \mathbf{C}\}$$

Remarque. — Cette fois, la notation n'est plus abusive dans le sens ou un G-revêtement ne dépend que du groupe abstrait G.

À nouveau, une fois fixés les points de branchement à $b_1, \ldots, b_r \in \mathbb{P}^1$, sur $\mathbb{C}$, grâce à la description en terme de π_1-ensembles, on dispose d'une description purement combinatoire de ses classes d'isomorphisme. Il suffit d'introduire :

$$\text{ni}^{\text{in}}(G) = \text{Ni}_r(G)/G \qquad \text{et} \qquad \text{ni}^{\text{in}}(G,\mathbf{C}) = \text{Ni}_r(G,\mathbf{C})/G$$

alors on a les correspondances bi-univoques suivantes :

$$\text{ni}(G)^{\text{in}} \longleftrightarrow \{G\text{-revêtements ramifiés en } b_1, \ldots, b_r\}$$
$$\text{ni}(G,\mathbf{C})^{\text{in}} \longleftrightarrow \{G\text{-revêtements ramifiés en } b_1, \ldots, b_r \text{ et d'inertie } \mathbf{C} \text{ (à l'ordre près)}\}$$

Enrichissement de structures successifs. — Évidemment, on ne se contente pas de cette description ensembliste et on souhaite munir les ensembles $\mathcal{H}_r(G)^{\text{ab/in}}$ de structures, en commençant par une topologie, puis une structure analytique, puis une structure de variétés algébriques sur $\mathbb{C}$, puis pour terminer une structure de variétés algébriques sur $\mathbb{Q}$. Pour cela, la démarche est la même que celle qui prévaut au théorème d'existence de Riemann mais en dimension supérieure.

L'idée de départ consiste à partir d'un revêtement, puis à en «faire bouger» les points de branchements. C'est pourquoi, on s'appuie sur l'espace topologique sous-jacent à l'ensemble des familles de r points de branchements. Il s'agit de

$$\mathcal{U}_r = \big\{\{b_1, \ldots, b_r\},\ b_i \in \mathbb{P}^1_{\mathbb{C}}, b_i \neq b_j, \text{si } i \neq j\big\}$$

On peut munir cet ensemble d'une topologie héritée de celle de $\mathbb{C}$. Mieux, on peut aussi le munir d'une structure de variété algébrique quasi-projective lisse. C'est le complémentaire dans $\mathbb{P}^r = \text{Proj}(\mathbb{C}[a_0, \ldots, a_r])$ de l'hypersurface «discriminantielle» définie par l'équation $\text{disc}(a_r X^r + \cdots + a_0) = 0$. Si $b_i = (x_i : y_i)$ alors le point de $\mathbb{P}^r$ qui lui correspond est celui dont les coordonnées sont les coefficients du polynôme (homogène de degré r) $\prod_{i=1}^r (x_i X - y_i Y)$.

On dispose de l'application (pour l'instant ensembliste) «point de branchement»

$$\text{br} : \mathcal{H}_r(G)^{\text{ab/in}} \longrightarrow \mathcal{U}_r,$$

qui à $[\varphi]$ ou $[\psi, \epsilon]$ associe l'ensemble des points de branchement. On remonte les structures sur $\mathcal{U}_r$ via br.

La première phase consiste à installer une topologie sur les espaces $\mathcal{H}_r(G)^{\text{ab/in}}$. Il faut définir une notion de voisinage sur les revêtements : deux revêtements sont décrétés voisins si leur points de branchement le sont et si les actions de monodromie sont reliées par une transformation continue. On montre alors que l'application $\text{br} : \mathcal{H}_r(G)^{\text{in/ab}} \to \mathcal{U}_r$ est un revêtement topologique.

Ensuite, il faut procéder comme dans le théorème d'existence de Riemann à un enrichissement progressif de structures. Fried & Völklein font assez peu de cas des ces étapes, les considérant comme acquises. Dans son survey sur le domaine, P.Dèbes donne plus de détails. Le passage de topologique à analytique est une conséquence d'un résultat de Grauert & Remmert ; le fait que $\mathcal{U}_r$ soit le complémentaire d'un fermé de $\mathbb{P}^r$ joue à plein ici. A ce stade, l'application $\text{br} : \mathcal{H}_r(G)^{\text{in/ab}} \to \mathcal{U}_r$ est un morphisme analytique.

Le passage, d'analytique à algébrique, est une conséquence de GAGA dû à Serre. Les variétés analytiques en jeu peuvent être munies d'une structure de variétés algébriques quasi projectives sur $\mathbb{C}$. L'application points de branchement devient un morphisme algébrique étale.

L'ultime étape, traitée en détail dans Fried & Völklein, est celle de la descente à $\mathbb{Q}$. Elle se fait en deux temps, en descendant d'abord à $\overline{\mathbb{Q}}$, puis à $\mathbb{Q}$ ensuite.

Le preuve de la descente à $\mathbb{Q}$ utilise de façon primordiale l'existence d'une *famille universelle* lorsque les objets paramétrés n'ont pas automorphisme. Rappelons que dans le cas pur (resp. G-revêtement), cela revient à supposer que le normalisateur de G dans $\mathcal{S}_E$ (resp. le centre de G) est trivial. Si tel est le cas, il existe une famille universelle $\mathcal{F}$, c'est-à-dire une variété quasi-projective lisse et un morphisme étale

$$\mathcal{F} \longrightarrow \mathcal{H}_r(G)^{\mathrm{ab}} \times \mathbb{P}^1$$

tel que pour tout $h \in \mathcal{H}_r(G)^{\mathrm{ab}}$, le morphisme spécialisé $\mathcal{F}_h \to \mathbb{P}^1$ est un exemplaire de la classe de revêtements correspondant au point h. Cette famille est aussi le cadre algébrique des calculs présentés ci-après.

Le résultat principal [FV91, Theorem 1], tiré de cette étude, peut s'énoncer ainsi.

Théorème 4.2 (Fried & Völklein (1991)) *Soit E un ensemble fini, G un sous-groupe fini transitif de $\mathcal{S}_E$ et $r \geqslant 3$ un entier tel que G puisse être engendré par $(r-1)$ éléments. Alors les espaces $\mathcal{H}_r(G)^{ab}$ et $\mathcal{H}_r(G)^{in}$ admettent une unique structure de variétés algébriques (compatible avec la structure analytique) définies sur $\mathbb{Q}$, de telle sorte que les applications :*

$$\mathcal{H}_r(G)^{in} \to \mathcal{H}_r(G)^{ab} \to \mathcal{U}_r$$

sont des morphismes algébriques définis sur $\mathbb{Q}$.

De plus si $[\varphi] \in \mathcal{H}_r^{ab}(G)$ alors le corps de définition de $[\varphi]$ est le corps des modules de φ relativement au corps de définition des points de branchement $\mathrm{br}([\varphi]) \in \mathcal{U}_r$. *De même si $[\psi, \epsilon] \in \mathcal{H}_r^{in}(G)$ alors le corps de définition de $[\psi, \epsilon]$ est le corps des modules de ψ relativement au corps de définition des points de branchement* $\mathrm{br}(\psi) \in \mathcal{U}_r$.

Enfin, si $\mathbf{C}$ est un r-uplet de classes de conjugaisons de G, alors $\mathcal{H}_r(G, \mathbf{C})^{in/ab}$ est une sous-variété qui est réunion de composantes absolument irréductibles et qui est définie sur $\overline{\mathbb{Q}}$ et même sur $\mathbb{Q}$ dès lors que les classes de $\mathbf{C}$ sont rationnelles.

C'est ce théorème qui fait le lien entre le problème inverse de Galois régulier sur un corps K et la recherche de points définis sur K sur les espaces de Hurwitz [FV91, Corollary 1]. La seule petite zone d'ombre qui perdure dans cette magnifique ré-interprétation du problème inverse de Galois est due au fait que le corps des modules d'un revêtement n'est pas forcément un corps de définition. Nous reviendrons en détail sur ce phénomène regrettable — mais est-ce vraiment regrettable ? — dans le chapitre 5.

Pour ce qui nous concerne c'est sous un angle explicite que nous nous proposons d'investir ce théorème dans la suite.

4.3 Philosophie du calcul

Les calculs explicites d'espaces de Hurwitz présentés ici suivent la méthode par déformation développée par J.-M. Couveignes ([Cou99, Cou00]). Il convient de noter que la mise en œuvre de la méthode est délicate et que chaque exemple a ses spécificités et soulève des problèmes algorithmiques différents. À l'heure actuelle, nous sommes très très loin de fournir une routine qui étant donnée une description en cycles de branchement retourne un modèle algébrique de la famille de revêtements correspondant. Algorithmiquement, on raisonne au cas par cas, ce que j'ai fait pour deux exemples différents avec chacun leur spécificités (cf. §4.3.5).

L'idée générale est, peu ou prou, de reprendre les étapes de la preuve du théorème 4.2 de façon constructive. Le seul détour — mais il est de taille — à cette voie toute tracée consiste à visiter le bord des espaces de Hurwitz. Ces bords, très bien étudiés en théorie par Wewers [Wew98], sont évidemment reliés aux compactifications adéquates des variétés quasi-projectives en jeu.

Si l'objectif initial (et accessoirement atteint) est de produire des polynômes à coefficients rationnels ayant un groupe de Galois donné et parfois d'autres propriétés comme celle d'avoir toutes ses racines réelles, le détail du calcul présente, à mon sens, un intérêt autre : celui d'illustrer des théories mathématiques assez subtiles. Pour ce qui me concerne, c'est en développant ces calculs que j'ai pu saisir ce que je sais des espaces de Hurwitz. Voici les principales étapes du calcul en quelques mots.

4.3.1 Restriction à une courbe de Hurwitz

Les variétés $\mathcal{H}_r(G,\mathbf{C})^{\mathrm{ab/in}}$ sont de trop grande dimension pour être vraiment maniables de façon effective. Surtout, on ne dispose d'aucun algorithme pour y trouver des points rationnels, ce qui est notre but ultime. Ou plutôt, le seul algorithme de recherche de points rationnels dont on dispose consiste à essayer de «dessiner» des courbes isomorphes à $\mathbb{P}^1_{\mathbb{Q}}$ sur ces variétés. Ceci est précisément l'enjeu de cette étape du calcul. Notons que cette démarche a été rendue plus ou moins systématique par Dettweiler [Det04].

Afin de faciliter les calculs, on commence en général par ordonner, totalement ou partiellement, les points de branchement. Dans le cas où l'ordre est total par exemple, cela revient à considérer [3] :

$$\mathcal{U}^r = \left\{(b_1,\dots,b_r),\ b_i \in \mathbb{P}^1_{\mathbb{C}}, b_i \neq b_j, \text{si } i \neq j\right\} \subset (\mathbb{P}^1)^r$$

ainsi que le morphisme $\mathcal{U}^r \to \mathcal{U}_r$ défini par $(b_1,\dots,b_r) \mapsto \{b_1,\dots,b_r\}$. Tout choix d'ordre pour les classes d'inertie correspond à une réunion de certaines composantes connexes du produit fibré $\mathcal{H}_r(G,\mathbf{C})^{\mathrm{ab/in}} \times_{\mathcal{U}_r} \mathcal{U}^r$. Notons :

$$\mathcal{H}^r(G,\mathbf{C})^{\mathrm{ab/in}} \hookrightarrow \mathcal{H}_r(G,\mathbf{C})^{\mathrm{ab/in}} \times_{\mathcal{U}_r} \mathcal{U}^r.$$

celle correspondant à l'ordre $(C_1,\dots,C_r)$ (attention au placement des indices/exposants r !)

Ce dernier espace revêt le premier espace et la dimension n'a pas diminué. Mais c'est sur cet espace que l'on cherche à «dessiner» des courbes. Pour cela, on tire en arrière un plongement bien choisi d'un ouvert $\mathcal{U}$ de $\mathbb{P}^1$ dans $\mathcal{U}^r$. Cette fois l'espace de module considéré est une courbe notée simplement $\mathcal{H}$ qui revêt $\mathcal{U} \subset \mathbb{P}^1$ par la restriction du morphisme br (et noté de même). Dans la mesure où le but ultime est de trouver des points rationnels sur cette courbe, on la souhaite de genre aussi petit que possible, voire même de genre zéro.

Si tel n'est pas le cas, il convient de remettre en cause le choix de la courbe de Hurwitz. Heureusement, la pertinence de ce choix est immédiatement vérifiable à l'occasion de l'étape suivante.

4.3.2 Étape combinatoire et action de tresses

Bien que moins intéressante que les autres du point de vue du calcul, cette étape n'en demeure pas moins cruciale. Elle repose intégralement sur les versions combinatoires des tous les objets considérés. On y manipule essentiellement des permutations.

Système de représentants des classes de Nielsen. — Le premier objectif est de déterminer un système de représentant des classes de Nielsen définies précédemment. Pour chaque choix d'un r-uplet $(b_1,\dots,b_r)$, on a donc une description en termes de r-ruplet de permutations de la fibre $\mathrm{br}^{-1}((b_1,\dots,b_r))$

3. Un aspect du «folklore» lié aux espaces de Hurwitz consiste à réserver les notations avec indice en bas aux objets *non ordonnés*, tandis que les exposants sont plutôt réservés aux objets *ordonnés*.

On en déduit déjà le degré du revêtement br : $\mathcal{H} \to \mathcal{U}$. Mais on souhaite beaucoup plus d'informations, notamment son type de ramification afin de pouvoir calculer le genre de $\mathcal{H}$.

Action de tresses. — Au même titre que les objets qu'ils paramètrent, les espaces de Hurwitz admettent une description purement «combinatoire» en terme de $\pi_1(\mathcal{U}_r)$-ensembles. Les deux revêtements «points de branchement» :

$$\mathcal{H}_r(G, \mathbf{C}) \to \mathcal{U}_r, \qquad \mathcal{H}^r(G, \mathbf{C}) \to \mathcal{U}^r,$$

peuvent être entièrement décrits en terme de π_1-ensemble, via le relèvement des lacets ; c'est encore la monodromie. Les groupes fondamentaux qui rentrent en jeu sont très bien connus ; pour $\mathcal{U}_r$, il s'agit *groupe de tresse de Hurwitz* dont on connaît une présentation par générateurs et relations. On dispose aussi de formule donnant l'action de monodromie sur une fibre (constituée des classes de Nielsen listées juste avant). Pour ce qui concerne les générateurs, souvent notés Q_i pour $1 \leqslant i \leqslant r-1$, ils agissent comme suit :

$$(g_1, \ldots, g_r).Q_i = (g_1, \ldots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_i, g_{i+1}, \ldots, g_r).$$

On déduit le même genre de résultat pour le revêtement ordonné $\mathcal{H}^r(G, \mathbf{C}) \to \mathcal{U}^r$. La connexité des variétés $\mathcal{H}_r(G, \mathbf{C})$ et $\mathcal{H}^r(G, \mathbf{C})$ est équivalente au fait que l'action de monodromie ainsi calculée est transitive.

En suivant le plongement $\mathcal{U} \hookrightarrow \mathcal{U}^r$ au niveau des groupes fondamentaux, on en déduit la monodromie du revêtement de courbes $\mathcal{H} \to \mathcal{U}$. À l'issue de cette étape on est donc capable de dire si la courbe $\mathcal{H}$ est connexe, et on connaît le degré et la ramification du revêtement $\mathcal{H} \to \mathcal{U}$. Si jamais $\mathcal{H}$ n'a pas été trouvé de genre zéro, on remet en cause le choix de la courbe de Hurwitz et on trace une autre courbe sur $\mathcal{H}^r(G, \mathbf{C})$.

4.3.3 Choix d'une dégénérescence et sa déformation

À partir de cette étape, les calculs prennent une saveur bien plus géométrique. Le contexte géométrique sous-jacent dans lequel on effectue tous les calculs est la *famille universelle* (qui existe : les revêtements constituant les deux familles considérées sont sans automorphisme).

Après restriction à la courbe de Hurwitz, la famille universelle de Hurwitz devient une surface algébrique quasi-projective, encore notée $\mathcal{F}$, et on dispose d'un revêtement $\mathcal{F} \to \mathcal{H} \times \mathbb{P}^1$. Composée avec la première projection, cela fait de $\mathcal{F}$ une *surface arithmétique*. C'est précisément un modèle algébrique de cette surface que l'on cherche à calculer dans la suite.

L'idée principale de la méthode est de reconstruire toute la famille par déformation d'une de ses dégénérescences. On va donc travailler au voisinage d'un point du bord de notre espace $\mathcal{H}$. Topologiquement, il est assez facile de comprendre à quoi ressemblent les dégénérescences d'une famille de revêtements. Il s'agit de faire coalescer les points de branchement. Cela revient à pincer la sphère marquée à r points de la base, pour obtenir deux sphères marquées à $(r-1)$ points collées l'une à l'autre en un de ces points. Algébriquement, le revêtement dégénéré a pour base deux exemplaires de $\mathbb{P}^1$ qui se coupent en un point et pour espace total une courbe réductible (mais connexe) dont chacune des composantes revêt l'une des composantes irréductibles de la base. L'action de tresse nous rend alors un ultime service en nous permettant de déterminer exactement le nombre de composantes ainsi que le type de ramification des restrictions du revêtement dégénéré à chacune de ces composantes. Le point clé est que toutes ces restrictions sont des revêtements de $\mathbb{P}^1$ qui ne sont plus ramifiés en r points mais en simplement $(r-1)$ points. Le calcul de modèles algébriques est donc beaucoup moins problématique. C'est d'autant plus le cas pour $r = 4$ qui est vérifié dans les deux exemples traités.

On détermine des modèles algébriques des revêtements sur chacune des composantes ; dans les deux exemples, ce sont tous des revêtements de $\mathbb{P}^1$ ramifiés en seulement trois points et des méthode ad hoc permettent souvent de s'en sortir.

Ensuite on choisit des fonctions sur $\mathcal{F}$ et on recolle les modèles calculés sur chaque composante au moyen de ces fonctions. Des calculs d'intersection sur la surface arithmétique $\mathcal{F} \to \mathcal{H}$ sont nécessaires pour ajuster les fonctions choisies de telles sorte qu'elles se spécialisent en des fonctions non constantes sur une composante donnée.

4.3.4 Algébrisation

À l'issue de la déformation, on dispose d'un modèle algébrique (heuristique) de la famille universelle $\mathcal{F}$ sur un localisé complété en un point du bord de $\mathcal{H}$ (le point correspondant à la dégénérescence choisie). Concrètement, on connaît tous les coefficients d'un modèle reliant les fonctions choisies, dans un complété de $\mathbb{Q}(\mathcal{H})$; il s'agit de séries formelles. On souhaite redescendre à $\mathbb{Q}(\mathcal{H})$. Comme $\mathcal{H}$ est de genre zéro, on peut choisir un paramètre, disons T, sur $\mathcal{H}$ que l'on peut lui aussi développer formellement. Trouver les expressions de tous les coefficients en fonction du paramètre T revient à déterminer des relations algébriques entre séries formelles. C'est facile.

4.3.5 Similitudes et différences entre les deux familles calculées

Avant de rentrer un petit peu plus dans le détail des calculs, voici quelques spécificités qui rapprochent les deux familles étudiées :

- les revêtements constituant la famille sont sans automorphisme...
- ...et avec quatre points de branchement,
- l'espace de Hurwitz que l'on cherche à calculer est un espace «absolu»...
- ...et la courbe de Hurwitz tracée dessus est de genre zéro,
- certains éléments des deux familles possèdent des fibres totalement réelles et conduisent donc à des polynômes à coefficients rationnels ayant certains groupe de Galois avec la propriété supplémentaire d'être totalement réels.

En voici d'autres qui les distinguent :

- dans le premier exemple, le degré des revêtements est un entier pair non fixé (il y a une famille pour chaque degré pair), alors que dans le second cas, le degré des revêtements vaut 9.
- dans le premier exemple, il s'agit d'une famille de revêtement de $\mathbb{P}^1$ par lui même, et dans le second par une courbe elliptique,
- dans le premier cas, le groupe de départ est auto-normalisateur dans $\mathcal{S}_E$, donc il n'y a pas lieu de distinguer en les espaces de Hurwitz «ab» et «in», dans ce second exemple, ce n'est plus le cas et on verra que cela rend l'exemple plus riche et subtil,
- la deuxième famille possède un illustre élément, en la personne d'un revêtement entre courbes de Shimura ; le trouver est l'objet d'un autre prolongement au calcul proprement dit de la famille.

4.4 L'exemple $\mathcal{H}_4\left(\mathcal{S}_n, (n-2, 3, 2^{\frac{n-2}{2}}, 2^{\frac{n}{2}})\right)$

Avec E.Riboulet-Deyris [HRD03], nous avons mis en oeuvre la méthode précédente pour déterminer explicitement une famille de revêtements de $\mathbb{P}^1$ qui nous a été suggérée par G.Malle. On choisit $r = 4$ et comme données de groupe et d'action de groupe, les suivantes :

$$G = \mathcal{S}_n,\ n \text{ pair}, \qquad \text{et} \qquad \mathbf{C} = (C_1, C_2, C_3, C_4) = (n-2, 3, 2^{\frac{n-2}{2}}, 2^{\frac{n}{2}})$$

où chaque classe de conjugaison est donnée par son type de décomposition en cycles à supports disjoints. Une rapide application de Riemann-Hurwitz permet de vérifier que l'on s'intéresse donc à la famille des revêtements $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$, de degré pair égal à n, de groupe de Galois $\mathcal{S}_n$, et ramifiés en quatre points avec inertie $\mathbf{C}$.

4.4.1 Choix de la courbe de Hurwitz

Tout d'abord, comme $\mathcal{S}_n$ est auto-normalisateur dans lui même, il n'y a pas lieu, dans cet exemple, de distinguer les espaces de Hurwitz «in» et «ab» et on note simplement $\mathcal{H}_4(\mathcal{S}_n, \mathbf{C})$ le dit espace.

Afin de faciliter les calculs, on ordonne les points de branchement et on introduit $\mathcal{H}^4(\mathcal{S}_n, \mathbf{C}) = \mathcal{H}_4(\mathcal{S}_n, \mathbf{C}) \times_{\mathcal{U}_4} \mathcal{U}^4$ l'espace de Hurwitz paramétrant les revêtements de notre famille mais avec points de branchement ordonnés. C'est une variété de dimension 4 peu maniable de façon explicite. D'où la nécessité de tracer une courbe dite de Hurwitz sur cette variété. Le choix dans cet exemple est l'un des plus naturels : étant donné $(z_1, z_2, z_3) \in (\mathbb{P}^1)^3$ à coordonnées deux-à-deux distinctes, on introduit la courbe de Hurwitz, notée $\mathcal{H}'_{(z_1,z_2,z_3)}$, obtenue par tiré en arrière de $\mathrm{br} : \mathcal{H}^4(\mathcal{S}_n, \mathbf{C}) \to \mathcal{U}^4$ le long du morphisme :

$$\mathbb{P}^1 \setminus \{z_1, z_2, z_3\} \hookrightarrow \mathcal{U}^4, \qquad z \longmapsto (z_1, z_2, z_3, z)$$

Par restriction, on obtient un revêtement «4-ème point de branchement» encore noté br :

$$\mathrm{br} : \mathcal{H}'_{(z_1,z_2,z_3)} \longrightarrow \mathbb{P}^1 \setminus \{z_1, z_2, z_3\}.$$

La pertinence du choix de la courbe de Hurwitz peut être immédiatement validé par la suite des calculs.

4.4.2 Étape combinatoire et action de tresses

Le but est de déterminer les principaux invariants du revêtement $\mathrm{br} : \mathcal{H}'_{(z_1,z_2,z_3)} \to \mathbb{P}^1 \setminus \{z_1, z_2, z_3\}$ (ou plutôt de l'unique prolongement de ce revêtement aux courbes complètes sous-jacentes) que sont le degré, le type de ramification.

Le fait que le degré des revêtements constituant la famille ne soit pas fixé, apporte un peu de sel à l'étape purement combinatoire. Tout se passe dans $\mathcal{S}_n$.

Étape combinatoire. — Le premier enjeu est l'énumération des classes de Nielsen. Comme nous avons ordonné les points de branchement, il s'agit des classes de Nielsen dites *strictes*. La seule différence avec les classes introduites dans la section 4.1 réside dans la relation d'équivalence. Dans l'exemple qui nous concerne, on veut trouver un système de représentants des classes :

$$\mathrm{sni}^{\mathrm{ab}}(\mathcal{S}_n, \mathbf{C}) = \left\{ (\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in (\mathcal{S}_n)^4, \ \left\{ \begin{array}{l} \sigma_1\sigma_2\sigma_3\sigma_4 = 1, \ \sigma_i \in C_i \ \forall i \\ \langle \sigma_1, \sigma_2, \sigma_3, \sigma_4 \rangle = \mathrm{Perm}\, n \end{array} \right\} \right/ \sim$$

où $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) \sim (\sigma'_1, \sigma'_2, \sigma'_3, \sigma'_4)$ si et seulement s'il existe $\tau \in \mathcal{S}_n$ tel que $\sigma'_i = \tau\sigma_i\tau^{-1}$ pour $1 \leqslant i \leqslant 4$. Compte tenu de la généricité, nous n'avons pas pu déléguer ce calcul à l'ordinateur et avons dû trouver une façon systématique de lister les classes. Le résultat est résumé dans la table 1 de l'article ; elle compte $3\left(\frac{n}{2} - 1\right)$ éléments, ce qui nous donne déjà le degré du revêtement br : $\mathcal{H}'_{(z_1,z_2,z_3)} \to \mathbb{P}^1 \setminus \{z_1, z_2, z_3\}$.

Étape topologique. — Les formules décrivant l'action de monodromie rappelée à la section 4.3.2 étant on ne peut plus explicites, cette étape ne pose guère de difficulté calculatoire. Il convient simplement d'être soigneux dans le choix des différentes bases homotopiques afin de suivre le morphisme $\mathbb{P}^1 \setminus \{z_1, z_2, z_3\} \to \mathcal{U}^4$ au niveau des groupes fondamentaux. C'est un exercice de topologie élémentaire. À l'issue de cette étape, nous sommes en mesure d'énoncer :

Proposition 4.3 (H. & Riboulet-Deyris (2003)) *La courbe $\mathcal{H}'_{(z_1,z_2,z_3)}$ est irréductible, de genre zéro et $\mathbb{Q}$-isomorphe à $\mathbb{P}^1_{\mathbb{Q}}$. De plus le revêtement $\mathcal{H}'_{(z_1,z_2,z_3)} \to \mathbb{P}^1$ est ramifié en z_1, z_2, z_3 avec comme type de ramification :*

$$\begin{cases} \left(\left(\frac{n}{2}, \frac{n}{2} - 1, \frac{n}{2} - 2\right), \left(5, 1^2, 2^{\frac{3n}{4}-5}\right), \left(3, 2^{\frac{3n}{4}-3}\right)\right) & \text{si } 4 \mid n, \\ \left(\left(\frac{n}{2}, \frac{n}{2} - 1, \frac{n}{2} - 2\right), \left(5, 1, 2^{\frac{3(n-6)}{4}}\right), \left(3, 1, 2^{\frac{3n-14}{4}}\right)\right) & \text{si } 4 \nmid n. \end{cases}$$

On est d'ores et déjà rassuré sur la pertinence du choix de la courbe de Hurwitz. En effet, étant $\mathbb{Q}$-isomorphe à $\mathbb{P}^1_{\mathbb{Q}}$, on est dans le cas le plus favorable du point de vue des calculs et de la recherche de points rationnels.

Indépendemment de l'action de tresses, notons que la topologie nous donne un autre renseignement concernant les éléments de notre famille.

Profitant de la continuité de la conjugaison complexe, on peut facilement lire sur la description en cycles de branchement si un revêtement de la famille est oui ou non défini sur $\mathbb{R}$ et mieux s'il possède des fibres totalement réelles. Parmi les $3(\frac{n}{2}-1)$ descriptions en cycle de branchement, on a donc été en mesure d'en spécifier un qui possède un intervalle de points à fibres totalement réelles. Nous mettrons cette connaissance à profit afin de construire des polynômes totalement réels de groupe de Galois $\mathcal{S}_n$. Nous évoquerons à nouveau ce type de critère combinatoire pour la descente à $\mathbb{R}$ dans le chapitre 5.

4.4.3 Le modèle algébrique final

Je passe sur la description de l'étape géométrique, préférant m'étendre sur cette dernière à l'occasion de l'évocation du second exemple (cf. sections 4.5.3 et 4.5.4). Elle est néanmoins précisément décrite dans l'article. Je me contente de présenter le résultat final auquel nous sommes parvenus. Nous avons conduit tous les calculs jusqu'à l'entier $n = 20$, le résultat pour $n = 6$ étant complètement déployé dans l'article. Genre zéro oblige, il consiste en deux fractions rationnelles.

La première, $H_n(T) \in \mathbb{Q}(T)$, fournit un modèle du morphisme «quatrième point de branchement» br : $\mathcal{H}'_{(z_1,z_2,z_3)} \to \mathbb{P}^1$, via $T \mapsto H_n(T)$. Elle est donc de hauteur $3(\frac{n}{2}-1)$ et ramifiée en trois points z_1, z_2, z_3 que l'on a affectés à $0, 1$ et ∞.

La seconde, $S_n(T,X) \in \mathbb{Q}(T,X)$, fournit un modèle de la fibre générique de la famille universelle $\mathcal{F} \to \mathcal{H}'_{(z_1,z_2,z_3)} \times \mathbb{P}^1$, ces deux surfaces étant fibrées sur $\mathcal{H}'_{(z_1,z_2,z_3)}$ via la première projection. Le morphisme de $\mathbb{P}^1_{\mathbb{Q}(T)} \to \mathbb{P}^1_{\mathbb{Q}(T)}$ donné par $X \mapsto S_n(T,X)$ est de degré n, de groupe de Galois $\mathcal{S}_n$, ramifié en $0, 1, \infty$ et $H_n(T)$ avec inertie $\mathbf{C}$.

En spécialisant le paramètre T à $t \in \mathcal{H}'_{(z_1,z_2,z_3)}(\mathbb{Q})$, le morphisme de $\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ donné par $X \mapsto S_n(t,X)$ est un modèle du revêtement de notre famille correspondant au point $t \in \mathcal{H}'_{(z_1,z_2,z_3)}$.

Enfin, le choix du paramètre $t \in \mathbb{Q}$ peut être explicitement affiné de telle sorte que tous les points de l'intervalle $]0, H_n(t)[$ aient des fibres totalement réelles par le revêtement $X \mapsto S_n(t,X)$. En spécialisant à nouveau, on obtient ainsi des polynômes, à coefficients rationnels, de degré n, de groupe de Galois $\mathcal{S}_n$ et totalement réels. À ma connaissance, ce sont les premiers exemples de tels polynômes en tout degrés pairs qui aient été calculés.

4.5 L'exemple $\mathcal{H}_4\left(\mathrm{PSL}_2(\mathbb{F}_8),(2a,2a,2a,3a)\right)^{\mathbf{ab/in}}$

Ce calcul fait l'objet de l'article référencé [Hal05]. On considère le groupe $G = \mathrm{PSL}_2(\mathbb{F}_8)$ agissant sur les neuf points de $\mathbb{P}^1(\mathbb{F}_8)$ ainsi que son quadruplet de classes de conjugaison $\mathbf{C} = (2a, 2a, 2a, 3a)$, où les classes de conjugaison $2a$ et $3a$ sont décrites par leur type de décomposition en cycles, à savoir $2^4 \cdot 1$ et 3^3. Autrement dit, la famille à laquelle on s'intéresse est celle des revêtements $\varphi : E \to \mathbb{P}^1$ (le X des généralités est devenu un E, genre 1 oblige) dont la clôture galoisienne $\widehat{E} \to \mathbb{P}^1$ a $\mathrm{PSL}_2(\mathbb{F}_8)$ pour groupe de Galois.

4.5.1 Choix de la courbe de Hurwitz

Dans cet exemple, on a choisi de *partiellement* ordonner les points de branchement en imposant que le quatrième point de branchement est de type $3a$. Formellement, on introduit

$$\mathcal{U}^1_3 = \left\{(\{b_1,b_2,b_3\},b_4) \mid b_i \in \mathbb{P}^1_{\mathbb{C}}, b_i \neq b_j, \text{si } i \neq j\right\},$$

puis on tire en arrière le revêtement d'espaces de Hurwitz $\mathcal{H}_4(G,\mathbf{C})^{\mathrm{in}} \to \mathcal{H}_4(G,\mathbf{C})^{\mathrm{ab}} \to \mathcal{U}_4$, le long du morphisme $\mathcal{U}_3^1 \to \mathcal{U}_4$ défini par $(\{b_1,b_2,b_3\},b_4) \longmapsto \{b_1,b_2,b_3,b_4\}$. Ensuite, afin de se ramener à une *courbe* de Hurwitz, on tire à nouveau en arrière le long de

$$\begin{array}{ccc} \mathbb{P}^1 \setminus \left\{-\frac{27}{4},0,\infty\right\} & \longrightarrow & \mathcal{U}_3^1 \\ t & \longmapsto & (\{\text{racines de } X^3+t(X+1)\},\infty) \end{array}$$

Le panorama des variétés introduites est résumé dans le diagramme

$$\begin{array}{ccccc} \mathcal{H}^{\mathrm{in}} & \hookrightarrow & \mathcal{H}_3^1(G,\mathbf{C})^{\mathrm{in}} & \to & \mathcal{H}_4(G,\mathbf{C})^{\mathrm{in}} \\ \downarrow & & \downarrow & & \downarrow \\ \mathcal{H}^{\mathrm{ab}} & \hookrightarrow & \mathcal{H}_3^1(G,\mathbf{C})^{\mathrm{ab}} & \to & \mathcal{H}_4(G,\mathbf{C})^{\mathrm{ab}} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{P}^1_{\mathbb{Q},t} \setminus \left\{-\frac{27}{4},0,\infty\right\} & \hookrightarrow & \mathcal{U}_3^1 & \to & \mathcal{U}_4 \end{array}$$

4.5.2 Passe combinatoire et action de tresses

L'opération qui consiste à ordonner les points de branchement et surtout celle consistant à «rationaliser» un point de branchement n'est pas toujours opportune dans la mesure où cela peut contribuer à faire augmenter le genre de la courbe de Hurwitz associée. Le but ultime étant de trouver un point rationnel sur cette courbe, on la préfère de genre petit, et même de genre zéro si possible.

Heureusement, l'énumération des classes de Nielsen, suivi du calcul de l'action de tresse, permet, sans difficulté notoire, de calculer le degré et type de ramification du revêtement «points de branchements». On en déduit que la courbe de Hurwitz $\mathcal{H}^{\mathrm{ab}}$ est bel et bien $\mathbb{Q}$-isomorphe à $\mathbb{P}^1_{\mathbb{Q}}$ et avec un petit effort supplémentaire, on parvient même à déterminer un modèle algébrique du revêtement «points de branchements»

Proposition 4.4 (H. (2005)) *Les courbes $\mathcal{H}^{ab}$ et $\mathcal{H}^{in}$ sont définies sur $\mathbb{Q}$, de genre zéro, et $\mathbb{Q}$-isomorphe à $\mathbb{P}^1_{\mathbb{Q}}$. Plus précisément :*

(i) le revêtement $\mathcal{H}^{ab} \to \mathbb{P}^1_{\mathbb{Q},t}$ est de degré 18, ramifié en $t=-\frac{27}{4},0$ et ∞ avec comme type de ramification $9\cdot 7\cdot 2$, $3^5\cdot 1^3$ et 2^9 et est donné par la fraction rationnelle $t=H(T)$ avec :

$$H(T) = -\frac{27}{4}\frac{(T+3)\left(T^2+\frac{6}{49}T+\frac{9}{49}\right)\left(T^5-\frac{9}{49}T^4-\frac{3366}{2401}T^3+\frac{2430}{2401}T^2-\frac{2187}{2401}T+\frac{2187}{2401}\right)^3}{D(T)^2}$$

$$H(T)+\frac{27}{4} = -\frac{2^{28}3^{12}}{7^{14}}\frac{T^9(T-1)^2}{D(T)^2}$$

où le polynôme D vaut

$$D(T) = T^9+\tfrac{9}{7}T^8-\tfrac{1188}{343}T^7+\tfrac{7668}{16807}T^6+\tfrac{188082}{823543}T^5+\tfrac{1246590}{823543}T^4-\tfrac{498636}{117649}T^3+\tfrac{2125764}{823543}T^2-\tfrac{531441}{823543}T+\tfrac{531441}{823543}\ ;$$

(ii) le revêtement $\mathcal{H}^{in} \to \mathcal{H}^{ab}$ est cyclique de degré 3, totalement ramifié en les deux points conjugués dont les T-coordonnées sont les racines de $T^2+\frac{6}{49}T+\frac{9}{49}$.

En revanche, à ce stade du calcul, il est impossible de calculer le $\mathbb{Q}$-modèle de ce revêtement. Pour descendre à $\mathbb{Q}$, il faut attendre le calcul du $\mathbb{Q}$-modèle de la famille universelle...exactement comme dans la théorie !

Les renseignements collectés jusqu'ici permettent de définir la classe d'isomorphisme sur $\mathbb{C}$ (et même sur $\mathbb{Q}(j)$) du revêtement $\mathcal{H}^{\mathrm{in}} \to \mathcal{H}^{\mathrm{ab}}$. En effet, le degré, les points de ramification, ainsi

que les indices associés, du revêtement $\mathcal{H}'^{\mathrm{in}} \to \mathcal{H}^{\mathrm{ab}}$ sont connus. C'est un revêtement cyclique de degré 3 ramifié en deux points et donc entièrement déterminé, sur $\mathbb{C}$!, par une fraction rationnelle (à un cube près). En revanche, pour ce qui est du $\mathbb{Q}$-modèle, de nature purement arithmétique, la combinatoire n'est plus d'aucun secours. C'est grâce à la famille universelle que l'on a été en mesure en calculer ce $\mathbb{Q}$-modèle. D'un point de vue théorique, on peut remarquer qu'il en est exactement de même. Fried et Volklein [FV91] établissent la $\mathbb{Q}$-structure grâce à la famille universelle. Quand un cas particulier illustre des considérations bien plus générales.

4.5.3 La dégénérescence et sa déformation

Les revêtements composant notre famille étant sans automorphisme, on sait qu'il existe une famille universelle. Après restriction à la courbe de Hurwitz, cette sous-famille, notée $\mathcal{E}$, est une surface quasi-projective lisse définie sur $\mathbb{Q}$ avec un morphisme :

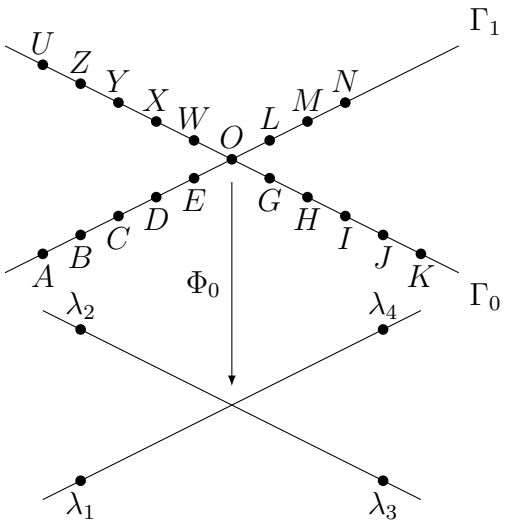
$$\Phi : \mathcal{E} \to \mathcal{H}^{\mathrm{ab}} \times \mathbb{P}^1,$$

de telle sorte que pour tout $h \in \mathcal{H}^{\mathrm{ab}}$, la fibre $\Phi_h : \mathcal{E}_h \to \mathbb{P}^1$ est un modèle sur $\mathbb{Q}(h)$ de la classe d'isomorphisme associée à h. Composée avec la première projection, le morphisme Φ fournit un morphisme $\mathcal{E} \to \mathcal{H}^{\mathrm{ab}}$ faisant de $\mathcal{E}$ une *surface arithmétique*. C'est dans cette surface que nous allons nous placer pour effectuer nos calculs.

C'est une surface ouverte et nous allons plutôt nous placer sur son bord, en l'occurrence au dessus de la dégénérescence correspondant à la valeur du paramètre $T = 0$. Afin de disposer de sections dans la surface, nous avons été amené à effectuer une extension de la base et à travailler sur $\mathbb{Q}[[\mu]]$ une extension de degré 2 de $\mathbb{Q}[[T]]$. La maxime selon laquelle *plus il pèse de contraintes sur les objets paramétrés, plus l'espace des modules est compliqué* prend alors tout son sens.

On note encore $\Phi : \mathcal{E} \to \mathrm{Spec}(\mathbb{Q}[[\mu]])$ la surface elliptique obtenue à partir de la famille universelle après localisation. On note $\mathcal{E}_\eta$ et $\mathcal{E}_0$ les fibres générique et spéciale.

Grâce à l'action de tresses, on est en mesure de déterminer la fibre spéciale $\mathcal{E}_0$. Elle est réunion de deux composantes irréductibles, l'une Γ_0 de genre zéro, l'autre Γ_1 de genre 1. L'action de tresse nous donne aussi comment s'intersectent ces deux composantes ; ici on a $\Gamma_0 \cdot \Gamma_1 = 1$. On est aussi en mesure de déterminer comment se spécialise le morphisme Φ en $\mu = 0$.



Sur chaque composante, la spécialisation Φ_0 n'est plus un revêtement de $\mathbb{P}^1$ ramifié en quatre points mais en seulement trois (deux parmi les quatre ont coalescé). Cela nous facilite grandement la tache pour calculer des modèles algébriques des chacun des revêtements $\Gamma_i \to \mathbb{P}^1$.

Il convient ensuite de recoller ces deux modèles afin d'obtenir un modèle de la fibre spéciale $\mathcal{E}_0$. On le fait de façon heuristique. Pour cela, on définit des fonctions par leur diviseur sur la fibre

générique, ou ce qui revient au même par leur partie horizontale sur la surface $\mathcal{E} \to \mathrm{Spec}(\mathbb{Q}[[\mu]])$. Grâce à un calcul d'intersection sur cette surface, on en déduit la partie verticale de chacun de ces diviseurs principaux. On connaît alors exactement la puissance de l'uniformisante μ par laquelle il faut multiplier chaque fonction pour avoir une spécialisation non constante sur chacune des composantes de la fibre spéciale. Cela permet de raccrocher les fonctions au modèle algébrique de la fibre spéciale préalablement calculé grâce à l'action de tresse. À l'issue de cette étape, on a calculé le premier ordre du modèle algébrique.

Il faut ensuite le déformer afin d'obtenir ce même modèle mais à un ordre aussi grand que souhaité. Pour cette étape, on profite du fait que l'espace total est une courbe elliptique. Cela nous permet de calculer les valeurs de certaines fonctions. On procède pas-à-pas ce qui nous permet à chaque étape de n'avoir à résoudre que des *systèmes linéaires*. On voit ici l'un des apports principaux du point de vue «déformation» comparé à un calcul plus «force brute» de résolution d'un système algébrique définissant notre famille à la Gröbner. A l'issue de cette étape, on peut considérer que l'on a calculé un modèle analytique de notre famille au voisinage de $T = 0$ (en fait $\mu = 0$ car on travaille sur une extension de $\mathcal{H}$).

4.5.4 Le modèle algébrique final

Pour achever le calcul, il reste à déduire du modèle local précédent, un modèle global. Pour cela, on commence par montrer abstraitement l'existence d'un modèle cubique dans $\mathbb{P}^2_{\mathbb{Q}(\mathcal{H})}$ de la fibre générique $\mathcal{E}_\eta$ de $\mathcal{E}$. Ce modèle résulte classiquement de l'existence de deux fonctions de degré 3 dont on connaît les diviseurs. En utilisant le modèle analytique à peine calculé, on est en mesure de développer μ-adiquement tous les coefficients de l'équation reliant les deux fonctions de degré 3. Ces coefficients sont connus pour être des fractions rationnelles en T dont on connaît aussi le développement μ-adique. Il s'agit alors de trouver des relations algébriques entre deux séries. C'est facile.

Notons que les développements de Couveignes [Cou00] permettent d'estimer la hauteur de chacun des coefficients. On dispose d'une borne pour les degrés des relations algébriques cherchées.

Le modèle algébrique le plus abouti que l'on ait obtenu du revêtement $\mathcal{E} \to \mathcal{H}$ est donné par la cubique (ce n'est pas le modèle figurant dans l'article initial [Hal05] mais plutôt celui figurant dans la suite donné à ce travail [Hal09]) :

$$\begin{aligned} E(f,g,h) = {} & \left(T^3 + \tfrac{531}{223}T^2 + \tfrac{189}{223}T + \tfrac{81}{223}\right) f^3 - \left(T + \tfrac{3}{5}\right) f^2 g \\ & - \left(T^2 + \tfrac{18}{37}T + \tfrac{9}{37}\right) f^2 h + \frac{7 \cdot 223 \left(T + \frac{9}{7}\right)}{2^2 3 \cdot 5 \cdot 37 (T+3)} fgh \\ & + \frac{163 \cdot 223 \left(T^2 + \frac{84}{163}T + \frac{81}{163}\right)}{3 \cdot 5^2 37^2 (T+3)} fh^2 \\ & + \frac{223^2}{2 \cdot 3^3 5^3 7^2 (T+3)(T^2 + \frac{6}{49}T + \frac{9}{49})} g^3 \\ & - \frac{2 \cdot 223}{3^2 5^3 37^2 (T+3)} gh^2 - \frac{2^3 7 \cdot 223^2 \left(T^2 - \frac{48}{7}T + 97\right)}{3^3 5^3 37^3 (T+3)^2} h^3. \end{aligned}$$

C'est un modèle minimal dans le sens où toutes les fibres sont des courbes de genre 1 ; autrement dit le morphisme $\mathcal{E} \to \mathcal{H}$ est lisse. On le vérifie en calculant l'analogue pour les cubiques planes, du discriminant pour les cubiques de Weierstrass ; il vaut

$$\Delta = \frac{3^{12} 223^{12}}{2^3 5^{24} 7^8 37^{12}} \frac{(T-1)^{13}}{(T+3)^{12} (T^2 + \frac{6}{49}T + \frac{9}{49})^4},$$

et son support ne rencontre pas $\mathcal{H}$.

On a aussi calculé la fonction $\varphi \in \mathbb{Q}(\mathcal{H})(\mathcal{E})$ qui est telle que $\mathcal{E}_\eta \xrightarrow{\varphi} \mathbb{P}^1_{\mathbb{Q}(T)}$ est de degré 9, de groupe de Galois (géométrique) égal à $\mathrm{PSL}_2(\mathbb{F}_8)$, ramifié en quatre points $\varphi = \infty$ de type 3^3, et φ égal à l'une des racines de $X^3+H(T)(X+1)$ de type $2^4\cdot 1$, où la fraction rationnelle $H \in \mathbb{Q}(T)$ a été calculée dans la proposition 4.4).

4.5.5 Fin du calcul et polynômes totalement réels

À mon goût, la spécificité la plus savoureuse de cette famille réside dans le fait qu'elle met en lumière la nécessaire distinction entre les espaces de Hurwitz $\mathcal{H}^{ab}$ et $\mathcal{H}^{\mathrm{in}}$.

À la fin de la section 4.5.1, la topologie nous avait laissée un peu désoeuvré avec un modèle du revêtement $\mathcal{H}^{in} \to \mathcal{H}^{\mathrm{ab}}$ sur $\mathbb{C}$ mais dans l'incapacité de descendre sur terre, euh sur $\mathbb{Q}$. Connaissant la ramification de ce revêtement cyclique de degré 3 (grâce à l'action de tresses), il est facile de voir qu'on le connaît à une constante de $\mathbb{Q}(j)^*$ près. Cette constante nous est maintenant accessible, grâce au $\mathbb{Q}$-modèle de la famille universelle.

En spécialisant la famille en une valeur du paramètre T rationnelle, on obtient un revêtement de $\mathbb{P}^1_{\mathbb{Q}}$ de groupes de Galois *géométrique* égal à $\mathrm{PSL}_2(\mathbb{F}_8)$ et de groupe de Galois *arithmétique* égal à $\mathrm{PSL}_2(\mathbb{F}_8)$ si cette valeur est totalement décomposée dans $\mathcal{H}^{\mathrm{in}}$ et à $P\Gamma L_2(\mathbb{F}_8)$ si cette valeur est inerte dans $\mathcal{H}^{\mathrm{in}}$.

Enfin en spécialisant judicieusement un tel revêtement, on obtient dans le premier cas :

Proposition 4.5 (H. (2005)) *Le polynôme :*

$$\begin{aligned} &x^9 - 4x^8 - 23908787388x^7 - 759515260327432x^6 \\ &\quad + 1580037311850766399 33x^5 + 952261161378623989643982 0x^4 \\ &\quad - 827738782216529877093838210 92x^3 - 167307009896512243981112148712743 84x^2 \\ &\quad - 383866034575302084802931793638509630716x \\ &\quad - 263692091645532308205828937593259228110772 8 \end{aligned}$$

est totalement réel et a $\mathrm{PSL}_2(\mathbb{F}_8)$ *pour groupe de Galois.*

Dans le second cas, cela permet de produire des polynômes totalement réels de groupe Galois $P\Gamma L_2(\mathbb{F}_8)$ comme c'est fait dans l'article mais je ne pousserai pas le vice jusqu'à le faire figurer ici.

4.5.6 Recherche d'un point «modulaire»

De façon assez fortuite — en écoutant un exposé de Noam D. Elkies sur le calcul de modèles de revêtements entre courbes de Shimura —, je me suis rendu compte que cette famille possède un illustre élément en son sein. Conformément au titre de l'exposé, il s'agit d'un revêtement entre courbes de Shimura. Cette observation m'a donné l'occasion de prolonger le travail précédent, le problème étant de savoir comment identifier cet élément avec comme point de départ le résultat des calculs précédents. L'idée : mettre en évidente une propriété géométrique qui le distingue ce revêtement de Shimura des autres éléments de sa famille afin de le pointer du doigt ou plutôt du calcul.

La première étape de ce travail a donc consisté à étudier en détail le revêtement de Shimura, avec pour but d'identifier une propriété géométrique qui le distingue des autres éléments de la famille.

Le revêtement de Shimura qui appartient à la famille est le revêtement $\mathcal{X}_0(2) \to \mathcal{X}(1)$ où $\mathcal{X}(1)$ est la courbe de Shimura associée à l'unique algèbre de quaternions ramifiée en deux des places réelle du corps cubique cyclique de discriminant 13^2. Ce revêtement a le bon degré, le bon groupe de Galois et la bonne donnée de ramification. De plus les trois points non ramifiés $Q_1, Q_2, Q_3 \in$

$\mathcal{X}_0(2)$ au-dessus des points de branchement de type $2^3 \cdot 1$ de $\mathcal{X}(1)$ correspondent à des points spéciaux bien identifiés.

Sur $\mathbb{C}$, Shimura et Deligne ont montré l'existence de modèles canoniques définis sur des corps de nombres bien identifiés dépendant du centre de l'algèbre de quaternions de départ et du niveau. Pour ce qui concerne, le revêtement qui nous intéresse, les résultats généraux de Shimura et Deligne stipulent qu'il admet un modèle sur K. Cependant, comme cela avait déjà été observé par Elkies et Voight [Elk98, Elk06, Voi06] pour d'autres classes d'exemples, parfois, ces courbes descendent à des corps plus petits que ceux prévus par la théorie générale des modèles minimaux. C'est le cas dans l'exemple qui nous intéresse : la descente à $\mathbb{Q}$ est possible. Autrement dit, le point de $\mathcal{H}$ que l'on recherche est un point rationnel. Pour intéressante qu'elle soit, cette information n'en demeure pas moins insuffisante dans la mesure où le fait de savoir qu'un point est rationnel n'a jamais aidé à le calculer en pratique. Il manque donc une autre spécificité. À l'instar des courbes modulaires standards, la courbe $\mathcal{X}_0(2)$ est muni d'un automorphisme involutif d'Atkin-Lehner, lui aussi défini sur $\mathbb{Q}$ (cet automorphisme n'est pas un automorphisme du revêtement $\mathcal{X}_0(2) \to \mathcal{X}(1)$ pour des questions de degré mais aussi parce que les revêtements de la famille considérée sont réputés être sans automorphisme). De plus trois des quatre points de $\mathcal{X}_0(2)$ fixés par l'automorphisme ne sont ni plus ni moins que les points Q_1, Q_2, Q_3 mentionnés précédemment. Si on choisit l'un de ces trois points comme origine de la courbe elliptique $\mathcal{X}_0(2)$, on en déduit l'égalité entre les points $2P_1 = 2P_2 = 2P_3$.

Revenons maintenant à la surface elliptique $\mathcal{E} \to \mathcal{H}$; on peut y définir les diviseurs horizontaux $\mathcal{Q}_1, \mathcal{Q}_2, \mathcal{Q}_3$ associés aux trois points non ramifiés par $\varphi : \mathcal{E}_\eta \to \mathbb{P}^1_{\mathbb{Q}(\mathcal{H})}$ au dessus des points de branchement de φ de type $2^2 \cdot 1$. Au prix d'une extension de la base, on peut supposer que l'un des diviseurs $\mathcal{Q}_i$ définisse une section de $\mathcal{E} \to \mathcal{H}$. On peut alors calculer le diviseur horizontal $\mathcal{D} = 2\mathcal{Q}_1 + 2\mathcal{Q}_2 + 2\mathcal{Q}_3$.

Enfin, on sait que $\mathcal{E}$ a une de ses spécialisation $\mathcal{E}_t$ pour $t \in \mathcal{H}(\mathbb{Q})$ telle que $\mathcal{E}_t \simeq \mathcal{X}_0(2)$ et tel que les spécialisations $\mathcal{Q}_{1,t}, \mathcal{Q}_{2,t}, \mathcal{Q}_{3,t}$ ne sont rien d'autre que Q_1, Q_2, Q_3. C'est précisément ce t que l'on cherche. Ce paramètre n'est ni plus ni moins que le point totalement ramifié du revêtement $\mathcal{D} \to \mathcal{H}$. C'est un revêtement de courbes. Identifier ce point ne pose pas de problème calculatoire.

Pour l'anecdote, le revêtement de Shimura correspond au point $T = -1$ de la famille. Compte tenu des calculs précédents, on déduit facilement de cette information un modèle explicite du revêtement de Shimura.

Proposition 4.6 (H. (2009)) *La courbe $\mathcal{X}_0(2)$ a pour équation :*

$$f^3 - f^2g - f^2 - \tfrac{25}{84}fg + \tfrac{40}{147}f - \tfrac{625}{702}g^3 + \tfrac{50}{441}g - \tfrac{640}{9261} = 0$$

et le revêtement $\mathcal{X}_0(2) \to \mathcal{X}(1)$ est donné par la fonction :

$$\varphi = -\tfrac{241129}{125}f^2g - \tfrac{36309}{125}f^2 + \tfrac{1715}{3}fg^2 + \tfrac{22099}{30}fg - \tfrac{637}{200}f - \tfrac{1715}{9}g^3 + \tfrac{1225}{36}g^2 - \tfrac{1708}{45}g - \tfrac{1301}{75}.$$

Elle est de degré 9, ramifiée en $\varphi = \infty$ et en les trois racines du polynôme $x^3 - x^2 - 992x - 20736$.

4.6 Et après ?

C'est J.Klueners qui m'a suggéré, par e-mail, d'étudier la seconde famille de groupe $PGL_2(\mathbb{F}_8)$ et d'inertie $(2a, 2a, 2a, 3a)$. Dans ce même e-mail, il mentionnait deux autres exemples susceptibles d'être intéressants.

> «The group $G = PGL_2(11)$ with :
> — inertia $\mathbf{C} = (2b, 2b, 2b, 4a)$ realization over Q(t), stem field genus 1,
> — or $\mathbf{C} = (2a, 2b, 2b, 11a)$ realization over Q(t), stem field genus 2,

> where $2a$ has cycle shape 2^6 and $2b$ has cycle shape 2^5, the other conjugacy classes are identified by their element orders.»

Je n'ai jamais eu le courage de m'y pencher — il faut avouer que l'aventure $\mathrm{PSL}_2(\mathbb{F}_8)$ m'épuisa tant elle fut semée d'embûches, d'impasses calculatoires et de rebondissements. Pourtant, ces deux exemples sont sûrement intéressants, notamment le deuxième où le genre de la courbe du haut vaut deux. Cela ajoute, à coup sûr, quelques difficultés techniques rendant le calcul attrayant.

Concernant l'application aux courbes de Shimura, il ne fait guère de doute que l'on peut calculer d'autres exemples de revêtements de courbes de Shimura avec cette méthode. La théorie des courbes et variétés de Shimura est en plein essor. Du point de vue explicite, c'est encore un terrain à défricher même si Elkies et Voight ont déjà livré quelques pistes. Certains enjeux algorithmiques vont d'ailleurs rejoindre ceux du chapitre 3

Enfin, j'ai un autre regret : je n'ai jamais utilisé les espaces de Hurwitz en caractéristique p.

Chapitre 5

Obstructions globales à la descente

Je relate ici le travail effectué en collaboration avec Jean-Marc Couveignes [CH11] sur les obstructions globales à la descente. Si des théories très avancées ont fourni des résultats assez généraux concernant les corps de modules ou de définition de certains objets algébriques, il n'en reste pas moins que les exemples concrets et explicites d'obstructions ne sont pas légion.

5.1 Obstructions à la descente pour les revêtements

Dans le chapitre précédent, sont apparues les notions de corps «*des modules*» et «*de définition*» d'un revêtement de $\mathbb{P}^1$. En particulier, étant donné un revêtement de $\mathbb{P}^1$, on a interprété le premier comme le corps de définition du point de l'espace des modules correspondant à l'objet de la famille considéré, d'où la terminologie. Sans hypothèse supplémentaire, il est aussi apparu que l'on ne peut pas affirmer que ce corps des modules est un corps de définition de l'objet correspondant. Et pour cause, il n'en est rien en général ; autrement dit, il existe des exemples de revêtements dont le corps des modules n'est pas un corps de définition. Si tel est le cas, on dit qu'il y a une *obstruction à la descente*.

En partie grâce à l'étude des espaces de Hurwitz, la catégorie des revêtements de $\mathbb{P}^1$ est assurément l'une des catégories dans laquelle la différence entre corps des modules et corps de définition a été le mieux étudiée, cernée, et mise en exergue. Voici où en sont les recherches pour ce qui concerne la zoologie des obstructions à la descente dans la catégorie des revêtements.

Tout d'abord, on connaît quelques classes de revêtements où il n'y a pas d'obstruction. Un revêtement $X \to \mathbb{P}^1$ sans automorphisme ou galoisien est toujours défini sur son corps des modules (cf. [Fri77] et [CH85, Proposition 2.5]). Dans les deux cas, la preuve de non-obstruction consiste à se ramener à utiliser le critère de descente de Weil ([Wei56]) ; la condition corps des modules permet d'exhiber un système d'isomorphismes $\varphi_\sigma : X \to {}^\sigma X$ pour tout $\sigma \in \mathrm{Gal}(L/K)$, où K désigne le corps des modules du revêtement de départ et où L est un corps de définition du revêtement, galoisien et fini sur K. Il ne reste alors plus qu'à vérifier la condition de cocycles. Celle-ci est forcément satisfaite, par unicité, dans le cas où le revêtement de départ est sans automorphisme ; dans le cas opposé où le revêtement est galoisien, on dispose d'assez de marge de manoeuvre pour ajuster les isomorphismes φ_σ de telle sorte que le nouvelle famille satisfasse la condition de cocyle.

Cependant, dans le cas galoisien, on ne prouve pas que la descente est galoisienne ; autrement dit le revêtement descendu n'est pas forcément galoisien. La cause ? C'est que les automorphismes ne sont pas, a priori, définis sur le corps des modules. D'où l'intérêt de se poser la question de l'obstruction à la descente au corps des modules dans la catégorie des G-revêtements (i.e. avec les automorphismes étiquetés). Dans l'article cité ci-avant, Coombes et Harbater fournissent un exemple de G-revêtement, pour G égal au groupe quaternionique, qui a $\mathbb{Q}$ pour corps des modules mais qui n'est pas défini sur $\mathbb{Q}$. Depuis ce résultat, l'obstruction à la descente a été assez finement

étudiée. Dèbes et Douai l'ont en particulier très précisément décrite en termes cohomologiques. Cela les a conduit, par exemple, à établir qu'un G-revêtement est défini sur son corps des modules si et seulement s'il l'est sur tous ses complétés (cf. [DD97]).

Enfin dans la catégorie des revêtements purs, les premiers exemples d'obstructions à la descente remontent à une série d'articles de Couveignes ([Cou97, CG94, Cou94]) puis d'autres de Fried et Dèbes ([DF94]). Dans la plupart des exemples la non descente au corps des modules est montrée localement, c'est-à-dire que l'on prouve que le revêtement ne peut pas être défini sur son corps des modules dans la mesure où ce n'est pas vrai quand on complète judicieusement le corps de base. Pour cette stratégie, la non descente de $\mathbb{C}$ à $\mathbb{R}$ s'est montrée «bonne joueuse» et a permis de construire un nombre conséquent d'obstructions. La raison du succès de ce complété par rapport aux autres réside dans le fait que, grâce à la topologie et à la continuité de la conjugaison complexe, on dispose d'un critère purement combinatoire en terme de monodromie pour certifier si $\mathbb{R}$ est corps des modules ou de définition d'un revêtement : partant d'un revêtement $\varphi : X \to \mathbb{P}^1_{\mathbb{C}}$ de degré n, à points de branchement réels pour simplifier, et donné par sa monodromie, on détermine la monodromie du conjugué de φ (pour la conjugaison complexe) puis on en déduit que $\mathbb{R}$ est corps des modules de φ si et seulement si les deux monodromies sont conjuguées par un élément de $\mathcal{S}_n$, alors que le corps $\mathbb{R}$ est corps de définition de φ si et seulement si les deux monodromies sont conjuguées par un élément d'ordre 2.

Toujours dans la catégorie des revêtements purs, Dèbes et Douai ont poursuivi leur approche cohomologique et ont donné une description l'obstruction en termes de H^2. Cette description est nettement plus délicate que celle pour les G-revêtements (cf. [DD97]).

Choisissons pour corps de base un corps global, disons $\mathbb{Q}$ pour fixer les idées. Malgré une diversité non démentie, toutes les obstructions évoquées jusqu'ici sont qualifiées de *locales*. Autrement dit la non-descente au corps des modules provient du fait que la non descente au corps des modules est déjà avérée quand on étend les scalaires à au moins un des complétés du corps des modules. Il s'est naturellement posée la question de savoir s'il existe des obstructions dites *globales*, c'est-à-dire des exemples de revêtements de corps des modules $\mathbb{Q}$, définis sur tous les complétés de $\mathbb{Q}$ mais pas sur $\mathbb{Q}$ lui même.

On a déjà rappelé qu'il n'en est rien dans la catégorie des G-revêtements. En revanche, la réponse est positive dans la catégorie des revêtements purs et c'est un résultat montré par Couveignes et Ros [CR04, Corollaire 2].

Théorème 5.1 (Couveignes & Ros (2004)) *Il existe un $\mathbb{Q}$-revêtement ramifié et connexe de $\mathbb{P}^1_{\mathbb{Q}}$ qui a $\mathbb{Q}$ pour corps des modules, qui est défini sur tous les complétés de $\mathbb{Q}$ mais qui ne l'est pas sur $\mathbb{Q}$ lui même.*

En conséquence le tableau des obstructions à la descente dans la catégorie des revêtements est assez complet.

5.2 Obstructions à la descente pour les courbes

Les notions de corps des modules et de définition ne se limitent évidemment pas à la catégorie des revêtements. On peut très bien définir les notions de corps des modules et de définition d'une variété en général.

Pour ce qui est des courbes (projectives, lisses, absolument irréductibles), se pose alors à nouveau la question de savoir si elle peut oui ou non être définie sur son corps des modules.

Une nouvelle fois, la réponse à cette question est *non* en général. Cependant les exemples d'obstructions dans la catégorie des courbes restent moins nombreux et variés que dans celle des revêtements.

À ma connaissance, une des premières mentions, dans la littérature, du fait que le corps des modules d'une courbe puisse ne pas être un corps de définition figure dans Shimura [Shi71, DE99]. Il s'était aperçu du phénomène en construisant les modèles canoniques des courbes de Shimura.

Mais le premier article étudiant en détail les obstructions remonte au début des années 90 avec l'article de Mestre [Mes91]. Ce n'est évidemment pas un hasard, si l'obstruction à la descente apparaît lors de la construction d'un modèle de la courbe à partir de son module dans $\mathcal{M}_2$ l'espace des modules des courbes de genre 2 (plus précisément, l'article se restreint à l'ouvert de $\mathcal{M}_2$ correspondant aux courbes ne possédant pas d'autres involutions que l'hyperelliptique). Il s'agit du même phénomène que celui déjà rencontré dans le contexte des espaces de Hurwitz (cf. théorème 4.2). Toujours est-il, qu'étant donné k un corps de base parfait de caractéristique distincte de 2, et à partir d'un module d'une courbe de genre 2 défini sur k, Mestre construit une conique sur k et montre que cette conique admet un point rationnel sur k si et seulement si la courbe correspondant au point de l'espace des modules admet un modèle sur k. La construction est complètement explicite et Mestre en déduit des exemples de courbes de genre 2 de corps des modules $\mathbb{Q}$ mais non définissable sur $\mathbb{Q}$. Plus précisément, il est en mesure de spécifier une extension quadratique de $\mathbb{Q}$ sur laquelle la courbe admet un modèle. Récemment, Lercier et Ritzenthaler [LR12] ont poursuivi ce travail et ont généralisé les constructions explicites en genre plus grand que deux. Cela les a conduit, eux aussi, a donner des exemples de courbes qui ne sont pas définies sur leur corps des modules.

Cependant toutes ces obstructions rentrent dans la catégorie des obstructions dites *locales* et à l'instar du travail effectué dans la catégorie des revêtements, on aimerait étoffer le catalogue des obstructions à la descente pour les courbes.

Il est évidemment tentant d'essayer de profiter de l'expertise acquise dans la catégorie des revêtements pour aboutir à différents types d'obstructions à la descente dans la catégorie des courbes.

C'est la stratégie suivie par Dèbes et Emsalem dans leur article consacré au corps des modules d'une courbe [DE99]. Essentiellement, ils relient l'obstruction à la descente pour une courbe X à celle pour le revêtement $X \to X/\operatorname{Aut}(X)$.

Notre travail s'inscrit dans cette stratégie mais dans un esprit sensiblement différent. L'objectif est de fournir un exemple d'obstruction *globale* à la descente dans la catégorie des courbes lisses et complètes. L'idée est de partir du théorème 5.1 fournissant un exemple de telle obstruction dans la catégorie des revêtements. On veut faire migrer cette obstruction vers d'autres catégories. On peut distinguer deux aspects dans ce travail. Tout d'abord, on présente diverses constructions géométriques permettant de passer d'une catégorie à une autre. Ensuite on assure le transfert des propriétés de module et de définition, c'est-à-dire que l'on prouve que ces propriétés ne sont pas altérées lors des constructions introduites.

Les constructions relèvent de la géométrie algébrique classique dont on utilise certains outils standards comme le produit fibré, les revêtements, la normalisation, les déformations.

Afin de prouver les bonnes propriétés de transfert, nous avons fait usage des champs et gerbes des modèles des objets considérés. L'introduction de ce formalisme, outre le fait qu'il nous rapproche des travaux de Dèbes et Douai [DD99], nous a permis de dissocier l'aspect transfert de l'aspect construction. Pour ce qui me concerne, cela m'a permis de rentrer un peu dans le domaine des champs et des gerbes que je trouvais très obscur avant d'y être confronté pour ce travail.

5.3 Les constructions géométriques

Le point de départ est donc un revêtement $\varphi : Y \to \mathbb{P}^1$ possédant des propriétés de modules et de définition intéressantes, par exemple, celui du théorème 5.1. Au moyen de diverses constructions géométriques (quatre pour être précis), il s'agit de passer de la catégorie des revêtements

de $\mathbb{P}^1$ à d'autres catégories.

Pour pouvoir appliquer le théorème de transfert sur lequel nous revenons dans la section suivante, il convient de veiller à ce que les constructions aient de bonnes propriétés fonctorielles pour ce qui est des extensions des scalaires. D'autre part, il est préférable que ces constructions préservent le groupe d'automorphismes des objets considérés ; si tel n'est pas cas, il convient au moins de maîtriser la variation du groupe d'automorphismes. En effet, les exemples d'obstructions à la descente dans la catégorie des revêtements de courbes nous enseignent l'importance du groupe d'automorphismes : s'il est «tros gros» ou «tros petit», il n'a pas d'obstruction. Du coup, une trop forte variation du groupe d'automorphismes des objets construits pourrait tuer l'obstruction.

L'intérêt des premières constructions réside précisément dans le fait qu'elles vont faciliter le travail de contrôle du groupe d'automorphismes dans les constructions ultérieures. L'idée est de faire fondre le groupe d'automorphismes des objets considérés, en veillant tout de même à ce qu'il ne devienne pas trivial pour ne pas tuer les obstructions à la descente. Dans cette optique-ci, la première étape consiste à remplacer la courbe de base $\mathbb{P}^1$ par une autre courbe de base X qui ne possède pas d'automorphisme non trivial. Au moyen d'un produit fibré adéquat, on parvient à passer du revêtement $\varphi : Y \to \mathbb{P}^1$ de départ à un revêtement $\psi : Y' \to X$ où X est de genre au moins deux sans automorphisme non trivial. Au passage, on a aussi montré que l'on peut aussi multiplier le degré du revêtement considéré par un entier aussi grand que souhaité. C'est un détail technique qui se révélera pourtant utile dans la suite.

La deuxième construction a consisté à passer d'un revêtement $\varphi : Y \to X$ comme précédemment à une surface quasi-projective lisse. Cette construction est assez naturelle puisqu'elle consiste simplement à considérer ce que l'on a appelé l'*empreinte* du revêtement φ, c'est-à-dire le complémentaire dans la surface $X \times Y$ du graphe du revêtement φ.

Le but de la troisième construction est de passer de la surface quasi projective précédente à une autre surface qui est propre et normale. Un bon candidat pour une telle surface est obtenue en considérant une surface qui revêt $X \times Y$ par un revêtement abélien ramifié le long du graphe du revêtement φ.

L'ultime étape consiste à construire une courbe lisse projective à partir de la surface précédente. Pour cela, on commence par dessiner sur cette surface une courbe non lisse mais stable. La courbe lisse est alors obtenue par déformation de cette dernière.

Pour chacune de ces construction géométriques, il convient à chaque fois de contrôler le groupe d'automorphismes des nouveaux objets construits.

5.4 Champ et gerbe des modèles d'une variété

Le deuxième aspect de ce travail consiste à montrer que les propriétés de modules et de définition sont préservées au cours de toutes les constructions précédentes. Sur suggestion d'un rapporteur d'une première version de ce travail, nous avons été convaincu que le bon formalisme pour traiter ce genre de question est celui des champs et des gerbes. Plus précisément, nous avons utilisé le champ, puis la gerbe des «modèles» d'une variété. Les guillemets sont là pour signifier, que les objets de cette catégorie sont les modèles de la variété de départ *au sens large*, c'est-à-dire incluant les modèles standards mais aussi les modèles de ses conjugués. Ce champ est un exemple non trivial de champ et/ou de gerbe qui, semble-t-il, fait partie du folklore du domaine, sans pour autant faire l'objet, à notre connaissance, d'une présentation dans un ouvrage ou une publication. Une importante partie de ce travail a donc consisté à décrire en détail ce champ ainsi que cette gerbe.

La catégorie des «modèles» d'une variété. — Soit k un corps de caractéristique zéro dont on note k^a la clôture algébrique. Étant donnée X une variété sur k^a, on lui associe la catégorie $\mathbb{M}_X$ des «modèles» de X : c'est une *catégorie fibrée* sur le site étale de k dont les objets sur l extension de k ne sont rien d'autres que les l-modèles de X ou d'une de ses conjuguées

(d'où les guillemets). Le fait de considérer les modèles au sens large assure la stabilité par tirés en arrière le long des morphismes du site étale de k. On dispose alors d'un foncteur fibre $\mathbb{M}_X(l)$ défini pour toute k-extension (ou toute k-algèbre étale) l. Dire que la fibre $\mathbb{M}_X(l)$ est non vide revient à dire que X admet un «modèle» sur l.

Champs versus Gerbes. — Si maintenant X fait partie des variétés pour lesquelles les données de descentes sont effectives, alors la catégorie fibrée $\mathbb{M}_X$ est un *champ*. C'est le cas des variétés affines ou projectives et c'est encore une conséquence de la descente de Weil ([Wei56]).

Enfin dans ce formalisme, la condition corps des modules est équivalente au fait que le champ des «modèles» $\mathbb{M}_X$ est une *gerbe*.

Transferts. — Aidés de ce formalisme, on peut maintenant énoncer le théorème de transfert qui nous a permis de passer d'une catégorie à une autre dans les constructions précédentes.

Proposition 5.2 (Couveignes & H. (2011)) *Soit X et Y des $\overline{k}$-variétés ou des revêtements de courbes. S'il existe un morphisme de champs $\mathbb{F} : \mathbb{M}_X \longrightarrow \mathbb{M}_Y$ alors :*

- *si k est corps des modules de X alors k est corps des modules de Y ;*
- *si l est un corps de définition de X alors l est un corps de définition de Y.*

Si de plus k est le corps des modules de X et si $\mathbb{F}$ est pleinement fidèle, alors :

- *le corps l est un corps de définition de X si et seulement si le corps l est un corps de définition de Y.*

On a donc ramené la preuve de la préservation des propriétés de modules et de définition dans les constructions précédentes à la vérification qu'elles induisent un morphisme sur les champs des modèles sous-jacents. Cela consiste essentiellement à vérifier de bonnes propriétés de fonctorialité vis-à-vis de l'extension des scalaires. Quant à la pleine fidélité, elle consiste précisément à vérifier que les groupes d'automorphismes des objets restent inchangés.

5.5 Les catégories visitées

Outre l'objectif initial des courbes projectives lisses, la preuve nous apprend l'existence d'obstructions dans les catégories suivantes :

Théorème 5.3 (Couveignes & H. (2011)) *Il existe des obstructions globales à la descente dans les catégories :*

- *des revêtements de courbes sur $\mathbb{Q}$;*
- *des surfaces quasi-projectives lisses sur $\mathbb{Q}$;*
- *des surfaces propres et normales sur $\mathbb{Q}$;*
- *des courbes projectives lisses sur $\mathbb{Q}$.*

5.6 Et après ?

Une question qui m'a souvent été posée lorsque que j'ai eu la possiblilité d'exposer ce résultat lors de séminaires est la suivante *la courbe finale est-elle explicite* ? Dans une certaine mesure, je peux répondre positivement à cette question dans la mesure où le revêtement de départ est explicite et où toutes les constructions décrites ci-avant le sont aussi. Cela étant, nous ne pouvons fournir un modèle explicite sous la forme d'un système d'équations définissant cette courbe dans un certain espace projectif. Le faire demanderait un effort supplémentaire assez consistant. . .faute d'être très intéressant.

Plusieurs théories fournissent des obstructions potentielles à la descente. La théorie des invariants, comme l'ont montré les travaux de Mestre, suivis de ceux de Lercier et Ritzenthaler [Mes91, LR12]. Il semblerait que toutes ces obstructions soient locales. Cela reste à vérifier.

La théorie des modèles canoniques des courbes de Shimura (encore elles !) permettent aussi d'illustrer le phénomène de non descente à son corps des modules. Le seul exemple de ce type que je connaisse est encore une obstruction locale. Le sont-elles toutes ?

Chapitre 6

À notre tour

En collaboration avec Marc Perret, je me suis plus récemment intéressé aux tours récursives de corps de fonctions sur un corps fini ; un premier article a déjà été soumis il y a plusieurs mois ([HP13]), d'autres sont en préparation.

À la différence du chapitre précédent où les exemples explicites d'obstructions à la descente se font assez rares, les exemples de tours de corps de fonctions explicites sur $\mathbb{F}_q$ fournissant une minoration non triviale de $A(q)$ sont légion. Pour autant, hormis des tentatives d'Elkies [Elk01], Beelen [Bee04, BB05], Lenstra [Len02], peu d'études un tant soit peu générales, permettant de comprendre les spécificités des bonnes tours, ont vu le jour. Nous avons essayé de donner de nouvelles clés de compréhension et avons surtout introduit un nouvel outil permettant d'appréhender ces tours. Nous leur associons un *graphe infini orienté*.

6.1 La constante $A(q)$ pour q puissance d'un premier

Une des conséquences de la célèbre hypothèse de Riemann pour les courbes sur un corps fini, est la non moins célèbres majorations de Weil, améliorée par Serre :

$$N_q(X) \leqslant q + 1 + g\lfloor 2\sqrt{q} \rfloor \leqslant q + 1 + 2g\sqrt{q}, \tag{6.1}$$

où X désigne une courbe (lisse, absolument irréductible) sur $\mathbb{F}_q$, de genre g et possédant $N_q(X)$ points définis sur $\mathbb{F}_q$. Immédiatement s'est posée la question de l'optimalité de cette majoration. Asymptotiquement, c'est-à-dire quand le genre g tend vers l'infini, l'inégalité s'avère *non optimale*. C'est ce qu'ont montré Drinfeld et Vladut [VD83]. Plus précisément, pour q puissance d'un premier, ils ont introduit les quantités :

$$N_q(g) = \max_{\substack{X \text{ courbe lisse} \\ \text{sur } \mathbb{F}_q, \text{ de genre } g}} N_q(X) \qquad \text{et} \qquad A(q) = \limsup_{g \to +\infty} \frac{N_q(g)}{g}$$

et ont prouvé que :

$$A(q) \leqslant \sqrt{q} - 1. \tag{6.2}$$

Si la non optimalité de l'inégalité 6.1 en découle, se pose alors à nouveau la question de l'optimalité de la nouvelle inégalité asymptotique 6.2. Pour q carré, Tsfasman, Vladut et Zink [TVZ82] ont établi l'égalité $A(q) = \sqrt{q} - 1$. La question reste ouverte pour q non carré et est à l'origine de nombreux travaux.

Une des stratégies les plus fructueuses a été la recherche de tours explicites donnant une minoration non triviale de $A(q)$. Cela a donné lieu à de très nombreuses publications.

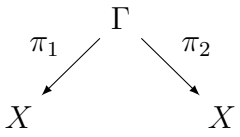
Le premier grand succès date de 1985 avec l'Inventiones de Garcia et Stichtenoth [GS95], où ils donnent une tour de type Artin-Schreier permettant de remontrer l'égalité $A(q) = \sqrt{q} - 1$ pour q carré. Depuis un nombre conséquent de mathématiciens se sont livrés au petit jeu consistant à

trouver une tour récursive explicite donnant une minoration non triviale de $A(q)$. Le Graal, en la matière, étant de donner une minoration non triviale de $A(p)$ pour p premier. La majeure partie de ces exemples sont dus à Garcia et Stichtenoth accompagnés de divers collaborateurs [BS07, BGS08, BGS05a, GSR03, GS95, BGS05b]...

6.2 Définition et invariants des tours récursives explicites

La définition d'une *tour récursive explicite* requiert uniquement deux données :
— une *courbe de base* X définie sur $\mathbb{F}_q$, projective, lisse, et absolument irréductible,
— et une *correspondance* Γ sur X elle aussi définie sur $\mathbb{F}_q$, absolument irréductible, réduite (mais pas forcément lisse), ni horizontale, ni verticale, et de *type* (d,d).

Précisons le sens des trois dernières hypothèses concernant Γ. Elles sont toutes relatives à la surface produit $X \times X$ dans laquelle Γ est plongée. Les deux projections sur chacune des composantes $\pi_i : X \times X \to X$, définies par $\pi_i(P_1, P_2) = P_i$ pour $i = 1, 2$, induisent le diagramme :



On note H et V les diviseurs horizontal et vertical de $X \times X$, c'est-à-dire les deux diviseurs fibres de π_1 et π_2. L'hypothèse selon laquelle Γ n'est ni horizontale ni verticale veut dire qu'elle n'est pas équivalente à H ou V. Quant au type (d,d), cela veut dire que $\Gamma \cdot H = \Gamma \cdot V = d$ (où $D \cdot D'$ désigne le produit d'intersection sur $X \times X$). Comme Γ n'est ni horizontale ni verticale, par restriction, π_1 et π_2 induisent deux morphismes non constants de Γ dans X.

La tour $\mathcal{T}(X, \Gamma)$ associée est la suite de courbes $(C_n)_{n \geqslant 1}$, définies par $C_1 = X$ et pour $n \geqslant 2$ par :

$$C_n = \{(P_1, \dots, P_n) \in X^n \mid (P_i, P_{i+1}) \in \Gamma,\ \forall i = 1, \dots, n-1\}.$$

Chaque courbe C_n est donc naturellement plongée dans X^n. De plus, il s'agit bien d'une tour dans la mesure où les applications $(P_1, \dots, P_n) \mapsto (P_1, \dots, P_{n-1})$ définissent des morphismes (non constants) de C_n vers C_{n-1}.

Les courbes C_n sont, a priori, singulières. On note $(\widetilde{C}_n)_n$, la suite des courbes désingularisées, g_n leur genre (géométrique), $N_r(\widetilde{C}_n)$ et $B_r(\widetilde{C}_n)$ les nombres de points de $\widetilde{C}_n$ respectivement définis sur $\mathbb{F}_{q^r}$ et de degré r sur $\mathbb{F}_q$.

Les invariants intéressants de la tour sont bien sûr relatifs au modèle lisse. Il s'agit des deux limites :

$$\lambda_r(\mathcal{T}(X,\Gamma)) = \lim_{n \to +\infty} \frac{N_{q^r}(\widetilde{C}_n)}{g_n} \quad \text{and} \quad \beta_r(\mathcal{T}(X,\Gamma)) = \lim_{n \to +\infty} \frac{B_r(\widetilde{C}_n)}{g_n}.$$

On vérifie facilement que ces deux limites existent toujours. Bien sûr, pour tout $r \geqslant 1$, on a $A(q^r) \geqslant \lambda_r(\mathcal{T}(X,\Gamma))$, si bien que la tour est décrétée *bonne* dès lors que l'un de ses λ_r est non nul.

J'ai toujours été surpris de constater à quel point les exemples les plus intéressants de tours récursives explicites sont **simples** ! Comme courbe de base, il n'est pas utile de faire preuve de beaucoup d'imagination puisque $X = \mathbb{P}^1_{\mathbb{F}_q}$ est à l'origine de la quasi totalité des exemples intéressants. Quant à la correspondance Γ, elle est aussi souvent confondante de simplicité. Si $X = \mathbb{P}^1_{\mathbb{F}_q}$, elle est donnée par un polynôme $E \in \mathbb{F}_q[X_1, Y_1, X_2, Y_2]$ bi-homogène de bi-degré (d,d) absolument irréductible. Mais en fait, on le prend souvent à variables séparées. J'en veux pour preuve ma tour récursive *favorite*, évidemment due à Gracia et Stichtenoth ; elle est donnée par :

$$\frac{x^2+1}{2x} = y^2 \qquad \Longleftrightarrow \qquad E(X_1, Y_1, X_2, Y_2) = (X_1^2 + Y_1^2)Y_2^2 - 2X_1Y_1X_2^2$$

C'est la fameuse tour modérée qui permet de montrer que $A(q^2) = q - 1$ en caractéristique distincte de 2. Je la choisis comme fil conducteur de ce chapitre.

6.3 Tours récursives et Graphes

À toute tour récursive définie par les données (X, Γ) comme en §6.2, on associe un graphe orienté infini :

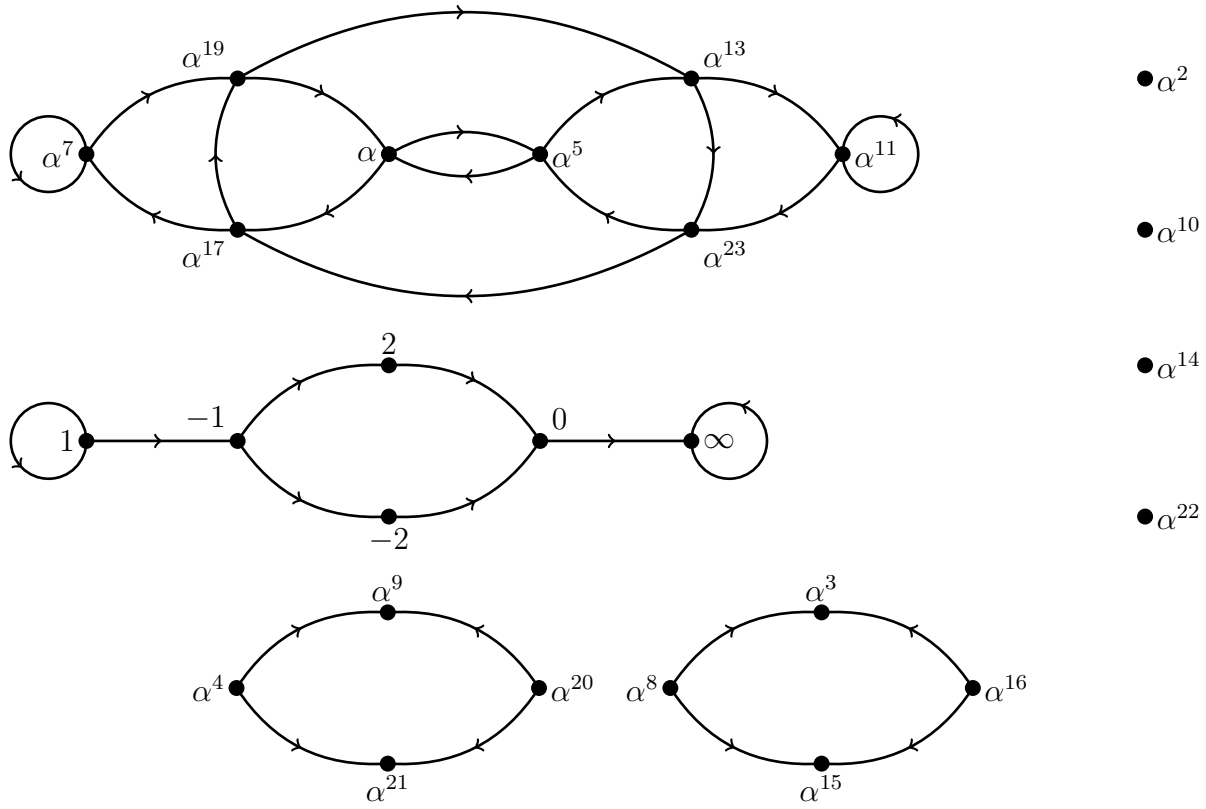
— dont les sommets sont les points géométriques $X(\overline{\mathbb{F}_q})$ de X,

— avec une arrête joignant deux points P et Q si et seulement si $(P, Q) \in \Gamma$.

On le note $\mathcal{G}_\infty(X, \Gamma)$ ou simplement $\mathcal{G}_\infty$. Ce graphe est évidemment intimement lié à la tour récursive $(C_n)_n$ associée au couple (X, Γ).

> **Remarque.** — Beelen [Bee04] a lui aussi associé un graphe à une tour récursive. Sa version diffère très légèrement de la notre. Cela étant, ce qui nous distingue de Beelen est surtout ce que nous faisons de ce graphe pour l'étude et la compréhension des phénomènes liés à une bonne tour.

C'est un graphe infini dont on va plutôt considérer certains sous-graphes. En particulier, pour $r \geqslant 1$, on définit le graphe *arithmétique* $\mathcal{G}_r(X, \Gamma)$ en restreignant l'ensemble des sommets à $X(\mathbb{F}_{q^r})$ l'ensemble des points définis sur $\mathbb{F}_{q^r}$. Voici le graphe $\mathcal{G}_2$ pour la tour qui nous sert de fil conducteur, en caractéristique 5 et où $\alpha \in \mathbb{F}_{25}$ est un générateur du groupe multiplicatif.



La première vertu du graphe est d'offrir une représentation synthétique et assez fidèle de la tour. À ce titre, il est bien plus révélateur que les équations elles mêmes.

Le degré d de chaque étage n'est ni plus ni moins que le degré sortant ou entrant commun à tous les sommets du graphe, sauf en un nombre fini d'entre eux. Les points de C_n sont en correspondance bi-univoque avec les chemins de longueur $(n-1)$ du graphe $\mathcal{G}_\infty$ (éternel décalage entre le nombre de piquets et le nombre de rambardes). En particulier, ceux de degré r se lisent tous sur le graphe $\mathcal{G}_r$.

Quant aux autres invariants plus fins, ils sont en général concentrés dans deux composantes finies connexes du graphe sur lesquelles nous nous proposons de nous attarder.

6.3.1 La composante singulière et le genre

Cette section aurait pu s'intituler *«Réinvestir la géométrie des tours récursives»* tant c'est un peu son leitmotiv. En effet, la plupart des articles sur le sujet gomment l'aspect géométrique de la construction en adoptant le langage des corps de fonctions. Nous avons souhaité prendre mieux en compte l'aspect géométrique de la construction. C'est pourquoi, nous avons distingué le modèle singulier $(C_n)_n$ de la tour, de son modèle lisse $(\widetilde{C}_n)_n$.

Ici le graphe ne nous apporte guère plus qu'un support visuel confortable même si nous avons espoir de faire bien plus (cf.§6.4).

D'ores et déjà, on y lit facilement les points singuliers des courbes C_n : il s'agit des chemin de longueur $(n-1)$ passant par un sommet $P \in X(\overline{\mathbb{F}_q})$ de degré entrant $< d$, puis par un sommet $Q \in X(\overline{\mathbb{F}_q})$ de degré sortant $< d$. Évidemment cette caractérisation visuelle des points singuliers n'est que la traduction en terme de graphes d'une caractérisation purement algébrique ; nous avons établi cette dernière grâce à une étude locale des variétés en jeu. Dans l'exemple, les points singuliers de C_n sont tous de la forme :

$$(1, \dots, 1, -1, \pm 2, 0, \infty, \dots, \infty),$$

avec la possibilité de n'avoir aucune coordonnée égale à 1 ou ∞. C'est donc à partir de $n = 3$ que les courbes C_n deviennent singulières.

La détermination des points singuliers est une étape décisive dans l'optique de calculer le genre géométrique g_n des courbes C_n à partir de leur genre arithmétique γ_n. Il est en effet classique que ces deux genres sont reliés par :

$$\gamma_n = g_n + \sum_{P \in X(\overline{\mathbb{F}_q})} \delta_P,$$

où δ_P désigne la *mesure de singularité* de C_n en P. Cette mesure vaut zéro en un point lisse, d'où la finitude de la sommation. D'autre part, en un point singulier P, la mesure de singularité δ_P se détermine grâce au calcul de la clôture intégrale de l'anneau local en P. Il se trouve que mes travaux de thèse portaient sur l'un des algorithmes les plus efficaces permettant d'effectuer ce type de calcul. J'ai ainsi eu l'occasion de renouer avec mes premiers amours de thèse ! Quant au genre arithmétique, son calcul est facilité par le fait que les courbes C_n sont plongées dans X^n. En fait, afin de se ramener à appliquer la formule d'adjonction sur une surface, nous avons plutôt calculé le genre arithmétique d'un avatar de la courbe C_n qui est plongé dans $\widetilde{C}_{n-1} \times X$. Toujours est-il que sur des cas concrets nous sommes en mesure de déterminer des formules closes pour le genre géométrique des courbes C_n. Notons que nous nous différencions ici des techniques usuelles pour évaluer le genre, à peu près toutes basées sur le théorème de Riemann-Hurwitz.

Un autre atout du point de vue consistant à considérer le modèle singulier des courbes est de permettre assez facilement de circonscrire le champs d'investigation des bonnes tours à deux cas bien distincts :

Proposition 6.1 (Perret & H. (2013)) *Soit (X, Γ) une correspondance comme au § 6.2 et soit $\mathcal{T} = (C_n)_{n \geqslant 1}$ la tour associée. Supposons que C_n est irréductible pour tout $n \geqslant 1$ et que la suite des genres $(g_n)_{n \geqslant 1}$ tend vers l'infini. S'il existe au moins un $r \geqslant 1$ tel que $\lambda_r(\mathcal{T}) > 0$, alors*

(i) soit les courbes C_n sont singulières pour n assez grand ;

(ii) soit $g_1 = g(X) \geqslant 2$ et les deux projections $\pi_i : \Gamma \to X$ pour $i = 1, 2$ sont étales sur X.

Mieux, dans la première alternative, on est en mesure d'estimer l'ordre de grandeur de la mesure de singularité des courbes C_n pour espérer obtenir une bonne tour.

6.3.2 Composante finie d-régulière et points totalement décomposés

Concentrons nous désormais sur la partie d-régulière du graphe. Un chemin de longueur $(n-1)$ de cette partie du graphe correspond à un point lisse de C_n donc à un point de $\widetilde{C}_n$. S'il existe un sous-graphe fini d-régulier d'ensemble de sommets Σ, alors cela révèle $\#\Sigma \times d^{n-1}$ points de $\widetilde{C}_n$, autant que de chemins de longueur $(n-1)$. Si de plus $\Sigma \subset X(\mathbb{F}_{q^r})$, on en déduit que :

$$N_{q^r}(\widetilde{C}_n) = \#\widetilde{C}_n(\mathbb{F}_{q^r}) \geqslant \#\Sigma \times d^{n-1}.$$

Autrement dit, on obtient une minoration non triviale du second invariant important. En général, une telle composante finie d-régulière saute au yeux sur le graphe.

Un sous graphe fini d-régulier est réunion de ses composantes connexes qui coïncident, régularité oblige, avec ses composantes fortement connexes. On s'est donc intéressé à ces composantes.

Théorème 6.2 (Perret & H. (2013)) *Soit (X, Γ) une correspondance vérifiant les hypothèses du §6.2. On suppose que les courbes $(C_n)_{n\geqslant 1}$ sont irréductibles. Alors le graphe $\mathcal{G}_\infty(X, \Gamma)$ contient au plus une composante finie, fortement connexe, d-régulière.*

La preuve de ce théorème se fait en deux temps. On commence par montrer qu'une telle composante est nécessairement *primitive* (en plus de savoir qu'entre deux quelconques sommets il y a un chemin orienté, on sait que l'on peut trouver une longueur commune à tous les chemins liant deux sommets quelconques), puis on établit le résultat.

L'idée est d'estimer le nombre *cycles de longueur n* dans la composante et dans le graphe tout entier de deux façons. Sur $C_{n+1} \subset X^{n+1}$ un cycle est un point ayant la première et dernière coordonnée égales. Sur le graphe $\mathcal{G}_\infty$, cela correspond à un chemin *fermé* ou *cycle* à n côtés. Cette double interprétation nous permet de mêler des données de nature assez différentes.

Comptage géométrique. — Tout d'abord combinant la formule de projection et des calculs d'intersection dans la surface $X \times X$, nous majorons géométriquement le nombre de cycles de longueur n *comptés avec multiplicité* dans C_{n+1}. Si $X = \mathbb{P}^1$, on montre facilement que le nombre de cycle global est inférieur ou égal à $2d^n$. Sinon, il y a un terme correctif qui, petit miracle, ne s'avère jamais essentiel.

Du point de vue du graphe $\mathcal{G}_\infty$, on en déduit donc la même majoration concernant son nombre de cycles de longueur n. Cela représente finalement assez peu de cycles et cela fait peser une forte contrainte sur le graphe.

Comptage à partir de la matrice d'adjacence. — Restreignons nous à une composante finie, fortement connexe d-régulière. Notons Σ l'ensemble de ses sommets, $\mathcal{G}_\Sigma$ la dite composante et $c_\Sigma(n)$ le nombre de cycles de longueur n à l'intérieur de $\mathcal{G}_\Sigma$. Soit A_Σ la matrice d'adjacence de cette composante. Tout d'abord, on vérifie facilement que $c_\Sigma(n) = \mathrm{tr}(A_\Sigma^n) = \sum_{\lambda\in \mathrm{Sp}(A_\Sigma)} \lambda^n$ (où $\mathrm{Sp}(A_\Sigma)$ désigne le spectre de A_Σ). Mais comme la composante est fortement connexe, la matrice d'adjacence A_Σ est irréductible et à coefficients positifs. Grâce au théorème de Perron-Frobenius, on connaît très bien le spectre d'une telle matrice. En particulier, on montre ici que le rayon spectral vaut d et que d est valeur propre simple de A_Σ.

En combinant ces deux comptages provenant d'horizons différents, toujours dans le cas $X = \mathbb{P}^1$, on en déduit que :

$$c_\Sigma(n) = \sum_{\lambda\in \mathrm{Sp}(A_\Sigma)} \lambda^n \leqslant 2d^n, \tag{6.3}$$

On commence par en déduire que A_Σ ne peux pas avoir d'autres valeurs propres de module d, ce qui caractérise le fait que la composante est primitive. Du coup, on peut affiner le décompte à la Perron-Frobenius et montrer que $c_\Sigma(n) = d^n + o(d^n)$ pour chaque composante finie fortement connexes d-régulière.

Si $\mathcal{G}_{\Sigma_1}, \ldots, \mathcal{G}_{\Sigma_k}$ désignent des composantes finies, fortement connexes d-régulières, on en déduit que $kd^n + o(d^n) \leqslant 2d^n$ si bien que $k \leqslant 2$. Autrement dit le nombre de composantes finies, fortement connexes d-régulières est forcément inférieur ou égal à 2. En fait, il ne peut pas dépasser 1, comme on s'en aperçoit en tenant compte du fait que le décompte à la Perron-Frobenius est un décompte sans multiplicité alors que le décompte géométrique est lui un décompte avec multiplicité. On utilise alors le fait que les cycles ont tous une puissance qui devient multiple.

6.3.3 Incidence du graphe sur l'asymptotique de la tour

On vient de voir que la géométrie de la tour fait peser de fortes contraintes sur le graphe de celle-ci. En retour, ces contraintes pesant sur le graphe ont des retombées sur la tour elle-même comme l'illustre résultat suivant.

Théorème 6.3 (Perret & H. (2013)) *Soit (X, Γ) une correspondance vérifiant les hypothèses du début de ce chapitre. Supposons que les courbes C_n de la tour associée sont toutes irréductibles et que la suite des genres géométriques $(g_n)_{n\geqslant 1}$ tende vers l'infini. Supposons de plus que :*

(i) le nombre de points géométriques de $\widetilde{C}_n$ provenant de la désingularisation des points singuliers de C_n est négligeable devant d^n pour n grand,

(ii) le graphe $\mathcal{G}_\infty$ contient au moins une (et donc exactement une) composante finie fortement connexe et d-régulière.

Alors, il existe au plus un entier $r \geqslant 1$ tel que $\beta_r(\mathcal{T}(X, \Gamma)) \neq 0$.

La preuve de ce résultat est assez similaire à celle du théorème 6.2 évoquée plus haut sauf que l'on ne compte plus simplement les cycles mais plutôt les chemins. Notons que les deux hypothèses techniques sont satisfaites par la quasi totalité des tours connues.

Le fait qu'un seul β_r puisse être non nul semble être une spécificité des tours récursives. On connaît des tours, fournies par la théorie du corps de classes, qui ont plusieurs β's non nuls.

6.4 Et après ?

C'est le sujet le plus frais et l'un de ceux qui occupe encore mes réflexions mathématiques du moment. Avec Marc Perret, nous travaillons actuellement à plusieurs prolongements.

Étude systématique d'une tour concrète. — Nous espérons pouvoir tirer des informations plus fines sur la tour par simple lecture du graphe quitte à enrichir encore ce dernier. La caractérisation des points singuliers de C_n que nous avons donné est un premier pas. Il nous a suffit pour établir des premiers résultats. Pour aller plus loin, il faudrait être en mesure d'estimer la multiplicité de ces points. Le salut est peut-être d'associer un poids à chaque arrête non étale, puis d'effectuer une intégration sur le graphe singulier. Dans le même genre d'idées, il nous semble plausible que le genre géométrique de la tour puisse, lui aussi, être obtenu par une intégration sur graphe singulier.

Si le graphe fait visuellement jaillir, en général, la partie totalement décomposée d'une bonne tour, ce qui donne la possibilité au moins empiriquement de décrire cette partie, il ne permet pas, pour l'instant, de prouver le fait que cette partie est bel et bien totalement décomposée. Nous sommes déjà en mesure de déduire du graphe une équation fonctionnelle du type de celle introduite par Lenstra [Len02]. C'est un premier pas. Il reste à calculer le plus petit corps contenant les corps de définition des points de la composante. C'est un renseignement purement arithmétique plus difficile à attraper.

Recherche de nouvelles tours. — En s'appuyant sur le graphe, nous avons développé de nouvelles stratégies permettant de découvrir de nouvelles tours. L'idée est de se fixer une base X et de chercher une correspondance susceptible de donner une bonne tour en visant soit un graphe singulier soit une partie finie fortement connexe d-régulière. Les premières expériences que nous avons pu mener dans ce sens sont assez encourageantes dans la mesure où elles nous ont permis de «retrouver» bien des tours déjà connues. Malheureusement, cette stratégie n'a pas encore débouché sur une nouvelle tour.

À l'inverse d'une recherche au cas par cas, on peut se fixer une courbe de base X et considérer l'ensemble des correspondances sur celle-ci. Peut-on munir cet ensemble d'une relation d'équivalence qui soit pertinente du point du vue des tours et dont l'ensemble des classes soit muni d'une structure algébrique ?

Une tour récursive est entièrement déterminée par une correspondance sur une courbe. Certes, la littérature sur les correspondances de courbes n'est pas très riche. Il n'en reste pas moins que certaines correspondances, notamment sur $\mathbb{C}$, font partie d'objets classiques étudiés par les géomètres. Un travail de «fouilles» dans ces correspondances s'impose pour voir dans quelle mesure certaines d'entre elles pourraient conduire à une bonne tour. Dans cette recherche, il conviendrait de se focaliser sur la recherche d'une correspondances laissant stable un ensemble fini de points. C'est assurément une contrainte forte.

Asymptotique encore et toujours. — Enfin, nous ne pensons pas avoir tiré tout le potentiel de la connexion entre la tour et son graphe. Pour aller plus loin, peut-être faudrait-il mieux comprendre la structure du graphe. Nous avons montré l'unicité d'une composante finie fortement connexe d-régulière. Mais qu'en est-il des composantes infinies ? Pour l'instant, les composantes infinies demeurent très mystérieuses. Si par exemple, il y avait deux composantes fortement connexes infinies distinctes, le système dynamique sous-jacent ne serait pas mélangeant. Cela aurait tendance à nous surprendre. Nous ne voyons pas encore de retombées possible sur la tour de telles propriétés.

Bibliographie

[BB05] Peter Beelen and Irene I. Bouw. Asymptotically good towers and differential equations. *Compos. Math.*, 141(6) :1405–1424, 2005.

[Bee04] Peter Beelen. Graphs and recursively defined towers of function fields. *J. Number Theory*, 108(2) :217–240, 2004.

[BGS05a] Juscelino Bezerra, Arnaldo Garcia, and Henning Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink's lower bound. *J. Reine Angew. Math.*, 589 :159–199, 2005.

[BGS05b] Juscelino Bezerra, Arnaldo Garcia, and Henning Stichtenoth. An explicit tower of function fields over cubic finite fields and Zink's lower bound. *J. Reine Angew. Math.*, 589 :159–199, 2005.

[BGS08] Alp Bassa, Arnaldo Garcia, and Henning Stichtenoth. A new tower over cubic finite fields. *Mosc. Math. J.*, 8(3) :401–418, 615, 2008.

[Brz83] J. Brzeziński. On orders in quaternion algebras. *Comm. Algebra*, 11(5) :501–522, 1983.

[BS07] Alp Bassa and Henning Stichtenoth. A simplified proof for the limit of a tower over a cubic finite field. *J. Number Theory*, 123(1) :154–169, 2007.

[CG94] Jean-Marc Couveignes and Louis Granboulan. Dessins from a geometric point of view. In *The Grothendieck theory of dessins d'enfants (Luminy, 1993)*, volume 200 of *London Math. Soc. Lecture Note Ser.*, pages 79–113. Cambridge Univ. Press, Cambridge, 1994.

[CH85] Kevin Coombes and David Harbater. Hurwitz families and arithmetic Galois groups. *Duke Math. J.*, 52(4) :821–839, 1985.

[CH11] Jean-Marc Couveignes and Emmanuel Hallouin. Global descent obstructions for varieties. *Algebra Number Theory*, 5(4) :431–463, 2011.

[Cou94] Jean-Marc Couveignes. Calcul et rationalité de fonctions de Belyĭ en genre 0. *Ann. Inst. Fourier (Grenoble)*, 44(1) :1–38, 1994.

[Cou97] Jean-Marc Couveignes. Quelques revêtements définis sur $\mathbf{Q}$. *Manuscripta Math.*, 92(4) :409–445, 1997.

[Cou99] Jean-Marc Couveignes. Tools for the computation of families of coverings. In *Aspects of Galois theory (Gainesville, FL, 1996)*, volume 256 of *London Math. Soc. Lecture Note Ser.*, pages 38–65. Cambridge Univ. Press, Cambridge, 1999. The following pages of this book were inadvertently numbered incorrectly : p. 21 should be p. 22, p. 22 should be p. 23 and p. 23 should be p. 21.

[Cou00] Jean-Marc Couveignes. Boundary of Hurwitz spaces and explicit patching. *J. Symbolic Comput.*, 30(6) :739–759, 2000. Algorithmic methods in Galois theory.

[CR04] J.-M. Couveignes and Nicolas Ros. Des obstructions globales à la descente des revêtements. *Acta Arith.*, 114(4) :331–348, 2004.

[DD97] Pierre Dèbes and Jean-Claude Douai. Algebraic covers : field of moduli versus field of definition. *Ann. Sci. École Norm. Sup. (4)*, 30(3) :303–338, 1997.

[DD99] Pierre Dèbes and Jean-Claude Douai. Gerbes and covers. *Comm. Algebra*, 27(2) :577–594, 1999.

[DE99] Pierre Dèbes and Michel Emsalem. On fields of moduli of curves. *J. Algebra*, 211(1) :42–56, 1999.

[Dèb01a] Pierre Dèbes. Méthodes topologiques et analytiques en théorie inverse de Galois : théorème d'existence de Riemann. In *Arithmétique de revêtements algébriques (Saint-Étienne, 2000)*, volume 5 of *Sémin. Congr.*, pages 27–41. Soc. Math. France, Paris, 2001.

[Dèb01b] Pierre Dèbes. Revêtements topologiques. In *Arithmétique de revêtements algébriques (Saint-Étienne, 2000)*, volume 5 of *Sémin. Congr.*, pages 163–214. Soc. Math. France, Paris, 2001.

[Dèb01c] Pierre Dèbes. Théorie de Galois et géométrie : une introduction. In *Arithmétique de revêtements algébriques (Saint-Étienne, 2000)*, volume 5 of *Sémin. Congr.*, pages 1–26. Soc. Math. France, Paris, 2001.

[Det04] Michael Dettweiler. Plane curve complements and curves on Hurwitz spaces. *J. Reine Angew. Math.*, 573 :19–43, 2004.

[DF90] Pierre Dèbes and Mike Fried. Arithmetic variation of fibers in families of curves. I. Hurwitz monodromy criteria for rational points on all members of the family. *J. Reine Angew. Math.*, 409 :106–137, 1990.

[DF94] Pierre Dèbes and Michael D. Fried. Nonrigid constructions in Galois theory. *Pacific J. Math.*, 163(1) :81–122, 1994.

[Elk98] Noam D. Elkies. Shimura curve computations. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 1–47. Springer, Berlin, 1998.

[Elk01] Noam D. Elkies. Explicit towers of Drinfeld modular curves. In *European Congress of Mathematics, Vol. II (Barcelona, 2000)*, volume 202 of *Progr. Math.*, pages 189–198. Birkhäuser, Basel, 2001.

[Elk06] Noam D. Elkies. Shimura curves for level-3 subgroups of the $(2, 3, 7)$ triangle group, and some other examples. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 302–316. Springer, Berlin, 2006.

[Fri77] M. Fried. Fields of definition of function fields and Hurwitz families—groups as Galois groups. *Comm. Algebra*, 5(1) :17–82, 1977.

[Ful69] William Fulton. Hurwitz schemes and irreducibility of moduli of algebraic curves. *Ann. of Math. (2)*, 90 :542–575, 1969.

[FV91] Michael D. Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.*, 290(4) :771–800, 1991.

[GS95] Arnaldo Garcia and Henning Stichtenoth. A tower of artin-schreier extensions of function fields attaining the drinfeld-vladut bound. *Invent. Math.*, 121 :211–222, 1995.

[GSR03] Arnaldo Garcia, Henning Stichtenoth, and Hans-Georg Rück. On tame towers over finite fields. *J. Reine Angew. Math.*, 557 :53–80, 2003.

[Hal01] Emmanuel Hallouin. Computing local integral closures. *J. Symbolic Comput.*, 32(3) :211–230, 2001.

[Hal05] Emmanuel Hallouin. Study and computation of a Hurwitz space and totally real $\mathrm{PSL}_2(\mathbb{F}_8)$-extensions of $\mathbb{Q}$. *J. Algebra*, 292(1) :259–281, 2005.

[Hal09] Emmanuel Hallouin. Computation of a cover of Shimura curves using a Hurwitz space. *J. Algebra*, 321(2) :558–566, 2009.

[HM06] Emmanuel Hallouin and Christian Maire. Cancellation in totally definite quaternion algebras. *J. Reine Angew. Math.*, 595 :189–213, 2006.

[HP08] Emmanuel Hallouin and Marc Perret. On generators of the group $\widehat{H}^{-1}(\mathrm{Gal}(L/K), E_L)$ in some abelian p-extension L/K. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 273–283. World Sci. Publ., Hackensack, NJ, 2008.

[HP13] Emmanuel Hallouin and Marc Perret. Recursive towers of curves over finite fields using graph theory. soumis, 2013.

[HRD03] Emmanuel Hallouin and Emmanuel Riboulet-Deyris. Computation of some moduli spaces of covers and explicit S_n and A_n regular $\mathbb{Q}(T)$-extensions with totally real fibers. *Pacific J. Math.*, 211(1) :81–99, 2003.

[Jac68] H. Jacobinski. Genera and decompositions of lattices over orders. *Acta Math.*, 121 :1–29, 1968.

[Kap69] Irving Kaplansky. Submodules of quaternion algebras. *Proc. London Math. Soc. (3)*, 19 :219–232, 1969.

[Len02] H. W. Jr. Lenstra. On a problem of garcia, stichtenoth, and thomas. *Finite Fields App.*, 8 :166–170, 2002.

[LR12] Reynald Lercier and Christophe Ritzenthaler. Hyperelliptic curves and their invariants : Geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372 :595–636, 2012.

[Mes91] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991.

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer, 1999.

[Odl76] Andrew Odlyzko. Tables for discriminant bounds. `http://www.dtc.umn.edu/~odlyzko/unpublished/index.html`, 1976.

[Shi71] Goro Shimura. On the field of rationality for an abelian variety. *Nagoya Math. J.*, 45 :167–178, 1971.

[Sme13] Daniel Smertnig. A note on cancellation in totally definite quaternion algebras. soumis, 2013.

[Swa70] Richard G. Swan. *K-theory of finite groups and orders*. Lecture Notes in Mathematics, Vol. 149. Springer-Verlag, Berlin, 1970.

[TVZ82] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109 :21–28, 1982.

[VD83] S. G. Vlèduts and V. G. Drinfel′d. The number of points of an algebraic curve. *Funktsional. Anal. i Prilozhen.*, 17(1) :68–69, 1983.

[Vig76] Marie-France Vignéras. Simplification pour les ordres des corps de quaternions totalement définis. *J. Reine Angew. Math.*, 286/287 :257–277, 1976.

[Voi05] John Michael Voight. *Quadratic forms and quaternion algebras : Algorithms and arithmetic*. ProQuest LLC, Ann Arbor, MI, 2005. Thesis (Ph.D.)–University of California, Berkeley.

[Voi06] John Voight. Computing CM points on Shimura curves arising from cocompact arithmetic triangle groups. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 406–420. Springer, Berlin, 2006.

[Voi09a] John Voight. Computing fundamental domains for Fuchsian groups. *J. Théor. Nombres Bordeaux*, 21(2) :469–491, 2009.

[Voi09b] John Voight. Shimura curve computations. In *Arithmetic geometry*, volume 8 of *Clay Math. Proc.*, pages 103–113. Amer. Math. Soc., Providence, RI, 2009.

[Völ96] Helmut Völklein. *Groups as Galois Groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge, 1996.

[Wei56] André Weil. The field of definition of a variety. *Amer. J. Math.*, 78 :509–524, 1956.

[Wew98] Stefan Wewers. *Construction of Hurwitz spaces.* PhD thesis, Universität-Gesamthochschule, Essen, 1998.