THÈSE DE DOCTORAT D'AIX MARSEILLE UNIVERSITÉ

UFR Sciences
Spécialité
Mathématiques

École doctorale Mathématiques et Informatique d'Aix-Marseille (ED184).

Présentée et soutenue publiquement par
Florent ULPAT ROVETTA
le Vendredi 4 Décembre 2015

Sujet :

Étude arithmétique et algorithmique de courbes de petit genre

Directeur de thèse : Christophe RITZENTHALER

Rapporteurs :

M.René SCHOOF	Professeur à l'Université de Rome II "Tor Vergata"
M.Jordi GUÀRDIA I RÚBIES	Professeur à l'Université Polytechnique de Catalogne

Composition du jury :

M. Christophe RITZENTHALER	Prof Université Rennes 1	Directeur de thèse
M. David KOHEL	Prof Univ AMU	Co-directeur
M. René SCHOOF	Prof Univ de Rome II "Tor Vergata"	Rapporteur
M. Jordi GUÀRDIA I RÚBIES	Prof Univ Polytechnique de Catalogne	Rapporteur
M. Renald LERCIER	Chercheur HDR, DGA Rennes 1	Examinateur
M. Pierrick GAUDRY	Prof Univ de Loraine	Examinateur

Remerciements

Table des matières

Introduction

L'essentiel de la thèse concerne l'algorithmique des courbes hyperelliptiques en caractéristique différente de 2, en particulier, la description des classes d'isomorphismes de ces courbes. Disposer de ces classes est très utile pour de nombreuses applications. Par exemple, cela sert à construire des courbes avec beaucoup de points en utilisant la théorie du corps de classes [Rök12] ou à élargir l'ensemble des courbes utiles pour des couplages basés sur la cryptographie. Cela est illustré en genre 2 par [FS11], [GV12] et [Sat09]. On aimerait aussi réaliser cela pour les courbes non hyperelliptiques (en genre supérieur à 3 donc). Cela est utilisé par exemple dans [Ber08] pour calculer la cohomologie de l'espace de modules et comme on le verra ici dans [LRRS14] pour l'étude de l'obstruction de Serre pour les quartiques planes lisses.

La stratégie est bien connue : un point de l'espace de modules sur un corps k correspond par définition à une classe d'isomorphismes sur $\overline{k}$ d'une courbe et on a des "coordonnées" naturelles pour ce point en termes d'invariants des formes binaires. Une fois un représentant sur k obtenu à partir des invariants (on parlera de reconstruction de la courbe), il suffit alors de parcourir l'ensemble des classes d'isomorphismes à l'intérieur de la classes d'isomorphismes sur $\overline{k}$. Des représentants de ces classes sont appelés des tordues de la courbe. En pratique, la mise en œuvre de cette méthode est loin d'être évidente et nous proposons divers algorithmes pour attaquer ces problèmes sur les courbes hyperelliptiques. La question des tordues sera abordée dans la partie I et la question des invariants dans la partie III.

La partie II quant à elle, concerne le premier exemple de courbes non hyperelliptiques : les quartiques planes lisses. L'absence d'une bonne théorie des invariants dans ce cas amène à une stratégie toute différente pour appréhender les classes d'isomorphismes. On donne ainsi de nouvelles familles "en bijection" avec les points rationnels de la plupart des strates de l'espace de modules sous l'action des groupes d'automorphismes (cf [LRRS14], Annexe C ou la section 3.3). Ces résultats étaient motivés par leur application à l'étude statistique de l'obstruction de Serre pour laquelle un modèle heuristique accompagne les résultats expérimentaux obtenus (cf Annexe D).

À présent, on présente les différentes parties.

Première partie

Ces travaux concernent l'étude des tordues. Ces objets sont étudiés théoriquement au moins depuis Weil ([Wei56]) et nous souhaitons les développer de manière algorithmique sur les corps finis. Nous rappelons dans un premier temps comment on peut expliciter la correspondance entre les tordues et un certain groupe de cohomologie galoisienne en se ramenant à l'étude des classes d'équivalence du groupe des automorphismes sous une conjugaison tordue par l'action du Frobenius [MT10]. Lorsque le groupe des automorphismes est de plus linéaire (c.-à-d. un sous groupe de PGL) et connu explicitement, nous développons alors un programme pour automatiser le calcul (cf. section 1.3.2 et annexe B.1.1). Nous étudions la complexité de notre algorithme (cf. paragraphe 1.3.3) et montrons que les bornes sont atteintes dans certains cas extrêmes. Dans un second temps, nous regardons deux exemples particuliers de courbes.

Pour les courbes hyperelliptiques, de nombreux cas particuliers ont été explicités, notam-

ment dans [CN07], [CNP05] et [CQ07]. Cependant, aucun algorithme systématique n'était, à notre connaissance, disponible et implémenté pour le cas des courbes hyperelliptiques en genre quelconque. En utilisant les programmes de [LRS12] que l'on améliore ici légèrement dans certains cas (cf. paragraphe 2.1.5), nous pouvons alors donner le premier algorithme complet en `Magma` qui calcule pour une courbe hyperelliptique sur un corps fini l'ensemble de ses tordues (cf. annexe B.1.2). Les courbes hyperelliptiques ne rentrent pas directement dans l'ensemble des variétés pour lesquelles la stratégie initiale a été expliquée. Néanmoins une opération de dévissage permet de se ramener au groupe des automorphismes réduits qui est lui linéaire (cf paragraphe 2.1.2). Il reste alors à prendre en compte un phénomène dit d'auto-dualité qui peut conduire une courbe et sa tordue quadratique à être isomorphes ([CN07]).

Le second exemple est celui des courbes de genre 3 non hyperelliptiques qui a servi dans les calculs de l'article donné dans l'annexe C. Nous ne détaillons pas l'ensemble des cas[1] mais présentons des cas typiques selon l'ordre du groupe des automorphismes de la courbe.

Deuxième partie

Cette partie reprend essentiellement les résultats de [LRRS14] (cf. annexe C). Une des notions centrales en géométrie arithmétique est la notion d'espace de modules de courbes d'un genre donné $\mathtt{g}$. Ce sont des variétés algébriques telles que les points géométriques classifient les courbes à isomorphisme géométrique près (cf paragraphe 3.1.2). La difficulté principale du traitement des espaces de modules (sans structure additionnelle) est l'absence de familles universelles qui permettrait de représenter naturellement les éléments de ces espaces. Sur les corps finis, l'existence d'une famille universelle optimiserait des algorithmes permettant d'écrire les classes d'isomorphismes de courbes. Dans l'article [LRRS14], on considère le cas des courbes de genre 3 non hyperelliptiques. L'énumération de leur classe sur les corps finis permet en effet de visualiser un phénomène arithmétique qui n'apparaît pas en genre inférieur, appelé obstruction de Serre, et de l'étudier statistiquement. On se réfèrera à l'introduction des articles en annexes C et D pour des références et les conclusions à ce propos et nous focaliserons ici sur les aspects constructifs de l'énumération de ces courbes. En l'absence de méthode de reconstruction de la courbe à partir de ses invariants, on introduit trois substituts à la notion de familles universelles, le meilleur candidat pour pallier à la notion de familles universelles étant celui de famille représentative, introduit en section 3.2. Il s'agit d'une famille de courbes telles que leurs classes soient en bijection naturelle avec les points d'une sous-variété S donnée de l'espace de modules. Ces familles présentent l'intérêt de pouvoir être construites explicitement dans beaucoup de cas lorsque S est une strate de courbes avec un groupe d'automorphismes donné (cf paragraphe 3.1.3). Dans les cas des quartiques planes lisses, ces familles peuvent être construites pour quasiment tous les groupes d'automorphismes (cf paragraphe 3.3.2). En effet, seuls le groupe trivial et le groupe à deux éléments dérogent à cette règle. Un des points importants de cette partie est le détail de la preuve de la construction des familles représentatives de [LRRS14] qui n'est donnée qu'en partie dans l'article pour des raisons de place. On en profite pour corriger quelques typos de l'article au passage.

Notons qu'un travail similaire pourrait être intéressant à entreprendre dans le cas des courbes hyperelliptiques, où on peut espérer un résultat en tout genre.

Troisième partie

Cette partie se décompose en deux temps.

1. qu'on peut trouver dans les programmes disponibles sur https://perso.univ-rennes1.fr/christophe.ritzenthaler/programme/qdbstats-v3_0.tgz

On s'intéresse tout d'abord dans le chapitre 5 au calcul des covariants de formes binaires en petite caractéristique dans une optique similaire à [Bas15] et en liaison avec l'espace de modules des courbes hyperelliptiques. Si, en caractéristique 0 ou en grande caractéristique, il s'agit d'un problème classique (mais encore redoutable en pratique dès que le degré de la forme est supérieur à 10), en petite caractéristique, les approches classiques basées sur les transvections (qui sont des opérateurs différentiels) s'effondrent. Dans cette optique, on a voulu tester l'efficacité d'une méthode alternative en s'inspirant de [Gey74] et [Stu08]. L'idée est de considérer l'algèbre des covariants de n-points de $\mathbb{P}^1$ sur l'action de $\mathrm{GL}_2(k)$ (cf. définition 25 (p. 59)). Le principal avantage de cette algèbre est qu'elle admet un système de générateurs de covariants explicite et *indépendant* de la caractéristique. Les covariants pour les formes binaires sont alors obtenus comme la sous-algèbre symétrisée par $\mathcal{S}_n$. Bien que séduisante en théorie, notre implémentation actuelle est extrêmement limitée car l'action du groupe $\mathcal{S}_n$ dans le cas modulaire (c.à-d. lorsque la caractéristique divise l'ordre du groupe) sur les covariants de n points n'aboutit pas avec les algorithmes génériques de `Magma` dès que $n = 6$ (cf. section 5.2.6). Toutefois, cette méthode a permis de déterminer un ensemble séparant (une condition un peu plus faible qu'être un système générateur, voir la définition 27 (p. 61)) dans le cas des quartiques binaires en caractéristique 3. Chemin faisant, on s'est rendu compte que certains des invariants/covariants apparaissant en petite caractéristique pouvaient être dérivés de covariants classiques par une nouvelle opération différentielle simple (cf. paragraphe 5.3.2.1) sous certaines conditions que nous explicitons. Pour les octiques, on obtient ainsi le nouvel invariant de degré 1 trouvé par [Bas15] ainsi que des nouveaux covariants en degré 4 et 6 (cf. paragraphe 5.2.3). Cette opération, bien qu'elle enrichit l'algèbre des covariants obtenus par réduction de ceux en caractérisque nulle, n'est cependant pas suffisante pour obtenir tous les covariants comme en le montrera sur un exemple en degré 4. La question de la génération en pratique en petite caractéristique reste donc grande ouverte.

Dans un second temps, en liaison avec l'énumération des courbes à isomorphisme près, on s'intéresse au problème de la reconstruction d'une courbe d'invariants donnés. En caractéristique 0, la méthode de Mestre [Mes91] permet d'effectuer ce calcul dans le cas générique. En genre 2, [CQ05] a montré comment réaliser ce calcul dans de nombreux autres cas, à l'exception notable de la caractéristique 3 et 5. Reprenant les résultats précédents, Lercier et Ritzenthaler ont alors réalisé une implémentation [2] en complétant de manière *ad hoc* les cas résiduels. Cependant, le détail des calculs n'a jamais été publié. On présente ici la première démonstration complète de la validité des algorithmes et nous effectuons notre propre implémentation en `Sage` (cf. annexe A.3). Cela nous a permis au passage d'améliorer certaines procédures.

Notations

Soit p un nombre premier ou $p = 0$. On désigne par k un corps commutatif de caractéristique p et $\overline{k}$ sa clôture algébrique. Lorsque k est un corps fini de cardinal q on le note $\mathbb{F}_q$ Lorsque l'on parle d'une courbe, on suppose toujours qu'elle est algébrique, projective, absolument irréductible et lisse. Pour un entier $\mathtt{g}$, on désigne par $\mathcal{C}$ une courbe de genre $\mathtt{g}$. Le cardinal d'un ensemble X sera noté $|X|$. On donne quelques groupes qui apparaissent tout au long du manuscrit :

— $\mathbf{C}_n$, le groupe cyclique d'ordre n,
— $\mathbf{D}_{2n}$, le groupe diédral d'ordre $2n$,
— $\mathcal{A}_n$, le groupe alterné d'ordre $n!/2$,
— $\mathcal{S}_n$, le groupe symétrique d'ordre $n!$.

Pour d'autres symboles, propres à ce document, on pourra se reporter à la liste des notation, qui se trouve à la page 190. Enfin, au sein de chaque section d'un chapitre, les définitions, théorèmes, propositions, etc... adoptent une numérotation linéaire, par exemple, le nombre pour la définition X indique qu'il s'agit de la X ième définition du manuscrit. Pour les lecteurs

2. disponible dans `Magma` depuis la version 2.13 et aussi sur https://perso.univ-rennes1.fr/christophe.ritzenthaler/programme/g2twists-v1.tgz

qui accèdent à ce document sous forme électronique, les références croisées (de cette couleur) et les références bibliographiques (de cette couleur) sont des liens hypertextes.

Première partie

Des Algorithmes sur les tordues

Chapitre 1

Tordues des Variétés quasi-projectives

Dans ce chapitre, V désigne une variété algébrique lisse quasi-projective absolument irréductible définie sur le corps k que l'on suppose parfait. Pour simplifier, on utilisera juste l'expression variété algébrique, ou encore variété, définie sur le corps k. On notera $\mathrm{Aut}(V)$ le groupe des $\overline{k}$-automorphismes de V dans lui-même et $\mathrm{Aut}_k(V)$ le sous-groupe de $\mathrm{Aut}(V)$ des automorphismes définis sur k. Comme k est parfait, on pourra utiliser son groupe de Galois absolu que l'on notera $\mathrm{Gal}_{\overline{k}/k}$.

1.1 Le cas général

Cette section présente les notions et principaux résultats concernant les tordues de variété algébrique sur le corps k. Les démonstrations des résultats cités sans preuve se trouvent dans [Sil09] ,[Ser94] et [MT10]. On va d'abord rappeler la définition d'une tordue de V et expliquer comment ramener l'étude des tordues de V, à isomorphisme sur k près, à l'étude d'un ensemble de cohomologie. On illustrera notre propos à travers l'exemple de la quartique de Dyck-Fermat.

1.1.1 Définition des objets

Définition 1. *Une tordue de V est une variété algébrique V' définie sur k qui est isomorphe à V sur $\overline{k}$. Lorsqu'un isomorphisme V sur V' est défini sur k, on dit que V' est une tordue triviale de V. On identifie généralement deux tordues si elles sont isomorphes sur k. L'ensemble des tordues de V, à k-isomorphismes près est noté* $\mathrm{Twist}(V)$.

On illustre cette première définition par l'exemple suivant. Il va nous servir de fil rouge tout au long de ce paragraphe.

Exemple 1. *On considère la quartique D de Dyck-Fermat donnée par l'équation*

$$X^4 + Y^4 + Z^4 = 0.$$

Sur $k = \mathbb{F}_{13}$, cette courbe possède 32 points rationnels. La quartique plane D' d'équation

$$X^4 + 4Y^4 - X^2Y^2 + 7Z^4 = 0$$

a 8 points rationnels ; ces deux courbes ne sont donc pas isomorphes sur $\mathbb{F}_{13}$. Cependant, sur le corps $\mathbb{F}_{13}(\sqrt{2})$, l'application

$$\varphi : (X : Y : Z) \to (X + \sqrt{2}Y : X - \sqrt{2}Y : Z)$$

définit un isomorphisme de D sur D'. Ainsi, D' est une tordue non triviale de D.

Définition 2. *Soient $\sigma \in \mathrm{Gal}_{\overline{k}/k}$ et $\varphi \in \mathrm{Aut}(V)$, on définit φ^σ comme un élément de* $\mathrm{Aut}(V)$ *obtenu en remplaçant les coefficients c de φ par $\sigma(c)$. On nomme cet automorphisme l'élévation de φ à la puissance σ.*

Si V' est une tordue de V alors il existe un isomorphisme $\varphi : V \to V'$ définie sur $\overline{k}$. Pour mesurer l'écart de φ à être définie sur k, on peut considérer l'application

$$\begin{aligned} \zeta : \mathrm{Gal}_{\overline{k}/k} &\to \mathrm{Aut}(V) \\ \sigma &\to \zeta_\sigma \end{aligned} \tag{1.1.1}$$

où pour tout $\sigma \in \mathrm{Gal}_{\overline{k}/k}$, $\zeta_\sigma = (\varphi^\sigma)^{-1}\varphi$.
On se rend alors compte que φ est définie sur k si et seulement si ζ_σ est égal à l'identité pour tout σ. De plus, pour tout σ, τ dans $\mathrm{Gal}_{\overline{k}/k}$,

$$\zeta_{\sigma\tau} = (\varphi^{\sigma\tau})^{-1}\varphi = (\varphi^{\sigma\tau})^{-1}\varphi^\tau(\varphi^\tau)^{-1}\varphi = \Big((\varphi^\sigma)^{-1}\varphi\Big)^\tau\Big((\varphi^\tau)^{-1}\varphi\Big).$$

On a donc la propriété suivante :

$$\forall \sigma, \tau \in \mathrm{Gal}_{\overline{k}/k} \qquad \zeta_{\sigma\tau} = (\zeta_\sigma)^\tau \zeta_\tau. \tag{1.1.2}$$

Ceci nous amène à la définition :

Définition 3. *Un cocycle de* $\mathrm{Gal}_{\overline{k}/k}$ *à valeur dans* $\mathrm{Aut}(V)$ *est une application*

$$\zeta : \mathrm{Gal}_{\overline{k}/k} \to \mathrm{Aut}(V)$$

qui vérifie la relation (1.1.2). Le cocycle trivial est l'application $\zeta^0 : \mathrm{Gal}_{\overline{k}/k} \to \mathrm{Aut}(V)$ *telle que* $\forall \sigma \in \mathrm{Gal}_{\overline{k}/k}\ \zeta^0_\sigma = Id_{\mathrm{Aut}(V)}$.

Exemple 2. On reprend notre exemple fil rouge de la quartique de Dyck-Fermat.

On considère un autre isomorphisme de D sur D' donné par $\xi = \varphi \circ P$ où P est la permutation des deux dernières variables. On note ζ (respectivement δ) le cocycle associé à φ (respectivement ξ). Soit ς, le morphisme de Frobenius sur $\mathbb{F}_{13}$, $\varsigma \in \mathrm{Gal}_{\overline{\mathbb{F}}_{13}/\mathbb{F}_{13}}$. On a :

$$\zeta_\varsigma(X : Y : Z) = (X : -Y : Z) \text{ et}$$

$$\delta_\varsigma(X : Y : Z) = (X : Y : -Z).$$

Grâce à ces deux égalités, il apparaît que ζ et δ sont deux cocycles différents pour une même tordue.

L'exemple précédent illustre le fait que prendre seulement des cocycles ne permet pas de classer les tordues de V. Il y a plus de cocycles que de tordues. On introduit une relation d'équivalence sur les cocycles. Celle-ci permet de regrouper les cocycles correspondant à une même tordue. La relation est la suivante :

Définition 4. *Deux cocycles* ζ *et* δ *sont dits* cohomologues *(ou* équivalents*) s'il existe un élément* $\alpha \in \mathrm{Aut}(V)$ *tel que pour tout* $\sigma \in \mathrm{Gal}_{\overline{k}/k}$

$$\alpha^\sigma \zeta_\sigma = \delta_\sigma \alpha.$$

Exemple 3. *On reprend les notations de l'exemple précédent. Puisqu'on a*

$$\alpha^\varsigma \zeta_\varsigma(X : Y : Z) = (X : \sqrt{2}Y : -\sqrt{2}Z) = \delta_\varsigma \alpha(X : Y : Z),$$

un α *qui conviendrait est*

$$\alpha : (X : Y : Z) \to (X : \sqrt{2}Y : \sqrt{2}Z).$$

Grâce à la proposition 1 (p. 10), on expliquera pourquoi l'élévation à la puissance ς est suffisante dans ce cas là pour conclure que ζ et δ sont cohomologues.

Définition 5. *L'ensemble des classes d'équivalence de cocycles par cette relation est appelé l'ensemble des* classes de cohomologie de $\mathrm{Aut}(V)$. *On le note* $H^1(\mathrm{Gal}_{\overline{k}/k}, \mathrm{Aut}(V))$.

1.1.2 Lien entre classes de cohomologie et tordues

Le théorème suivant ([Sil09, p. 285] et [Ser94, Chap III par 1.3 prop 5]) va permettre de ramener le calcul des tordues de V définies sur k à un calcul de classes de cohomologie.

Théorème 1. *Pour chaque tordue V' de V, on choisit un isomorphisme $\varphi : V \to V'$ et on définit une application ζ comme dans (1.1.1).*

1. *ζ est un cocycle.*
2. *La classe de cohomologie $\{\zeta\}$ est déterminée par la classe de k-isomorphismes de V' indépendamment du choix de φ. Ainsi, on obtient une application naturelle*

$$\mathrm{Twist}(V) \to H^1(\mathrm{Gal}_{\overline{k}/k}, \mathrm{Aut}(V)).$$

3. *L'application définie en 2. est une bijection d'ensembles. En d'autres termes, les tordues de V (à k-isomorphismes près) correspondent aux éléments de l'ensemble cohomologique $H^1(\mathrm{Gal}_{\overline{k}/k}, \mathrm{Aut}(V))$.*

Exemple 4. *Dans le cas de la quartique de Dick-Fermat D définie sur $\mathbb{F}_{13}$, il y a 10 classes de cohomologie associées à 10 tordues. L'élément ζ (ou δ) est bien sûr un représentant de la classe de cohomologie associée à la tordue D'. On a aussi la classe de cohomologie de ζ_1 définie par*

$$\forall\, \sigma \in \mathrm{Gal}_{\overline{\mathbb{F}}_q/\,\mathbb{F}_q} \qquad \zeta_{1\sigma} = (\varphi_1^{\sigma})^{-1}\varphi_1,$$

où $\varphi_1 : (X : Y : Z) \longrightarrow (\sqrt{2}X, \sqrt[4]{7}Y, \sqrt[4]{7}Z)$.

Le théorème 1 (p. 9) établit une correspondance entre les tordues de la variété V et les classes de cohomologie de $\mathrm{Aut}(V)$. À présent, on va s'intéresser au cas particulier des corps finis et montrer que l'on peut encore réduire l'étude des tordues à un ensemble plus simple.

1.2 Sur les corps finis

À partir de maintenant, et jusqu'à la fin de cette partie, on considère que $k = \mathbb{F}_q$. Dans ce cas, $\mathrm{Gal}_{\overline{\mathbb{F}}_q/\,\mathbb{F}_q}$ est un groupe pro-cyclique topologiquement engendré par le morphisme de Frobenius $\varsigma : x \to x^q$.

1.2.1 Réduction de $H^1(\mathrm{Gal}_{\overline{k}/k}, \mathrm{Aut}(V))$ lorsque k est fini

On va montrer que lorsque tous les éléments de $\mathrm{Aut}(V)$ ont un ordre fini, $H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_q/\,\mathbb{F}_q}, \mathrm{Aut}(V))$ est isomorphe à l'ensemble des classes de conjugaison par Frobenius de $\mathrm{Aut}(V)$. On va donc pouvoir exprimer les tordues de la variété V en terme de classes de conjugaison par Frobenius. On commence par rappeler une définition.

Définition 6. *On dit que deux éléments g et h de $\mathrm{Aut}(V)$ sont conjugués par Frobenius s'il existe $\alpha \in \mathrm{Aut}(V)$ tel que $g = \alpha^{\varsigma} h \alpha^{-1}$.*

Exemple 5. En reprenant les notations de l'exemple 3 (p. 8), on voit que $g = \zeta_{\varsigma}$ et $h = \delta_{\varsigma}$ sont deux automorphismes de D conjugués par Frobenius.

La conjugaison par Frobenius définit une relation d'équivalence. On appelle classe de conjugaison par Frobenius les classes d'équivalence de cette relation. On note cet ensemble $\mathrm{Fr}(\mathrm{Aut}(V))$. Si $g \in \mathrm{Aut}(V)$, on note $\{g\}_{\mathrm{Fr}}$ la classe de conjugaison par Frobenius de g.
Le résultat suivant ([MT10, p. 352], [vdGvdV92, p. 80]) nous sera très utile dans le calcul des tordues de V sur $\mathbb{F}_q$. En effet, au lieu de considérer l'action de tout le groupe de Galois, on prendra uniquement en compte l'action du morphisme de Frobenius.

Proposition 1. *Lorsque tous les éléments de* $\mathrm{Aut}(V)$ *ont un ordre fini, l'application*

$$H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_q/\,\mathbb{F}_q}, \mathrm{Aut}(V)) \to \mathrm{Fr}(\mathrm{Aut}(V))$$

donnée par

$$f : \{\zeta\} \to \{\zeta_\varsigma\}_{\mathrm{Fr}}$$

est une bijection d'ensemble. Ainsi,

$$\mathrm{Twist}(V) \cong \mathrm{Fr}(\mathrm{Aut}(V)).$$

Corollaire 1. *Pour tout* $\alpha \in \mathrm{Aut}(V)$*, il existe une tordue* V_α *(triviale ou non) et un isomorphisme de* φ_α *de* V *sur* V_α *qui vérifie*

$$\alpha = (\varphi_\alpha^\varsigma)^{-1}\,\varphi_\alpha\,.$$

Démonstration. Soit $\alpha \in \mathrm{Aut}(V)$. D'après la proposition 1 (p. 10), il existe un cocycle $\zeta \in H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_q/\,\mathbb{F}_q}, \mathrm{Aut}(V))$ tel que

$$\zeta_\varsigma = \alpha.$$

De plus, d'après le théorème 1 (p. 9), il existe une tordue V' de V et un isomorphisme φ telle que

$$(\varphi^\varsigma)^{-1}\,\varphi = \zeta_\varsigma = \alpha.$$

□

Ce résultat motive la définition suivante.

Définition 7. *Soit* $\alpha \in \mathrm{Aut}(V)$*, on appelle* V_α *la tordue de* V *associée à l'automorphisme* α*. On note aussi* φ_α *l'isomorphismes de* V *sur* V_α*.*

Démonstration de la proposition 1. Nous décomposons la preuve en deux temps.

Injectivité. Soient ζ et δ deux cocycles tels que $f(\{\zeta\}) = f(\{\delta\})$ c'est à dire il existe $\alpha \in \mathrm{Aut}(V)$ satisfaisant $\delta_\varsigma\alpha = \alpha^\varsigma\zeta_\varsigma$. Il s'agit de montrer que ζ et δ sont dans la même classe de cohomologie. Soit $\eta \in \mathrm{Gal}_{\overline{\mathbb{F}}_q/\,\mathbb{F}_q}$. Puisque $\mathrm{Gal}_{\overline{\mathbb{F}}_q/\,\mathbb{F}_q}$ est pro-cyclique, $\exists\, m \in \mathbb{Z}$ tel que $\eta = \varsigma^m$. On a donc

$$\alpha^\eta\zeta_\eta = \alpha^{\varsigma^m}\zeta_{\varsigma^m}.$$

Comme ζ_{ς^m} est un cocycle, on a

$$\alpha^\eta\zeta_\eta = \alpha^{\varsigma^m}(\zeta_\varsigma)^{\varsigma^{m-1}}\zeta_{\varsigma^{m-1}} = (\alpha^\varsigma\zeta_\varsigma)^{\varsigma^{m-1}}\zeta_{\varsigma^{m-1}}.$$

Puisque par hypothèse $\alpha^\varsigma\zeta_\varsigma = \delta_\varsigma\alpha$, on obtient

$$\alpha^\eta\zeta_\eta = (\delta_\varsigma)^{\varsigma^{m-1}}\alpha^{\varsigma^{m-1}}\zeta_{\varsigma^{m-1}}.$$

Ainsi, par récurrence immédiate, on en déduit

$$\alpha^\eta\zeta_\eta = (\delta_\varsigma)^{\varsigma^{m-1}}(\delta_\varsigma)^{\varsigma^{m-2}}\cdots\delta_\varsigma\alpha.$$

Puisque δ_{ς^m} est un cocycle, il vérifie l'égalité suivante

$$\delta_{\varsigma^m} = (\delta_\varsigma)^{\varsigma^{m-1}}\delta_{\varsigma^{m-1}} = (\delta_\varsigma)^{\varsigma^{m-1}}(\delta_\varsigma)^{\varsigma^{m-2}}\cdots\delta_\varsigma.$$

D'où

$$\alpha^\eta\zeta_\eta = \delta_{\varsigma^m}\alpha = \delta_\eta\alpha.$$

Les deux cocycles ζ et δ sont donc dans la même classe de cohomologie. L'injectivité de f est ainsi démontrée.

Surjectivité. Soit $\alpha \in \mathrm{Aut}(V)$, on cherche à montrer qu'il existe un cocycle ζ tel que $f(\{\zeta\}) = \{\alpha\}_{\mathrm{Fr}}$. L'automorphisme α étant défini sur $\overline{k}$, $\exists\, m \in \mathbb{Z}$ tel que $\alpha^{\varsigma^m} = \alpha$. On pose $\beta = \alpha\alpha^{\varsigma}\alpha^{\varsigma^2}\dots\alpha^{\varsigma^{m-1}}$. Puisque $\beta \in \mathrm{Aut}(V)$, il a un ordre fini. Soit n l'ordre de β et $\eta = \varsigma^m$, alors $\beta^\eta = \beta$ et

$$\alpha\alpha^{\varsigma}\alpha^{\varsigma^2}\dots\alpha^{\varsigma^{nm-1}} = \beta\beta^{\eta}\dots\beta^{\eta^{n-1}} = \beta^n = id.$$

Ainsi, l'application qui à ς associe α et ς^{mn} associe id se prolonge de manière unique en un cocycle continu $\zeta : \mathrm{Gal}_{\overline{k}/k} \to \mathrm{Aut}(V)$ qui vérifie $\zeta_\varsigma = \alpha$. Ceci montre la surjectivité de f. □

Remarque 1. *L'argument de la surjectivité repose sur le fait que tous les éléments de* $\mathrm{Aut}(V)$ *ont un ordre fini. Par contre, supposer que* $\mathrm{Aut}(V)$ *est fini est plus restrictif. Par exemple si* $V = \mathbb{P}^g$ *sur* $\mathbb{F}_q$ *alors* $\mathrm{Aut}(V)$ *est un groupe infini mais chaque élément est bien sûr d'ordre fini (puisque défini sur un corps fini).*

1.2.2 Quelques résultats sur le nombre de tordues

1.2.2.1 Un borne supérieure sur le nombre de tordues

Grâce à la proposition 1 (p. 10), il apparaît que le nombre de tordues est majoré par le nombre d'automorphismes de la variété. L'article [MT10, p. 352] donne le résultat suivant.

Proposition 2. *Supposons* $\mathrm{Aut}(V)$ *fini. Le nombre de tordue est plus petit que le nombre de classe de conjugaison de* $\mathrm{Aut}(V)$.

Démonstration. Dans l'article de [MT10], la preuve est faite pour des courbes. Cependant, l'argument se sert uniquement de la finitude du groupe des automorphismes. On peut donc le généraliser au cas des variétés algébriques qui ont un groupe d'automorphisme fini. □

Cette borne est même optimale. En effet, si $\mathrm{Aut}(V)$ est défini sur $\mathbb{F}_q$, les classes de conjugaison sont les classes de Frobenius.

1.2.2.2 Conditions pour qu'il n'y ait pas de tordue

Les résultats suivants se trouvent dans [vdGvdV92, p. 81]. On note toujours V' une tordue de V et φ l'isomorphisme qui envoie V sur V'. On note ϑ l'application qui à un élément $\alpha \in \mathrm{Aut}(V)$ associe $\vartheta(\alpha)$ défini par

$$\begin{aligned}\vartheta(\alpha) : \mathrm{Aut}(V) &\longrightarrow \mathrm{Aut}(V)\\ \epsilon &\longrightarrow \epsilon^{-1}\alpha\epsilon^{\varsigma}.\end{aligned}$$

D'après la proposition 1 (p. 10), le nombre d'orbite de ϑ est égal au nombre de tordue. De plus, l'ensemble des éléments ϵ tels que $\vartheta((\varphi^{\varsigma})^{-1}\varphi)(\epsilon) = (\varphi^{\varsigma})^{-1}\varphi$ est en bijection avec $\mathrm{Aut}_{\mathbb{F}_q}(V')$. Ainsi, en comptant le nombre d'élément par orbite de ϑ, on obtient :

$$|\mathrm{Aut}(V)| = \sum_{Tordues\ V'} \frac{|\mathrm{Aut}(V)|}{|\mathrm{Aut}_{\mathbb{F}_q}(V')|}.$$

Soit encore :

$$1 = \sum_{Tordues\ V'} \frac{1}{|\mathrm{Aut}_{\mathbb{F}_q}(V')|}.$$

Ceci nous amène au résultat suivant :

Proposition 3. *Si* $\mathrm{Aut}_{\mathbb{F}_q}(V)$ *est trivial, il n'y a pas de tordue non triviale.*

Après avoir étudié quelques résultats généraux sur le nombre de tordues, on s'intéresse au calcul de ces dernières lorsque $\mathrm{Aut}(V)$ est particulier. Puisqu'on sait qu'à chaque classe de conjugaison par Frobenius correspond une tordue, on regarde comment retrouver effectivement les tordues de la variété V à partir de $\mathrm{Fr}(\mathrm{Aut}(V))$. On sait qu'une tordue V' de V est entièrement déterminée par l'isomorphisme $\varphi : V \to V'$. Le problème est de retrouver φ à partir de sa classe de conjugaison par Frobenius. Dans la partie suivante, on détaillera comment faire si le groupe d'automorphisme de la variété V est linéaire, c'est à dire s'il est isomorphe à un sous-groupe de $\mathrm{PGL}_g(\overline{\mathbb{F}}_q)$ pour un certain entier naturel g.

1.3 Méthode de calcul des tordues quand $\mathrm{Aut}(V)$ est linéaire

Dans certain cas, le groupe d'automorphismes de V est linéaire. Puisque la variété V est définie sur un corps fini $\mathbb{F}_q$, tous les éléments de $\mathrm{Aut}(V)$ sont d'ordre fini. En effet, un élément de $\mathrm{Aut}(V)$ est défini sur une extension finie $\mathbb{F}_{q^n}$. On peut le considérer comme un élément de $\mathrm{PGL}_g(\mathbb{F}_{q^n})$ pour un certain entier g. Par suite, cet élément est d'ordre fini et ceci nous permet d'utiliser les résultats de la proposition 1 (p. 10). Pour le plongement canonique des courbes lisses projectives non hyperelliptiques, le groupe d'automorphismes est linéaire et si le genre est supérieur à 2, c'est un groupe fini. C'est également le cas pour la plupart des hypersurfaces lisses projectives. Plus précisément si V est une hypersurface de $\mathbb{P}^g$ de degré d alors si $g \geq 2$, $d \geq 3$ et (g, d) est différent de $(2, 3)$ et $(3, 4)$ alors le groupe des automorphismes est fini et linéaire. On se réfèrera à [Cha78] pour $g = 2$ (voir aussi [HKT08, th. 11.29 p. 469]) et à [MM64, Th.2] pour $g \geq 3$.
Dans cette partie, on détaillera une méthode pour calculer les tordues dans le cas où le groupe d'automorphismes de la variété est linéaire et fini. Soit g un entier naturel non nul, on suppose que $\mathrm{Aut}(V)$ est isomorphe à un sous-groupe de $\mathrm{PGL}_g(\overline{\mathbb{F}}_q)$.

1.3.1 Calcul des tordues de V

Dans cette partie, on utilise le théorème de Hilbert 90 pour trouver les tordues de V. Soit $\{\alpha\}_{\mathrm{Fr}} \in \mathrm{Fr}(\mathrm{Aut}(V))$. On note encore α un élément de $\{\alpha\}_{\mathrm{Fr}}$. Soit M la matrice $g \times g$ avec au moins un coefficient égal à 1 qui représente α dans une certaine base. On note $\mathbb{F}_{q^n}$ le corps *minimal* de définition de M. On cherche une matrice $A \in \mathrm{PGL}_g(\overline{\mathbb{F}}_q)$ représentant l'isomorphisme φ_α de V sur V_α. D'après le corollaire 1 (p. 10), A doit vérifier $A^{\varsigma}M = A$. Pour cela, on prend $m \in \mathbb{Z}$ et $\lambda \in \mathbb{F}_q$ tels que :

$$M^{\varsigma^{m-1}} \dots M^{\varsigma}M = \lambda id.$$

De tels éléments existent grâce à la proposition suivante :

Proposition 4. *Il existe un couple $(m, \lambda) \in \mathbb{N} \times \mathbb{F}_q$ tel que :*

$$M^{\varsigma^{m-1}} \dots M^{\varsigma}M = \lambda id, \text{ et } n \mid m. \tag{1.3.1}$$

De plus :
- *si e est l'exposant de $\mathrm{Aut}(V)$ alors $m \mid n \cdot e$;*
- *si m est minimal pour la propriété (1.3.1) alors on a encore $\lambda \in \mathbb{F}_q$ et $n \mid m$.*

Démonstration. On pose $B = M^{\varsigma^{n-1}} \dots M^{\varsigma}M$. Comme $B \in \mathrm{PGL}_g(\overline{\mathbb{F}}_q)$, il existe un entier N tel que $B^N = id$ dans $\mathrm{PGL}_g(\overline{\mathbb{F}}_q)$. Ainsi, il existe $\lambda_1 \in \overline{\mathbb{F}}_q$ tel que :

$$B^N = \lambda_1 id.$$

De plus, les matrices M et donc B sont définies sur $\mathbb{F}_{q^n}$; d'où $B^{\varsigma^n} = B$. Par suite, on peut réécrire B^N de la façon suivante :

$$B^N = B^{\varsigma^{(N-1)n}} \dots B^{\varsigma^n}B = M^{\varsigma^{Nn-1}} \dots M^{\varsigma^{(N-1)n+1}}M^{\varsigma^{(N-1)n}} \dots M^{\varsigma^{2n-1}} \dots M^{\varsigma^{n+1}}M^{\varsigma^n}.M^{\varsigma^{n-1}} \dots M^{\varsigma}M.$$

On pose $m_1 = N \cdot n$. On montre que $\lambda_1 \in \mathbb{F}_q$. En effet, on élève à la puissance Frobenius et on multiplie à droite par M, l'égalité :

$$M^{\varsigma^{m_1-1}} \dots M^{\varsigma} M = \lambda_1 id.$$

On obtient alors :

$$M^{\varsigma^m} \lambda_1 = \lambda_1^{\varsigma} M.$$

Puisque $n \mid m_1$, on a $M^{\varsigma^m} = M$; d'où $\lambda_1^{\varsigma} = \lambda_1$.
Ainsi, m_1 et λ_1 conviennent.

1. Si Aut(V) est d'exposant fini, on remplace N par e dans le raisonnement précédent et on en déduit le résultat.
2. On prend un couple $(m, \lambda) \in \mathbb{N} \times \overline{\mathbb{F}}_q$, vérifiant 1.3.1, tel que m soit minimal. On reprend les notations du début de la preuve. On a par division euclidiène de Nn par m :

   $$Nn = km + r \ \textit{ avec } r < m.$$

   Ainsi,

   $$\lambda_1 id = M^{\varsigma^{Nn-1}} \dots M^{\varsigma^{km-1}} \dots M = \lambda^{\varsigma^{k-1}} \dots \lambda^{\varsigma} \lambda M^{\varsigma^{Nn-1}} \dots M^{\varsigma^{km}} = \lambda^{\varsigma^{k-1}} \dots \lambda^{\varsigma} \lambda M^{\varsigma^{r-1}} \dots M^{\varsigma} M.$$

   C'est à dire :

   $$M^{\varsigma^{r-1}} \dots \ M^{\varsigma} M. = \frac{\lambda_1}{\lambda^{\varsigma^{k-1}} \dots \ \lambda^{\varsigma} \lambda} id.$$

   Ceci contredit la minimalité de m. On doit avoir $r = 0$. Ainsi, $m \mid Nn$.
   De même que précédemment, on a :

   $$M^{\varsigma^m} \lambda = \lambda^{\varsigma} M.$$

   Comme M contient un coefficient égal à 1, on a $\lambda = \lambda^{\varsigma}$. Ainsi, $M^{\varsigma^m} = M$ et par suite, $n \mid m$.

□

Remarque 2. *On verra dans le paragraphe 2.2.1 qu'on peut prendre $\lambda = 1$ dans certains cas.*

On choisit $x \in \mathbb{F}_{q^m}$ de norme λ sur $\mathbb{F}_q$. Un tel x est donné par une racine d'un polynôme irréductible unitaire de degré m sur $\mathbb{F}_q$ de coefficient constant $(-1)^m \lambda$. On remplace M par $\frac{1}{x} M$. À priori, ce nouveau M est défini sur $\mathbb{F}_{q^{\mathrm{ppcm}(n,m)}}$. Mais d'après la proposition 4 (p. 12), $n | m$ ainsi, M est défini sur $\mathbb{F}_{q^m}$. On pose :

$$A = P + \sum_{i=1}^{m-1} P^{\varsigma^i} M^{\varsigma^{i-1}} \dots M^{\varsigma} M,$$

où P est une matrice aléatoire de $\mathrm{GL}_g(\mathbb{F}_{q^m})$ telle que A est inversible. Le résultat suivant est une version effective de Hilbert 90 dans le cas de $\mathrm{PGL}_n(\overline{\mathbb{F}}_q)$

Proposition 5. *$A^{\varsigma} M = A$. C'est à dire, A est un cobord pour M.*

Démonstration. On a :

$$A^{\varsigma} M = P^{\varsigma} M + \sum_{i=1}^{m-1} P^{\varsigma^{i+1}} M^{\varsigma^i} \dots M^{\varsigma^2} M^{\varsigma} M.$$

En réorganisant les termes, on obtient :

$$A^{\varsigma} M = P^{\varsigma^m} M^{\varsigma^{m-1}} \dots M^{\varsigma} M + \sum_{i=1}^{m-1} P^{\varsigma^i} M^{\varsigma^{i-1}} \dots M^{\varsigma} M.$$

D'une part, P est un élément de $\mathrm{GL}_g(\mathbb{F}_{q^m})$, ainsi $P^{\varsigma^m} = P$. D'autre part, $M^{\varsigma^{m-1}} \dots M^{\varsigma} M = id$, d'où le résultat. □

Remarque 3. *On note que la probabilité que A soit inversible est plus grande que $1/4$ (voir [GH97] proposition 1.3).*

1.3.2 L'algorithme

Calcul des tordues

Entrée :

C : la courbe définie sur le corps $\mathbb{F}_q$;

G : le groupe d'automorphismes de la courbe C ;

Sortie : la liste T des tordues de C sur $\mathbb{F}_q$.

Description :

1: T = la future liste des tordues de C ;
2: Coh = les classes de cohomologie de G ;
3: **pour** M dans Coh **faire**
4: A = le cobord correspondant à M ;
5: f = le polynôme de la todue associée à A ;
6: ajouter à la liste T la courbe d'équation f ;
7: **fin pour**.

Calcul des classes de cohomologie

Entrée :

$\mathbb{F}_q$: le corps de base de la courbe C ;

G : le groupe d'automorphismes de la courbe C ;

Sortie : la liste Coh des classes de cohomologie de G sur $\mathbb{F}_q$.

Description :

1: Coh = la future liste des classes de cohomologie ;
2: L = une copie de G ;
3: **tant que** L n'est pas vide **faire**
4: ajoute à Coh le premier élément de L ;
5: n = la taille de Coh ;
6: supprime le premier élément de L ;
7: **pour** M dans G **faire**
8: supprime de L l'élément $M^{\varsigma}Coh[n]M^{-1}$; ($Coh[n]$ est le dernier élément de la liste Coh)
9: **fin pour** ;
10: **fin tant que**.

calcul du cobord avec la méthode de Hilbert 90

Entrée :

M : une matrice définie sur $\mathrm{GL}_g(\mathbb{F}_{q^n})$;

$\mathbb{F}_q$: un corps fini ;

Sortie : la matrice A du cobord.

Description :

1: $m =$ le plus petit entier tel que $M^{\varsigma^{m-1}} \cdots M^{\varsigma} M$ soit scalaire ;
2: **répète**
3: $P =$ une matrice aléatoire de $\mathrm{GL}_g(\mathbb{F}_{q^m})$;
4: $A = P$;
5: **pour** i dans $\{1, \cdots m-1\}$ **faire**
6: $P = P^{\varsigma} M$;
7: $A = A + P$;
8: **fin pour** ;
9: **jusqu'à ce que** A soit inversible.

1.3.3 Estimations de complexité de l'algorithme lorsque Aut(V) est fini

Soit V plongée dans $\mathbb{P}^{g-1}(\mathbb{F}_q)$ avec un groupe d'automorphisme linéaire d'ordre fini N. On va estimer la complexité de notre algorithme en fonction des variables suivantes

$M_g(\mathbb{F}_{q^a})$: la complexité bilinéaire de la multiplication de deux matrices de taille g dans le corps $\mathbb{F}_{q^a}$ sur le corps $\mathbb{F}_q$

$Inv_g(\mathbb{F}_{q^a})$: la complexité bilinéaire d'une inversion de matrice de taille g dans le corps $\mathbb{F}_{q^a}$ sur le corps $\mathbb{F}_q$

$Fr_g(\mathbb{F}_{q^a})$: la complexité bilinéaire de l'élévation à la puissance Frobenius d'une matrice de taille g dans le corps $\mathbb{F}_{q^a}$ sur le corps $\mathbb{F}_q$.

Soit $\alpha_i \in \mathrm{Aut}(V)$, on note n_i le degré minimal de l'extension sur laquelle α_i est définie et n est le ppcm des n_i. On a :

$$N = |\mathrm{Aut}(V)| = \sum |\{\alpha_i\}_{Fr}|,$$

où la somme est sur l'ensemble des classes de conjugaison par Frobenius. Comme l'ensemble des classes de conjugaison par Frobenius est isomorphe à l'ensemble des tordues, on peut considérer que cette somme s'effectue sur l'ensemble des tordues de V.
Puisque l'automorphisme α_i est défini sur $\mathbb{F}_{q^{n_i}}$, les n_i éléments $\alpha_i, \alpha_i^{\varsigma}, \ldots, \alpha_i^{\varsigma^{n_i-1}}$ de $\{\alpha_i\}_{Fr}$ sont distincts (dans la définition 6 (p. 9), il suffit de prendre $g = \alpha_i^{\varsigma^i}$, $h = \alpha_i^{\varsigma^{i-1}}$ et $\alpha = \alpha_i^{\varsigma^{i-1}}$ pour $i \in \mathbb{N}$). Ainsi, $|\{\alpha_i\}_{Fr}| \geq n_i$. On a donc :

$$\sum_{tordues} n_i \leq N.$$

Lemme 1. *Si m_i est le plus petit entier tel que $\alpha_i^{\varsigma^{m_i-1}} \ldots \alpha_i^{\varsigma} \alpha_i = id_{\mathrm{Aut}(V)}$ alors $m_i \leq N$.*

Démonstration. Soit $j \in \mathbb{N}$, on considère $\alpha_i^{\varsigma^j} \ldots \alpha_i^{\varsigma} \alpha_i \in \mathrm{Aut}(V)$. Puisque $\mathrm{Aut}(V)$ est un groupe fini de cardinal N, il existe $l \in \mathbb{N}$ tel que $l \leq N$ et

$$\alpha_i^{\varsigma^N} \cdots \alpha_i^{\varsigma} \alpha_i = \alpha_i^{\varsigma^l} \cdots \alpha_i^{\varsigma} \alpha_i.$$

Ainsi,

$$\alpha_i^{\varsigma^N} \cdots \alpha_i^{\varsigma^{l+1}} = 1.$$

On applique ς^{-l-1} à cette égalité et on obtient :

$$\alpha_i^{\varsigma^{N-l-1}} \cdots \alpha_i^{\varsigma} \alpha_i = 1.$$

Puisque m_i est minimal pour cette propriété, on obtient le résultat voulu. □

1.3.3.1 Complexité du calcul des classes de cohomologie

Pour chaque classe de cohomologie de $\mathrm{Aut}(V)$ calculée, on parcourt $\mathrm{Aut}(V)$. Dans ce parcours, on calcule l'inverse d'une matrice de taille g, on élève à la puissance Frobenius une matrice de taille g définie sur $\mathbb{F}_{q^n}$ et on fait le produit de trois matrices de taille g définie sur $\mathbb{F}_{q^n}$ (on rappelle que n est le ppcm des n_i). On a donc la complexité suivante :

$$C_{Coh} = \mathrm{O}\Big(\sum_{Tordues} N\{2M_g(\mathbb{F}_{q^n}) + Fr_g(\mathbb{F}_{q^n}) + Inv_g(\mathbb{F}_{q^n})\}\Big).$$

1.3.3.2 Complexité de l'implémentation de Hilbert 90

Soit $\alpha_i \in \{\alpha_i\}_{\mathrm{Fr}}$, on calcule m_i fois dans $\mathbb{F}_{q^{m_i}}$ le produit de deux matrices de taille g définies sur $\mathbb{F}_{q^{m_i}}$ et on élève m_i fois dans $\mathbb{F}_{q^{m_i}}$ à la puissance Frobenius une matrice de taille g définie sur $\mathbb{F}_{q^{m_i}}$. On a donc une complexité de

$$C_{H90} = \mathrm{O}\left(m_i\Big\{Fr_g(\mathbb{F}_{q^{m_i}}) + M_g(\mathbb{F}_{q^{m_i}})\Big\}\right).$$

1.3.3.3 Complexité de l'algorithme dans le cas général

On calcule les classes de cohomologie, puis pour chaque classe on fait un Hilbert 90. La complexité est donc :

$$C_{Tordues} = \mathrm{O}(C_{Coh} + \sum_{Tordues} C_{H90}).$$

1.3.3.4 Complexité de l'algorithme dans certains cas extrêmes

1. Cas où $\mathrm{Aut}(V) = \mathrm{Aut}_{\mathbb{F}_q}(V)$ est cyclique avec N un nombre premier.

Puisque tous les éléments de $\mathrm{Aut}(V)$ sont définis sur $\mathbb{F}_q$, les classes de conjugaison par Frobenius sont les classes de conjugaison classiques (car $\varsigma_{|\mathbb{F}_q} = id$). De plus, $\mathrm{Aut}(V)$ est cyclique. Il y a donc exactement N classes de conjugaison et, par suite, N tordues. La complexité du calcul des classes de cohomologie peut donc se reécrire :

$$C_{Coh} = \mathrm{O}\left(N^2\{2M_g(\mathbb{F}_q) + Fr_g(\mathbb{F}_q) + Inv_g(\mathbb{F}_q)\}\right).$$

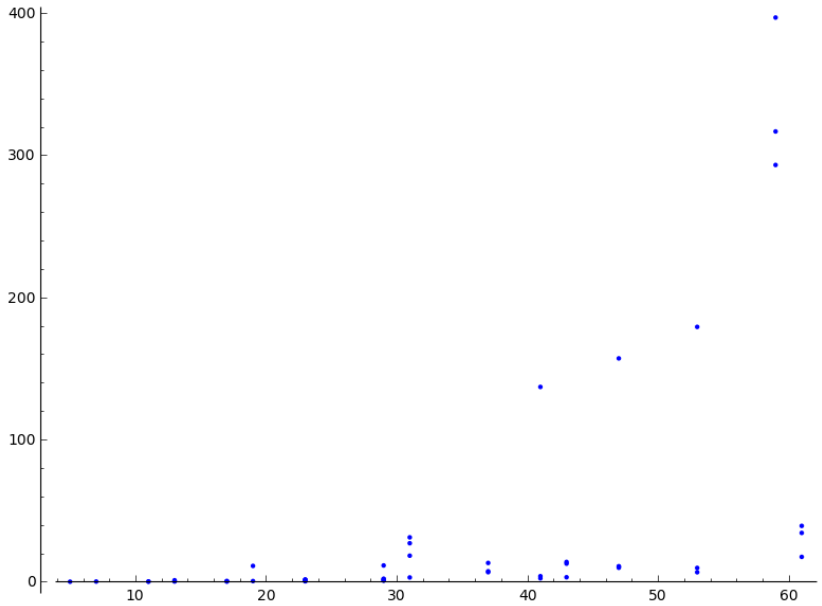
De plus, comme N est premier, tous les éléments non triviaux de $\mathrm{Aut}(V)$ sont d'ordre N. Par suite, le plus petit entier m_i tel que $\alpha_i^{\varsigma^{m_i-1}} \ldots \alpha_i^{\varsigma}\alpha_i = id_{\mathrm{Aut}(V)}$ est l'ordre de $\alpha_i \in \mathrm{Aut}(V)\backslash\{id\}$, à savoir N. L'isomorphisme est donc défini sur $\mathbb{F}_{q^N}$. Ainsi, la complexité dans ce cas est :

$$C_{Tordues} = \mathrm{O}\left(N^2\{2M_g(\mathbb{F}_q) + Fr_g(\mathbb{F}_q) + Inv_g(\mathbb{F}_q)\} + \sum_{Tordues} N\{Fr_g(\mathbb{F}_{q^N}) + M_g(\mathbb{F}_{q^N})\}\right)$$

$$= \mathrm{O}\left(N^2\{2M_g(\mathbb{F}_q) + Fr_g(\mathbb{F}_q) + Inv_g(\mathbb{F}_q) + Fr_g(\mathbb{F}_{q^N}) + M_g(\mathbb{F}_{q^N})\}\right).$$

Sachant que $Fr_g(\mathbb{F}_{q^N})$ et $M_g(\mathbb{F}_{q^N})$ assymptotiquement linéaires en N (conséquence de [BCP13, th.1]), la complexité de l'algorithme en N peut être effectuée en temps quasi linéaire. La figure 1.1 représente les temps de calculs des tordues en fonction de N. Ce temps est exprimé en secondes. Les courbes considérés sont de la forme $y^2 = x^N - 1$ et ont pour groupe d'automorphismes réduit isomorphe à $\mathbf{C}_N$ (voir la définition 10 (p. 20)).

FIGURE 1.1 – Temps de calcul de l'algorithme tordue en fonction de N lorsque le groupe d'automorphisme de la courbe G est isomorphe à $\mathbf{C}_N$. Le groupe G est défini sur $\mathbb{F}_p$ avec p un nombre premier que l'on fait varier entre 5 et 1201. L'entier N est représenté en abscisse. Le temps est exprimé en secondes et représenté en ordonnée



2. Cas où $m_i = n_i$ pour tout $\alpha_i \in \mathrm{Aut}(V)$.

La complexité de l'algorithme est alors :

$$C_{Tordues} = \mathrm{O}\Big(\sum_{tordues} \Big\{ N\{2M_g(\mathbb{F}_{q^n}) + Fr_g(\mathbb{F}_{q^n}) + Inv_g(\mathbb{F}_{q^n})\} + n_i\{Fr_g(\mathbb{F}_{q^{n_i}}) + M_g(\mathbb{F}_{q^{n_i}})\} \Big\} \Big).$$

On exprime cette complexité en N, n et n_i. Puisque $Fr_g(\mathbb{F}_{q^a})$, $Inv_g(\mathbb{F}_{q^a})$ et $M_g(\mathbb{F}_{q^a})$ sont linéaires en a, la complexité de l'algorithme en N, n et n_i peut se réécrire :

$$C_{Tordues} = \mathrm{O}\Big(\sum_{tordues} \Big\{ Nn + n_i^2 \Big\} \Big).$$

Puisque $\sum n_i^2 \leq (\sum n_i)^2$ et $\sum_{tordues} n_i \leq N$, on a :

$$C_{Tordues} = \mathrm{O}(N \sum_{tordues} n) + \mathrm{O}(N^2).$$

Bien que très particulier, un tel cas peut se produire. Par exemple, on prend la quartique plane lisse $\mathcal{C}$ qui a un groupe d'automorphismes de cardinal 6 et qui est définie sur $\mathbb{F}_{11}$ par l'équation suivante :

$$Z^3Y + X^4 + X^2Y^2 + Y^4 = 0.$$

Les classes de cohomologie sont :

$$\Big\{\{I_d\}, \{M\}\Big\} = \Big\{ \{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \}, \{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \zeta_6 \end{pmatrix} \} \Big\},$$

où ζ_6 est une racine primitive sixième de l'unité. Puisque $\mathcal{C}$ est définie sur $\mathbb{F}_{11}$, $\zeta_6 \in \mathbb{F}_{11^2}$. De plus,

$$M^{\varsigma}M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \overline{\zeta_6} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & \zeta_6 \end{pmatrix} = I_d.$$

Ainsi, on obtient $m_1 = n_1 = 1$ et $m_2 = n_2 = 2$.

Chapitre 2

Exemples sur les courbes

On va s'intéresser aux tordues de deux types de courbes (algébriques projectives absolument irréductibles et lisses) sur les corps finis : le cas des courbes hyperelliptiques puis celui des quartiques planes lisses. Dans le cas des courbes hyperelliptiques, nous obtenons le premier algorithme en genre quelconque pour calculer automatiquement les équations des tordues en fonction de l'équation de la courbe. Le cas des quartiques (courbe de genre 3 non hyperelliptiques) est un cas que nous avons développé spécifiquement pour être utilisé dans l'article dans l'appendice C.

2.1 Le cas des courbes hyperelliptiques

Dans cette partie $\mathcal{C}$ désigne une courbe de genre $\mathtt{g} > 1$ définie sur le corps k et $\mathbb{P}^1$ la droite projective définie sur $\overline{k}$. On se place dans le cas où la caractéristique de k est nulle ou impaire.

Le but de cette partie est de calculer les tordues de $\mathcal{C}$ à partir de la connaissance de son groupe d'automorphismes réduits. Dans ce but, on va montrer comment dévisser le groupe des automorphismes de $\mathcal{C}$ afin de se ramener à des automorphismes de $\mathbb{P}^1$ puis, on calculera les classes de cohomologie dans $\mathbb{P}^1$. Pour chaque classes d'automorphismes de $\mathbb{P}^1$, on a déjà étudié comment calculer le cobord. Il reste donc à chercher comment relever dans le groupe d'automorphismes. Ceci a été étudié dans [CN07, Partie II] dont nous reprenons les principaux résultats ici. Afin d'obtenir un algorithme complet, nous y ajoutons un raffinement du travail [LRS12] afin de calculer le groupe d'automorphismes réduits en fonction de l'équation de la courbe. Ce raffinement n'est valable que lorsque p ne divise pas le degré de la forme. L'algorithme complet ainsi obtenu a été implémenté en `Magma` (cf Annexe B.1.2) et nous donnons quelques tests réalisés pour diverses tailles de corps, genres et groupe d'automorphismes.

2.1.1 Définitions

Définition 8. *La courbe $\mathcal{C}$ est dite hyperelliptique s'il existe une courbe $\mathcal{C}_0$ définie sur k de genre 0 et un revêtement $\Phi : \mathcal{C} \to \mathcal{C}_0$ de degré 2.*

Une courbe de genre 0 est toujours isomorphe à une conique plane. Lorsque la conique admet un point rationnel (par exemple si k est algébriquement clos ou fini) alors elle est isomorphe à $\mathbb{P}^1$. Comme $[\overline{k}(\mathcal{C}) : \overline{k}(\mathcal{C}_0)] = 2$, en posant $\overline{k}(\mathcal{C}_0) = \overline{k}(X)$, on a

$$\overline{k}(\mathcal{C}) \cong \overline{k}(X)[Y]/(Y^2 - f(X)) \text{ avec } f(X) \in \overline{k}[X].$$

La courbe $\mathcal{C}$ a donc une équation de la forme $y^2 = f(x)$. Le théorème de Riemann-Hurwitz permet alors de montrer qu'on peut prendre f unitaire et $\deg(f) = 2\,\mathtt{g}+2$ ou $2\,\mathtt{g}+1$. On dit que $y^2 = f(x)$ est un *modèle hyperelliptique* (ou une équation hyperelliptique) de $\mathcal{C}$. Peut-on toujours trouver un modèle hyperelliptique de $\mathcal{C}$ défini sur k ? Cette interrogation motive la définition suivante.

Définition 9. *Une courbe hyperelliptique $\mathcal{C}$ définie sur k est* hyperelliptiquement définie sur k *s'il existe un modèle hyperelliptique de $\mathcal{C}$ sur k.*

Mestre ([Mes91] a montré que lorsque g est pair, une courbe hyperelliptique peut toujours être hyperelliptiquement définie sur k. En genre impair (voir par exemple [LR12]), il existe cependant des contre-exemples. Dans la suite nous ne considérons que des courbes sur les corps finis et nous pourrons donc toujours supposer que notre courbe a un modèle hyperelliptique.

On note ι l'automorphisme de $\mathcal{C}$ défini par $\iota(x, y) = (x, -y)$. L'automorphisme ι est appelé *involution hyperelliptique* de $\mathcal{C}$. Afin de traiter de manière analogue les cas de degré $2g + 1$ et $2g+2$, on considère une écriture projective de f comme polynôme homogène de degré $2g+2$ et on notera $f(x, z) = z^{2g+2} f(x/z)$. On appellera alors racines de $f(x, z)$ les points $(x_i : z_i) = (x_i : 1)$ avec $x_1, ..., x_{\deg(f)}$ les racines de f dans $\overline{k}$ lorsque $\deg f = 2g + 2$ auxquelles on ajoutera le point $(x_{2g+2}, z_{2g+2} = (1 : 0)$ lorsque $\deg f = 2g + 1$. On notera cet ensemble W. Ce sont les abscisses des points de Weierstrass de la courbe $\mathcal{C}$.

Définition 10. *Le groupe*

$$\mathrm{Aut}'(\mathcal{C}) := \{\alpha' \in \mathrm{Aut}(\mathbb{P}^1) | \alpha'(W) = W\}$$

est appelé le groupe d'automorphismes réduits de $\mathcal{C}$.

Plus généralement, entre deux courbes hyperelliptiques, on parlera de *d'isomorphisme réduit* pour désigner l'automorphisme de $\mathbb{P}^1$ qui envoie les racines projectives de la première sur celles de la seconde. Il apparaît facilement que les racines projectives de f détermine ce polynôme à une constante multiplicative près.

Proposition 6. $\mathrm{Aut}'(\mathcal{C})$ *est le sous-groupe de* $\mathrm{Aut}(\mathbb{P}^1)$ *qui préserve f à une constante près.*

Soit α un isomorphisme entre deux courbes hyperelliptiques $\mathcal{C}$ et $\mathcal{C}'$. D'après [Hug05, prop.3.1.1], l'élément α peut être considéré comme un couple (M, e) avec M un isomorphisme réduit de $\mathcal{C}$ et $e \in \overline{\mathbb{F}}_q$. Plus précisément, $\alpha \in \mathrm{Aut}(\mathcal{C})$ est donné par

$$\alpha : (x, y) \longrightarrow \Big(\frac{ax + b}{cx + d}, \frac{ey}{(cx + d)^{g+1}}\Big).$$

Ainsi, le couple (M, e) est unique modulo l'équivalence $(M, e) \sim (\lambda M, \lambda^{g+1} e)$.
Étant donné M et des modèles hyperelliptiques $\mathcal{C} : y^2 = f(x)$ et $\mathcal{C}' : y^2 = g(x)$, on peut facilement déterminer e au signe près (inévitable), en écrivant

$$e^2 = \frac{(cx + d)^{2g+2} f(\frac{ax+b}{cx+d})}{g(x)}.$$

Ainsi, la connaissance du groupe des automorphismes réduit est suffisante à la connaissance du groupe des automorphismes de la courbe.

2.1.2 Dévissage des classes de cohomologie

À présent et jusquà la fin de ce chapitre, $k = \mathbb{F}_q$. Dans cette section, on va ramener l'étude des tordues à l'étude de $\mathrm{Fr}(\mathrm{Aut}'(\mathcal{C}))$ afin de pouvoir utiliser les résultats de la section 1.3. En effet, $\mathrm{Aut}'(\mathcal{C})$ étant un sous-groupe de $\mathrm{Aut}(\mathbb{P}^1)$, on peut voir ses éléments comme des matrices 2×2 définies à une constante près. Ainsi, on pourra appliquer les résultats des sections 1.2 et 1.3 : à partir d'une matrice M appartenant à $\mathrm{Aut}'(C)$, on détermine une matrice A appartenant à $PGL_2(\overline{\mathbb{F}}_q)$ telle que

$$MA^{\varsigma} = A.$$

On va voir comment dévisser $H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_q}, \mathrm{Aut}(\mathcal{C}))$. En premier lieu, tout automorphisme α appartenant à $\mathrm{Aut}(\mathcal{C})$ s'inscrit dans un diagramme commutatif

$$\begin{array}{ccc} C & \xrightarrow{\alpha} & C \\ {\scriptstyle\Phi}\downarrow & & \downarrow{\scriptstyle\Phi} \\ \mathbb{P}^1 & \xrightarrow[\alpha']{} & \mathbb{P}^1 \end{array}$$

pour un certain automorphisme réduit α'. L'application $\alpha \to \alpha'$ est un morphisme de groupes (dépendant de Φ) et on a une suite exacte compatible avec l'action de Galois

$$1 \longrightarrow \{1, \iota\} \longrightarrow \mathrm{Aut}(\mathcal{C}) \longrightarrow \mathrm{Aut}'(\mathcal{C}) \longrightarrow 1$$

Il s'ensuit une longue suite exacte de cohomologie de Galois (cf. [CN07, partie II] et [Ser94, section 5.4]) :

$$1 \longrightarrow \{1, \iota\} \longrightarrow \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}) \longrightarrow \mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}) \longrightarrow H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_q/\mathbb{F}_q}, \{1, \iota\})$$

$$\longrightarrow H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_q/\mathbb{F}_q}, \mathrm{Aut}(\mathcal{C})) \longrightarrow H^1(\mathrm{Gal}_{\overline{\mathbb{F}}_q/\mathbb{F}_q}, \mathrm{Aut}'(\mathcal{C})) \longrightarrow 1.$$

Puisque tous les éléments des groupes considérés ont un ordre fini, la proposition 1 (p. 10) permet d'écrire la suite

$$1 \to \{1, \iota\} \to \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}) \to \mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}) \to \mathrm{Fr}(\{1, \iota\}) \to \mathrm{Fr}(\mathrm{Aut}(\mathcal{C})) \to^{\delta} \mathrm{Fr}(\mathrm{Aut}'(\mathcal{C})) \to 1. \quad (2.1.1)$$

Cette suite exacte montre qu'on peut calculer $Fr(\mathrm{Aut}(\mathcal{C}))$ dès qu'on connait $\mathrm{Fr}(\mathrm{Aut}'(\mathcal{C}))$ et $\mathrm{Fr}(\{1, \iota\})$. L'application

$$\delta : \mathrm{Fr}(\mathrm{Aut}(\mathcal{C})) \to \mathrm{Fr}(\mathrm{Aut}'(\mathcal{C}))$$

étant surjective, il suffit de calculer $\mathrm{Fr}(\mathrm{Aut}'(\mathcal{C}))$ et de compter le nombre de pré-image par δ de chacun de ses éléments. On est donc amené à calculer $|\mathrm{Fr}(\{1, \iota\})|$.

Lemme 2.

$$|\mathrm{Fr}(\{1, \iota\})| = 2$$

Démonstration. On va montrer que $\mathrm{Fr}(\{1, \iota\}) = \{\{1\}, \{\iota\}\}$. Pour cela, il suffit de vérifier que 1 et ι ne sont pas dans la même classe de conjugaison par Frobenius. C'est ce que dit le tableau suivant :

	$\alpha^{\varsigma} 1$	$\iota\alpha$
$\alpha = 1$	1	ι
$\alpha = \iota$	ι	1

□

D'après ce lemme, pour chaque élément α' de $\mathrm{Fr}(\mathrm{Aut}'(\mathcal{C}))$, α' a au plus 2 pré-images par δ. A présent, on va s'intéresser à une condition nécessaire et suffisante pour avoir qu'une seule pré-image.

2.1.3 Autodualité

On rappelle que ι est l'involution hyperelliptique (cf section 2.1.1). La tordue $\mathcal{C}_\iota$ est appelée la tordue hyperelliptique.

Remarque 4. *Lorsque $\mathcal{C}$ est définie par une équation de Weierstraß $y^2 = f(x)$, alors $\mathcal{C}_\iota$ admet une équation de la forme $y^2 = tf(x)$ où $t \in \mathbb{F}_q \setminus (\mathbb{F}_q)^2$. L'isomorphismes $\mathcal{C}$ sur $\mathcal{C}_\iota$ est alors donnée par :*

$$\varphi_\iota(x, y) \longrightarrow (x, \sqrt{t}y).$$

Dans les paragraphes suivants on étudie sous quelles conditions $\mathcal{C}$ et $\mathcal{C}_\iota$ sont isomorphes sur $\mathbb{F}_q$.

2.1.3.1 Définition et critères d'auto-dualité

Définition 11. *On dit que la courbe $\mathcal{C}$ est auto-duale si elle est $\mathbb{F}_q$-isomorphe à sa tordue hyperelliptique.*

On énonce un critère d'auto-dualité :

Proposition 7. *$\mathcal{C}$ est auto-duale si et seulement si $|Aut_{\mathbb{F}_q}(\mathcal{C})| = |\operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C})|$.*

Démonstration. Supposons que $\mathcal{C}$ soit auto-duale. De fait, $\mathcal{C}$ et sa tordue hyperelliptique $\mathcal{C}_\iota$ correspondent à une même classe de conjugaison par Frobenius dans $\operatorname{Fr}(\operatorname{Aut}(\mathcal{C}))$. D'après (2.1.1), le morphisme

$$\gamma : Fr(\{1, \iota\}) \to \operatorname{Fr}(\operatorname{Aut}(\mathcal{C}))$$

a pour noyau $\operatorname{Fr}(\{1, \iota\})$ de cardinal 2. On note

$$h : \operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C}) \to \operatorname{Fr}(\{1, \iota\}).$$

Par ailleurs, on a

$$|\operatorname{Ker}(h)| = \frac{|\operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C})|}{|Im(h)|}.$$

Ensuite, puisque $Im(h) = \operatorname{Ker}(\gamma)$ et $|\operatorname{Ker}(\gamma)| = 2$, on obtient

$$|\operatorname{Ker}(h)| = \frac{|\operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C})|}{2}.$$

On note

$$\beta : \operatorname{Aut}_{\mathbb{F}_q}(\mathcal{C}) \to \operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C}).$$

D'après la suite exacte (2.1.1), $|\operatorname{Ker}(\beta)| = 2$. On a donc

$$|Im(\beta)| = \frac{|\operatorname{Aut}_{\mathbb{F}_q}(\mathcal{C})|}{2}.$$

De plus, l'exactitude de la suite (2.1.1) permet d'écrire :

$$|Im(\beta)| = |\operatorname{Ker}(h)|.$$

Au final,

$$|\operatorname{Aut}_{\mathbb{F}_q}(\mathcal{C})| = |\operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C})|.$$

Réciproquement, on suppose que$|\operatorname{Aut}_{\mathbb{F}_q}(\mathcal{C})| = |\operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C})|$.
On reprend les mêmes notations que ci-dessus. Comme la suite (2.1.1) est exacte, on a

$$Im(\beta) = \operatorname{Ker}(h).$$

Ce qui entraine que

$$\frac{|\operatorname{Aut}_{\mathbb{F}_q}(\mathcal{C})|}{2} = \frac{|\operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C})|}{|Im(h)|}.$$

Étant donné que $|\operatorname{Aut}_{\mathbb{F}_q}(\mathcal{C})| = |\operatorname{Aut}'_{\mathbb{F}_q}(\mathcal{C})|$, on obtient

$$|Im(h)| = 2.$$

Grâce au lemme 2 (p. 21),

$$Im(h) = \operatorname{Fr}(\{1, \iota\}).$$

Et donc par exactitude de la suite (2.1.1) on a

$$\operatorname{Ker}(\gamma) = \operatorname{Fr}(\{1, \iota\}).$$

Par suite, 1 et ι sont dans la même classe de conjugaison par Frobenius dans $\operatorname{Fr}(\operatorname{Aut}(\mathcal{C}))$. Grâce à la proposition 1 (p. 10), on a montré que $\mathcal{C}$ et $\mathcal{C}_\iota$ sont $\mathbb{F}_q$-isomorphes. □

Remarque 5. *Cette proposition ainsi que la suite (2.1.1) entrainent que $\delta(\{\alpha\}_{\mathrm{Fr}})$ n'a qu'une pré-image par δ si et seulement si $\mathcal{C}_\alpha$ est auto-duale.*

Pour calculer toutes les tordues de $\mathcal{C}$, il est donc nécessaire de connaitre $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}_{\alpha'})$ et $\mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}_{\alpha'})$ pour tout $\{\alpha'\}_{\mathrm{Fr}} \in \mathrm{Fr}(\mathrm{Aut}'(\mathcal{C}))$.

2.1.3.2 Calcul de $\mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}_\alpha)$ et $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}_\alpha)$

Soit $\{\alpha\}_{\mathrm{Fr}} \in \mathrm{Fr}(\mathrm{Aut}(\mathcal{C}))$. On va calculer $\mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}_\alpha)$ et $\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}_\alpha)$ de la tordue $\mathcal{C}_\alpha$ de $\mathcal{C}$ en fonction de $\mathrm{Aut}'(\mathcal{C})$ et $\mathrm{Aut}(\mathcal{C})$.
Soit $\varphi_\alpha : C \to \mathcal{C}_\alpha$ un isomorphisme de C sur C_α. On a $\alpha = (\varphi_\alpha^{\varsigma})^{-1}\,\varphi_\alpha$. Le diagramme ci-dessous permet d'affirmer que $\mathrm{Aut}(\mathcal{C}_\alpha) = \varphi_\alpha\,\mathrm{Aut}(\mathcal{C})\,\varphi_\alpha^{-1}$.

$$\begin{array}{ccc} C & \longrightarrow & C \\ \downarrow{\scriptstyle \varphi_\alpha} & & \downarrow{\scriptstyle \varphi_\alpha} \\ \mathcal{C}_\alpha & \longrightarrow & \mathcal{C}_\alpha \end{array} \tag{2.1.2}$$

$\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}_\alpha)$ est donné par la proposition suivante.

Proposition 8.

$$\mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}_\alpha) = \{\varphi_\alpha\, u\, \varphi_\alpha^{-1} \,|u \in \mathrm{Aut}(\mathcal{C}), u = \alpha^{-1} u^{\varsigma} \alpha\}.$$

Démonstration. Soit $w \in \mathrm{Aut}_{\mathbb{F}_q}(\mathcal{C}_\alpha)$. D'après le diagramme précédent, il existe $u \in \mathrm{Aut}(\mathcal{C})$ tel que $w = \varphi_\alpha\, u\, \varphi_\alpha^{-1}$. De plus, $w^{\varsigma} = w$. Donc

$$(\varphi_\alpha\, u\, \varphi_\alpha^{-1})^{\varsigma} = \varphi_\alpha\, u\, \varphi_\alpha^{-1}\,.$$

Comme $\alpha = (\varphi_\alpha^{\varsigma})^{-1}\,\varphi_\alpha$, on obtient

$$u^{\varsigma}\alpha = \alpha u.$$

□

Soit $\Phi_\alpha : \mathcal{C}_\alpha \to \mathbb{P}^1$ le revêtement de degré 2 de $\mathcal{C}_\alpha$. Le diagramme (2.1.2) permet d'écrire

$$\begin{array}{ccccccc} C & \longrightarrow & C & \xrightarrow{\varphi_\alpha} & \mathcal{C}_\alpha & \longrightarrow & \mathcal{C}_\alpha \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi_\alpha} & & \downarrow{\scriptstyle \Phi_\alpha} \\ \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^1 \end{array}$$

Ainsi, il existe un unique automorphisme φ'_α de $\mathbb{P}_1$ tel que $\Phi_\alpha\,\varphi_\alpha = \varphi'_\alpha\,\Phi$. Le groupe réduit des $\mathbb{F}_q$-automorphismes de $\mathcal{C}_\alpha$ est donné par la proposition suivante.

Proposition 9.

$$\mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}_\alpha) = \{\varphi'_\alpha\, u'(\varphi'_\alpha)^{-1} | u' \in \mathrm{Aut}'(\mathcal{C}), (u')^{\varsigma}\alpha' = \alpha' u'\}$$

où α' est un représentant de l'image de $\{\alpha\}_{\mathrm{Fr}}$ par l'application naturelle $\mathrm{Fr}(\mathrm{Aut}(\mathcal{C})) \to \mathrm{Fr}(\mathrm{Aut}'(\mathcal{C}))$.

Démonstration. Soit $w' \in \mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}_\alpha)$. D'après le diagramme précédent, il existe $u \in \mathrm{Aut}(\mathcal{C})$ tel que $w'\Phi_\alpha = \Phi_\alpha\,\varphi_\alpha\, u\, \varphi_\alpha^{-1}$. Il existe aussi $u' \in \mathrm{Aut}(\mathbb{P}^1)$ tel que $\Phi u' = u\Phi$. On a alors :

$$w'\Phi_\alpha = \Phi_\alpha\,\varphi_\alpha\, u\, \varphi_\alpha^{-1} = \varphi'_\alpha\,\Phi u\, \varphi_\alpha^{-1} = \varphi'_\alpha\, u'\Phi\, \varphi_\alpha^{-1} = \varphi'_\alpha\, u'(\varphi'_\alpha)^{-1}\Phi_\alpha.$$

Comme Φ_α est surjectif, on obtient : $w' = \varphi'_\alpha\, u'(\varphi'_\alpha)^{-1}$. De plus, $w'^{\varsigma} = w'$. En conséquence

$$(\varphi'_\alpha\, u'(\varphi'_\alpha)^{-1})^{\varsigma} = \varphi'_\alpha\, u'(\varphi'_\alpha)^{-1}.$$

Comme $\alpha' = ({\varphi'_\alpha}^{\varsigma})^{-1}\,\varphi'_\alpha$, on obtient

$$(u')^{\varsigma}\alpha' = \alpha' u'.$$

□

2.1.4 Test pour l'auto-dualité

Soit $(M, e_M) \in \mathrm{Aut}(\mathcal{C})$ et A le cobord obtenu à partir de M grâce aux résultats de la partie 1.3.1. D'après la partie précédente, on construit le diagramme suivant :

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{(M,e_M)} & \mathcal{C} \\ \downarrow{\scriptstyle (A,e_A)} & & \downarrow{\scriptstyle (A,e_A)} \\ \mathcal{C}_\alpha & \xrightarrow[(M_\alpha, e^{M_\alpha})]{} & \mathcal{C}_\alpha \end{array}$$

avec $(M_\alpha, e_{M_\alpha}) = (AMA^{-1}, e_M)$. D'après la remarque 5 (p. 23), lorsque $\mathcal{C}_\alpha$ est auto-duale, $\delta(\{\alpha\}_{Fr})$ n'a qu'un antécédent. On n'a donc pas besoin de rajouter de tordue. Lorsqu'elle ne l'est pas, $\delta(\{\alpha\}_{Fr})$ a deux antécédents. Il faut rajouter la tordue quadratique. Dans ce cas, puisque δ envoie $\{\alpha\}_{Fr}$ et $\{\iota\alpha\}_{Fr}$ sur la même image [1], il faut rajouter la tordue associée à $\{\iota\alpha\}_{Fr}$, c'est à dire la tordue hyperelliptique de $\mathcal{C}_\alpha$.

Soit $M \in \mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}_\alpha)$. On pose

$$E_M = \frac{f(M.x) \times (cx+d)^{2g+2}}{f(x)}.$$

On a vu que $(M, \pm\frac{1}{\sqrt{E_M}}) \in \mathrm{Aut}(\mathcal{C}_\alpha)$. On déduit de cette écriture et des propositions précédentes un moyen efficace de savoir si la courbe $\mathcal{C}_\alpha$ est auto-duale ou non. C'est le test que nous utilisons dans l'implémentation (cf. la fonction `IsSelfDual` de l'annexe B.1.2).

Proposition 10. *Soit*

$$N_{\mathcal{C}_\alpha} = 2 \times \#\{E_M, E_M \in \mathbb{F}_q^{*2}, M \in \mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}_\alpha)\}.$$

$N_{\mathcal{C}_\alpha} = |\mathrm{Aut}'(\mathcal{C}_\alpha)|$ *si et seulement si* $\mathcal{C}_\alpha$ *est auto-duale.*

2.1.5 Calcul du groupe des automorphismes réduits

Dans ce paragraphe, on va expliquer comment calculer le groupe d'automorphismes réduits de $\mathcal{C}$. Dans ce but, on va détailler une approche utilisée dans l'article [LRS12] qu'on a légèrement améliorée dans le cas ou p ne divise pas le degré de la forme f. Soit f la forme binaire de degré n représentant le polynôme hyperelliptique de $\mathcal{C}$ définie sur $\overline{\mathbb{F}}_q$. On écrit $f(x,z) = \sum_{i=1}^{n} A_i x^i z^{n-i}$. Tout d'abord, quitte à appliquer une transformation $z \to z + \alpha x$, on peut supposer que A_n est non nul et donc, par homogénéité, choisir $A_n = 1$. Lorsque p ne divise pas n, on peut aussi supposer que $A_{n-1} = 0$ grâce à une seconde transformation linéaire. On suppose qu'on est dans ce cas. Déterminer le groupe d'automorphismes réduits de $\mathcal{C}$ revient à déterminer l'ensemble des matrices $M = (m_{i,j}) \in \mathrm{PGL}_2(\overline{\mathbb{F}}_q)$ telles que

$$f(m_{1,1}x + m_{1,2}z, m_{2,1}x + m_{2,2}z) = \lambda f(x,z) \text{ pour un certain } \lambda \in \overline{\mathbb{F}}_q^*. \tag{2.1.3}$$

Remarque 6. *C'est ici que l'on améliore l'approche de [LRS12]. Les auteurs éliminent directement le facteur λ. Ainsi, ils sont amenés à résoudre une équation polynomiale de degré n. En conservant λ, on évite la résolution d'une telle équation ce qui fait économiser le calcul dans une extension de $\mathbb{F}_q$ de degré n.*

Heuristiquement, on peut supposer que la forme f est suffisamment générale pour que $m_{1,1}m_{2,2} \neq 0$. Nous nous plaçons sous cette hypothèse. De ce fait, comme M est dans $\mathrm{PGL}_2(\overline{\mathbb{F}}_q)$, on peut chercher M sous la forme $M = \begin{pmatrix} 1 & b/d \\ c & 1/d \end{pmatrix}$. L'équation (2.1.3) se réécrit donc

$$f(x + b/dz, cx + 1/dz) = \lambda f(x,z).$$

1. car α et $\iota\alpha$ ne diffèrent que par leur action sur y et que cette dernière est tronquée par δ

Enfin, en changeant z en dz, le problème se réduit à chercher des éléments $\lambda, b, c, d \in \overline{\mathbb{F}}_q$ tels que

$$f(x + bz, cx + z) = \lambda f(x, dz). \tag{2.1.4}$$

Par la suite, on va exprimer λ, b, d en fonction de c puis calculer c.

1. On remplace (x, z) par $(1, 0)$ dans (2.1.4) et puisque $A_n = 1$, on obtient $\lambda = f(1, c)$.
2. On dérive (2.1.4) par rapport à z et on a

$$b\frac{\partial f}{\partial x}(x + bz, cx + z) + \frac{\partial f}{\partial z}(x + bz, cx + z) = \lambda d\frac{\partial f}{\partial z}(x, dz).$$

Puisque $A_{n-1} = 0$, $\frac{\partial f}{\partial z}(1, 0) = 0$; d'où

$$b\frac{\partial f}{\partial x}(1, c) = -\frac{\partial f}{\partial z}(1, c). \tag{2.1.5}$$

Remarque 7. *L'élément b est entièrement déterminé par l'équation (2.1.5). En effet, f étant homogène de degré n, $n\lambda = \frac{\partial f}{\partial x}(1, c) + c\frac{\partial f}{\partial z}(1, c)$. Puisque p ne divise pas n, si $\frac{\partial f}{\partial x}(1, c) = \frac{\partial f}{\partial z}(1, c) = 0$ alors $\lambda = f(1, c) = 0$. Or, λ est supposé non nul.*

Soit $i \in \{2 \dots n\}$. On dérive i fois (2.1.4) par rapport à z :

$$\sum_{j=0}^{i} \binom{i}{j} b^j \frac{\partial^i f}{(\partial x)^j (\partial z)^{i-j}}(x + bz, cx + z) = \lambda d^i \frac{\partial^i f}{(\partial z)^i}(x + bz, cx + z).$$

On multiplie cette équation par $\frac{\partial f}{\partial x}(1, c)$ puis on remplace (x, z) par $(1, 0)$, λ par $f(1, c)$, $\frac{\partial^i f}{(\partial z)^i}(1, 0)$ par $i!A_{n-i}$, et $b\frac{\partial f}{\partial x}(1, c)$ par $-\frac{\partial f}{\partial z}(1, c)$. On obtient ainsi les équations suivantes :

$$\sum_{j=0}^{i} \binom{i}{j} \Big(-\frac{\partial f}{\partial z}(1, c)\Big)^j \Big(\frac{\partial f}{\partial x}(1, c)\Big)^{i-j} \frac{\partial^i f}{(\partial x)^j (\partial z)^{i-j}}(1, c) = i!\, A_{n-i}\, f(1, c) d^i \Big(\frac{\partial f}{\partial x}(1, c)\Big)^i. \tag{2.1.6}$$

On remarque que la partie gauche de l'égalité (2.1.6) est un polynôme multiple de $f(1, c)$. On peut donc diviser chaque coté de l'égalité par $f(1, c)$. Il en résulte une équation de degré $i(n-1)$ en c et i en d.

3. Si on divise (2.1.6) pour $i = 3$ par (2.1.6) pour $i = 2$ on obtient une équation linéaire en d qui dépend de c.

Il faut donc déterminer la valeur de c. Dans cette logique, on divise le carré de (2.1.6) pour $i = 3$ par le cube de (2.1.6) pour $i = 2$. Cela permet d'éliminer la variable d. On a donc un polynôme, univarié, P_1 de degré au plus $9n - 12$ qui s'annule en c. Pour chaque racine c de P_1, on calcule λ, b et d grâce à 1., 2. et 3. On teste alors si l'élément obtenu est un automorphisme de f.

Afin de diminuer le degré du polynôme à tester et réduire ainsi la complexité de l'algorithme lorsque $n > 3$, on calcule un second polynôme, P_2. Pour l'obtenir, on divise (2.1.6) pour $i = 4$ par le carré de (2.1.6) pour $i = 2$. Ce polynôme est de degré au plus $6n - 8$. Génériquement, $\gcd(P_1, P_2) = 1$. Lorsque ce n'est pas le cas, on calcule les racines de ce pgcd et on effectue le même raisonnement que précédemment.

Remarque 8. *Dans nos programmes des annexes B.1.2 et B.2, on utilise l'implémentation de [LRS12] pour le calcul du groupe d'automorphismes réduits. Ce programme a été écrit pour calculer des isomorphismes définis sur un corps donné $\mathbb{F}_q$ et exécute un certains nombres de tirages aléatoires dans $\mathbb{F}_q$ pour se placer dans les hypothèses heuristiques du paragraphe. S'il n'y arrive pas, il se résigne à utiliser la fonction basique de* `Magma` *pour ce calcul. Au cours de nos tests, on s'est rendu compte que lorsque f est scindée et que $|\mathbb{F}_q|/\deg(f)$ est petit, le programme entre dans cette phase finale. Par exemple lorsque $f = x^{52} - 1$ sur $\mathbb{F}_{53}$, le temps de calcul sur*

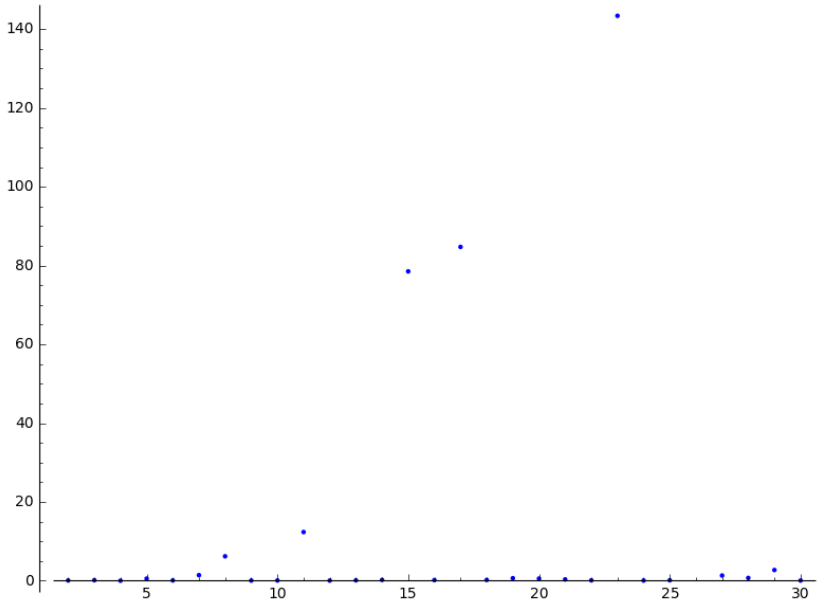
notre machine est $209.630s$ *alors que pour le même* f *mais sur* $\mathbb{F}_{10007}$*, le temps de calcul est* $7.060s$*. Le fait que l'on cherche un groupe d'automorphismes réduits nous permet cependant de sortir de* $\mathbb{F}_q$ *et de faire nos tirages sur une (petite) extension. Ainsi, lorsque l'on prend le même* f *mais sur* $\mathbb{F}_{53^2}$*, le temps de calcul n'est plus que de* $1.930s$*. Nous n'avons cependant pas réalisé une étude précise des cas d'application de cette stratégie.*

2.1.6 Tests de l'algorithme

Une implémentation `Magma` de ces résultats a été réalisée (cf Annexe B.1.2). Voici quelques statistiques sur l'efficacité de notre algorithme.

Lorsque l'on fixe le corps de définition et que l'on fait varier le genre de la courbe Soit $\mathtt{g}$ un entier naturel, la courbe hyperelliptique d'équation $y^2 = x^{2\,\mathtt{g}+2} - 1$ définie sur $\mathbb{F}_{10007}$ a un groupe d'automorphismes qui contient $\mathbf{D}_{2\,\mathtt{g}+2}$. On a fait varier $\mathtt{g}$ et on a obtenu la figure 2.1. On fait varier le genre entre 2 et 30 et les temps de calculs sont exprimés en seconde. Les temps de calculs sont d'autant plus long lorsque le groupe d'automorphismes est défini sur une extension grande de $\mathbb{F}_{10007}$.

FIGURE 2.1 – Temps de calcul de la procédure qui calcule les tordues de courbes hyperelliptique de l'annexe B.1.2 en fonction du genre de la courbe $y^2 = x^{2\,\mathtt{g}+2} - 1$ définie sur $\mathbb{F}_{10007}$.



Lorsque l'on fixe le corps de définition et que l'on fait varier le groupe d'automorphismes réduits On fixe le corps $k = \mathbb{F}_p$ avec

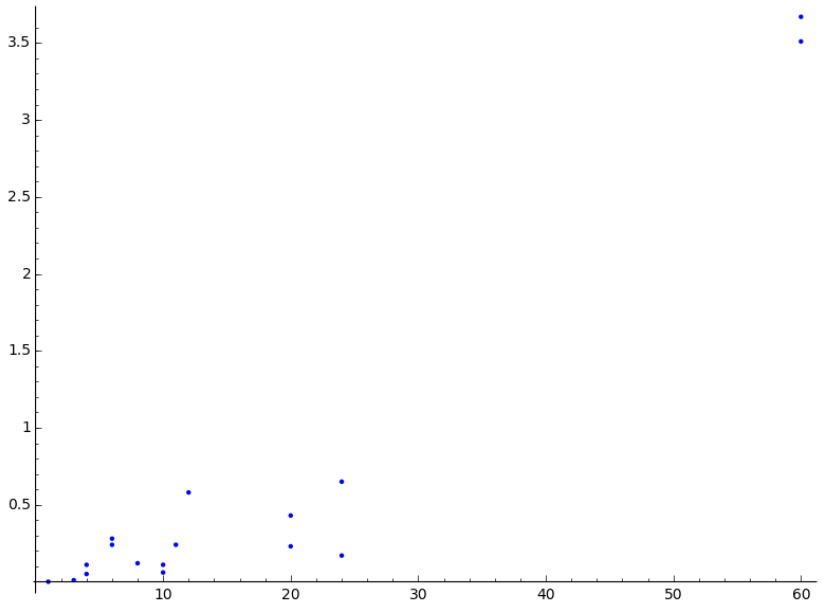
$$p = 10000000000000000000000000000000000000000000000577.$$

On note i une racine carré de -1 dans $\mathbb{F}_p$. On considère les courbes $\mathcal{C}_G$ suivantes qui sont toute de genre 6. Elles ont pour groupe d'automorphisme G.

$$
\begin{aligned}
\mathcal{C}_{\mathbf{C}_1} &: y^2 = x^{11} + 3x^9 + 7x^4 + 3x^2 + x + 1 \\
\mathcal{C}_{\mathbf{C}_3} &: y^2 = ((x^3 - 1)^2 + 1)^2 - (x^3 - 1) \\
\mathcal{C}_{\mathbf{C}_4} &: y^2 = ((x^4 - 1) + 1)^3 - (x^8 + 1) \\
\mathcal{C}_{\mathbf{D}_4} &: y^2 = (x^6 - 1)(x^4 + 1)x \\
\mathcal{C}_{\mathbf{D}_8} &: y^2 = (x^4 + 1)(x^8 + 1) \\
\mathcal{C}_{\mathbf{D}_6} &: y^2 = (x^9 - 1)(x^3 + 1) \\
\mathcal{C}'_{\mathbf{D}_6} &: y^2 = x^{12} + x^9 + x^6 + x^3 + 1 \\
\mathcal{C}_{\mathbf{D}_{10}} &: y^2 = x(x^{10} + 3x^5 + 1) \\
\mathcal{C}'_{\mathbf{D}_{10}} &: y^2 = (123x + 72)((123x + 72)^{10} - 1) + 245((123x + 72)^5 - 1)^2(123x + 72) \\
\mathcal{C}_{\mathbf{C}_{11}} &: y^2 = x^{11} - 1 \\
\mathcal{C}_{\mathbf{D}_{12}} &: y^2 = x^{12} + x^6 + 1 \\
\mathcal{C}_{\mathbf{D}_{20}} &: y^2 = x^{11} - x \\
\mathcal{C}'_{\mathbf{D}_{20}} &: y^2 = (23x + 42)^{11} - 23x - 42 \\
\mathcal{C}_{\mathbf{D}_{24}} &: y^2 = x^{12} - 1 \\
\mathcal{C}_{\mathcal{S}_4} &: y^2 = (x^4 + 1)(x^8 - 34x^4 + 1) \\
\mathcal{C}_{\mathcal{A}_n} &: y^2 = x(x^{10} + 11ix^5 + 1) \\
\mathcal{C}'_{\mathcal{A}_n} &: y^2 = (x - 1)((x - 1)^{10} + 11i(x - 1)^5 + 1)
\end{aligned}
$$

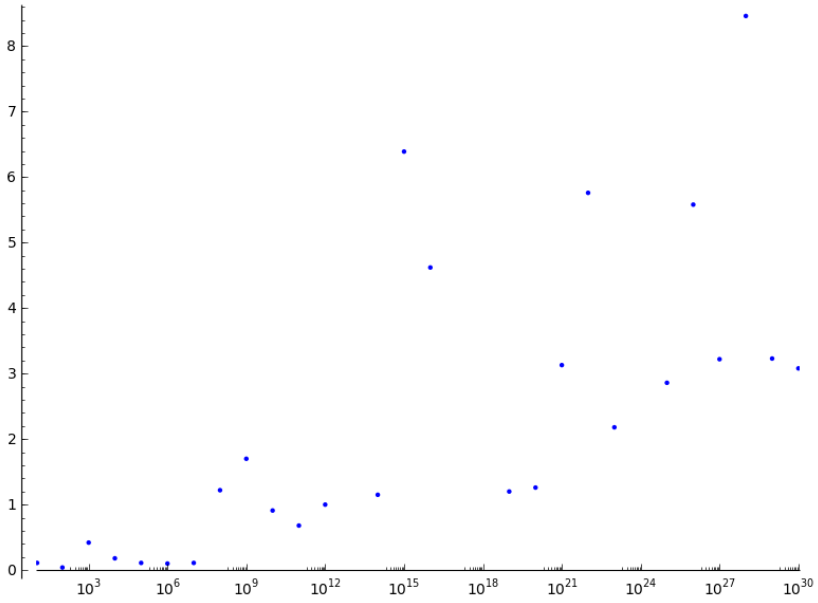
La figure 2.2 est la représentation du temps de calcul des tordues de $\mathcal{C}_G$ en fonction du cardinal de G.

FIGURE 2.2 – Temps de calcul de la procédure qui calcule les tordues de courbes hyperelliptiques de l'annexe B.1.2 en fonction cardinal du groupe d'automorphisme réduit de la courbe $\mathcal{C}$ de genre 6. On représente en abscisse la taille de $\mathrm{Aut}'(\mathcal{C})$ et en ordonnée le temps de calcul en secondes. Le temps de calcul du groupe des automorphismes réduits n'est pas pris en compte.



Lorsque l'on fixe le genre et que l'on fait varier le corps de définition On considère la courbe $\mathcal{C}$ définie sur $\mathbb{F}_p$ par $y^2 = x^{18} - 1$ et on fait varier p. On considère des p premiers tels que son groupe d'automorphisme est $\mathbf{D}_{36}$. Le temps de calcul du groupe des automorphismes réduits n'est pas pris en compte. Les résultats sont présentés dans la figure 2.3.

FIGURE 2.3 – Temps de calcul de la procédure qui calcule les tordues de courbes hyperelliptiques de l'annexe B.1.2 en fonction du corps de définition de la courbe $y^2 = x^{18} - 1$. On représente en abscisse le cardinal de $\mathbb{F}_q$ sur une échelle logarithmique et en ordonnée le temps de calcul en secondes. Le temps de calcul du groupe des automorphismes réduits n'est pas pris en compte.



En pratique on ne dispose que du groupe d'automorphismes réduits de la courbe $\mathcal{C}$. Grâce à la propositions 9 (p. 23), on retrouve aussi groupe d'automorphismes réduits des tordues de $\mathcal{C}$, ce qui rend ce critère facilement implémentable. En effet, soit A une représentation dans $\mathrm{PGL}_2(\overline{\mathbb{F}}_q)$ de la partie en x d'un isomorphisme de $\mathcal{C}$ sur $\mathcal{C}_\alpha$. Un élément de $\mathrm{Aut}'_{\mathbb{F}_q}(\mathcal{C}_\alpha)$ est donné par AMA^{-1} où $M \in \mathrm{Aut}'(\mathcal{C})$ tel que $AMA^{-1} \in \mathrm{PGL}_2(\mathbb{F}_q)$. On va à présent voir comment calculer le groupe d'automorphismes réduits de $\mathcal{C}$.

2.2 Le cas des quartiques planes lisses

Dans [LRRS14] (voir aussi l'annexe C, nous avons eu besoin d'un algorithme qui calcule toutes les quartiques planes lisses définies sur $\mathbb{F}_q$ à $\mathbb{F}_q$-isomorphismes près. L'utilisation de bonnes familles (voir la partie II) permet d'obtenir des représentants sur $\mathbb{F}_q$ pour les classes de $\overline{\mathbb{F}}_q$-isomorphismes. Une fois ces répresentants construits, il s'agit donc de calculer les tordues pour chaque classe d'isomorphismes géométriques. Deux stratégies différentes ont été employées et nous les expliquons dans cette section.
Lorsque la strate correspond à un groupe d'automorphismes large, comme par exemple pour la quartique de Dick-Fermat qui possède 96 automorphismes, les tordues sont calculées avec les résultats du paragraphe 1.3.2 alliés à l'amélioration ci-dessous qui est décrite dans le préprint [LG15] (voir section 2.2.1). Lorsque le groupe d'automorphismes est plus petit, on calcule les tordues manuellement (voir paragraphe 2.2.2).

2.2.1 Représentation affine des automorphismes

Dans la section 1.3.1, le fait que les automorphismes soient des éléments de $\mathrm{PGL}_3(\mathbb{F}_{q^n})$ (pour un certain $n \geq 1$) impose la présence d'un facteur multiplicatif λ dans les relations de cocycles. L'élimination de ce dernier, afin de réaliser un Hilbert 90 effectif, demande souvent une extension du corps de définition de l'automorphisme et donc un surcoût de complexité. Dans le cas présent, il est possible d'éviter ce problème. En effet l'action des automorphismes dans le plan projectif est induite par l'action sur les différentielles régulières. Il existe donc une représentation affine du groupe des automorphismes dans $\mathrm{GL}_3(\mathbb{F}_{q^n})$ et on peut travailler directement à ce niveau.

Pour chaque matrice représentant un automorphisme, nous devons donc simplement calculer un facteur multiplicatif de normalisation. Nous ne savons malheureusement pas comment faire cela simplement et nous utilisons la fonction pré-implémentée de `Magma` pour recalculer toute l'action de l'automorphisme sur les différentielles de la manière suivante.

```
MatrixRepresentation(A) : GrpAutCrv -> Grpmat, Map, SeqEnum.
```

Exemple 6. *Ci-dessous un exemple de calcul de cette représentation lorsque $\mathcal{C}$ est la quartique plane lisse définie par l'équation $12X^4 + Y^4 + Z^4 + 12X^2YZ + 3Z^2Y^2 = 0$ sur $\mathbb{F}_{13}$.*

```
magma : FF := GF(13);
magma : a:=12;
magma : b:=3;
magma : P<X,Y,Z>:=PolynomialRing(FF,3);
magma : PP:=ProjectiveSpace(P);
magma : Phi := a*X^4 + Y^4 + Z^4 + a*X^2*Y*Z + b*Z^2*Y^2;
magma : C := Curve(PP,Phi);
magma : g1 := iso<C->C|[X,5*Y,8*Z],[X,8*Y,5*Z]>;
magma : g2 := iso<C->C|[X,Z,Y],[X,Z,Y]>;
magma : L := AutomorphismGroup(C,[g1,g2]);
magma : G,f,B := MatrixRepresentation(L);
magma : G;

MatrixGroup(3, GF(13)) of order 2^3
Generators:
    [ 1  0  0]
    [ 0  5  0]
    [ 0  0  8]

    [12  0  0]
    [ 0  0 12]
    [ 0 12  0]

magma :  f;
Mapping from: GrpAutCrv: L to GrpMat: G
Composition of Mapping from: GrpAutCrv: L to GrpPerm: $, Degree 8, Order 2^3
given by a rule and
Mapping from: GrpPerm: $, Degree 8, Order 2^3 to GrpMat: G

magma :  B;
[ (1/($.1^4 + 1)*$.1^2 + 7*$.1/($.1^4 + 1)) d($.1), (7*$.1^2/($.1^8 + 3*$.1^6 +
    2*$.1^4 + 3*$.1^2 + 1)*$.1^3 + ($.1^5 + 10*$.1^3 + $.1)/($.1^8 + 3*$.1^6 +
    2*$.1^4 + 3*$.1^2 + 1)*$.1) d($.1), (7*$.1/($.1^8 + 3*$.1^6 + 2*$.1^4 +
```

```
3*$.1^2 + 1)*$.1^3 + ($.1^4 + 10*$.1^2 + 1)/($.1^8 + 3*$.1^6 + 2*$.1^4 +
3*$.1^2 + 1)*$.1) d($.1) ]
```

A présent, on va donner un exemple de calcul manuel d'une tordue de $\mathcal{C}$ dans un cas particulier.

2.2.2 Un exemple de calcul de tordue "à la main"

Quand le groupe d'automorphismes est relativement simple, il est souvent possible d'obtenir les classes représentatives dans $\mathrm{Fr}(\mathrm{Aut}(\mathcal{C}))$ et de calculer manuellement les tordues. Dans les programmes de [LRRS14], cela a été fait dans les cas $\mathrm{Aut}(\mathcal{C}) = \mathbf{C}_2$, $\mathbf{D}_4$, $\mathbf{C}_3$, $\mathbf{D}_8$, et $\mathcal{S}_3$. On prend par exemple $\mathbf{D}_8$. D'après [LRRS14, th. 3.3], toute quartique plane lisse $\mathcal{C}$ définie sur $\mathbb{F}_q$ avec $\mathrm{Aut}(\mathcal{C}) \simeq \mathbf{D}_8$ est $\overline{\mathbb{F}}_q$-isomorphe à une courbe d'équation $x^4 + x^2yz + y^4 + ay^2z^2 + bz^4$ avec $a, b \in \mathbb{F}_q$. Le problème se décompose en différents cas selon la congruence de $q - 1 \mod 4$ et de la classe de b dans $\mathbb{F}_q^*/(\mathbb{F}_q^*)^4$. On suppose que $4|(q-1)$ et b est une puissance de 2 dans $\mathbb{F}_q$ mais pas une puissance de 4, c'est à dire $b = r^4$ avec $r \in \mathbb{F}_{q^2}$ et $r^q = -r$. Les 8 automorphismes sont donc définis sur $\mathbb{F}_{q^2}$: si i est une racine carré de -1, le groupe d'automorphismes est généré par

$$S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{bmatrix} \text{ et } T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & r \\ 0 & r^{-1} & 0 \end{bmatrix}.$$

On a $\mathrm{Fr}(\mathrm{Aut}(\mathcal{C})) = \left\{ \{Id\}_{\mathrm{Fr}}, \{S\}_{\mathrm{Fr}}, \{T\}_{\mathrm{Fr}}, \{S^3\}_{\mathrm{Fr}} \text{ et } \{ST\}_{\mathrm{Fr}} \right\}$. Dans ce cas, il y a 5 tordues.

Voici les détails du calcul de la tordue correspondant à $\{T\}_{\mathrm{Fr}}$: on cherche une matrice A telle que $TA = A^{\varsigma}$. Choisissant A telle que $A(x, y, z)^t = (x, \alpha y + \beta z, \gamma y + \delta z)^t$, on a besoin de résoudre le système suivant :

$$\alpha^{\varsigma} = r\gamma,\ \gamma^{\varsigma} = r^{-1}\alpha,\ \beta^{\varsigma} = r\delta \text{ et } \delta^{\varsigma} = r^{-1}\beta.$$

La première équation détermine γ en fonction de α. On doit donc seulement satisfaire les conditions de compatibilité données par la seconde équation. On applique ς à cette dernière et on obtient : $\alpha^{q^2} = (r\gamma)^q = -r\gamma^q = -\alpha$. Ainsi, $\alpha^{q^4} = \alpha$ Comme le raisonnement sur β et δ est totalement analogue, il suffit de trouver α et β dans $\mathbb{F}_{q^4}$ tels que

$$\det \begin{pmatrix} \alpha & \beta \\ \alpha^q/r & \beta^q/r \end{pmatrix} \neq 0.$$

On peut choisir $\alpha = \sqrt[4]{\tau}$ et $\beta = \alpha^3$ avec τ un élément primitif de $\mathbb{F}_q^*$. De part la définition de τ, $\alpha^q = i\alpha$ avec i une racine carrée de -1 et $\beta^q = -i\alpha^3$. Après avoir appliqué cette transformation, on obtient la tordue suivante :

$$x^4 + (2\tau - a\tau r^2)y^4 + (2\tau^2 - a\tau^3 r^2)z^4 + i\frac{\sqrt{\tau}}{r}x^2y^2 - i\frac{\sqrt{\tau}}{r}\tau x^2z^2 + (12\tau + 2a\tau^2 r^2)y^2z^2.$$

On remarque qu'elle est bien définie sur $\mathbb{F}_q$ car i, τ et $r^2 \in \mathbb{F}_q$. De plus, $\frac{\sqrt{\tau}}{r} \in \mathbb{F}_q$ car $(\frac{\sqrt{\tau}}{r})^q = \frac{-\sqrt{\tau}}{-r} = \frac{\sqrt{\tau}}{r}$.

Deuxième partie

Descente et espace de modules

Chapitre 3

Utilisation de la descente pour la construction de familles représentatives des quartiques planes lisse d'un corps fini

Ce chapitre reprend les résultats de [LRRS14] et complète les preuves esquissées dans l'article faute de place. On va, dans un premier temps introduire les éléments de théorie dont nous avons besoin. Ensuite, on construira des familles représentatives pour les quartiques planes lisses. On donnera les preuves détaillées de la construction de ces familles.

3.1 La théorie

3.1.1 Descente de Weil

Dans ce paragraphe, on énonce d'abord le théorème de Weil avec sa formulation originelle. On s'inspire pour cela de [Wei56, p. 510].

Soit K une extension algébrique séparable de k de degré n. On appèle $\mathrm{Iso}_k(K \to \overline{k})$ l'ensemble des isomorphismes de K dans $\overline{k}$ laissant invariant k. Si $\sigma \in \mathrm{Iso}_k(K \to \overline{k})$, on note K^σ le sous corps de K invariant par σ. Soient $\xi \in K$ et $\sigma \in \mathrm{Iso}_k(K \to \overline{k})$, on note ξ^σ l'image par σ de ξ. Si ω est un isomorphisme de K^σ laissant invariant k, on note $\sigma\omega$ l'isomorphisme de K défini par $\xi^{\sigma\omega} := (\xi^\sigma)^\omega$ pour tout $\xi \in K$.

Soit V une variété définie sur K. Weil définit la descente galoisienne en terme de morphisme birationnel.

Définition 12. *On dit que la variété V* descend *sur k s'il existe une variétée V_0, définie sur k, et un morphisme birationnel f, définie sur K, entre V et V_0.*

Dans ce cas pour tout $\sigma, \tau \in \mathrm{Iso}_k(K \to \overline{k})$, l'application $f_{\tau,\sigma} = f^\tau \circ (f^\sigma)^{-1}$ est un morphisme birationnel entre V^σ et V^τ. Weil énonce le problème de descente suivant :
"Soient V une variété définie sur K et pour chaque paire d'élément (σ, τ) de $\mathrm{Iso}_k(K \to \overline{k})$, $f_{\tau,\sigma}$ un morphisme birationnel entre V^σ et V^τ. Trouver une variétée V_0 définie sur k et un morphisme birationnel f, définies sur K, entre V_0 et V, telles que $f_{\tau,\sigma} = f^\tau \circ (f^\sigma)^{-1}$ pour tout $\sigma, \tau \in \mathrm{Iso}_k(K \to \overline{k})$."

Théorème 2. *Ce problème a une solution si et seulement si les applications $f_{\tau,\sigma}$ sont définies sur une extension algébrique séparable de k et satisfont les propriétés suivantes :*

- *$f_{\tau,\rho} = f_{\tau,\sigma} \circ f_{\sigma,\rho}$ pour tout $\sigma, \tau, \rho \in \mathrm{Iso}_k(K \to \overline{k})$;*
- *$f_{\tau\omega,\sigma\omega} = (f_{\tau,\sigma})^\omega$ pour tout automorphismes ω de $\overline{k}$ sur k.*

De plus, quand cela est vérifié, la solution est unique à transformation birationnelle de V_0 définie sur k.

On préfère de nos jours une formulation en terme d'isomorphismes plutôt que de morphismes birationnels (dans le cas des courbes lisses, il n'y a bien sûr pas de différence).

Définition 13. *On dit que la variété V* descend *sur k s'il existe une variétée V_0, définie sur k, et un isomorphisme f, définie sur K, entre V et V_0.*

Le théorème de Weil ci-dessus reste valide en remplaçant les morphismes birationnels par les isomorphismes lorsque V est une sous-variétées localement fermée dans un espace projectif [Ser84, ch.V sec.4 par.20], ce qui sera toujours notre cas dans la suite. On utilisera dans nos démonstration la formulation équivalente suivante.

Corollaire 2. *Soient K est une extension galoisienne finie de k et V une variété localement fermée dans un espace projectif définie sur K. Pour chaque élément σ du groupe de Galois de K sur k, s'il existe un isomorphisme $h_\sigma : V \to V^\sigma$ alors la variété V descend sur k avec f vérifiant $h_\sigma = f^\sigma f^{-1}$ si et seulement si pour tout élément σ, τ du groupe de Galois de K sur k, $h_{\sigma\tau} = (h_\sigma)^\tau h_\tau$.*

Démonstration. On pose $f_{\tau,\sigma} = h^\sigma_{\tau\sigma^{-1}}$ alors $f_{\tau,\sigma}$ est un isomorphisme entre V^σ et V^τ. Supposons que $h_{\sigma\tau} = (h_\sigma)^\tau h_\tau$. Soient σ, τ, ρ des éléments du groupe de Galois de K sur k et ω un automorphisme de $\overline{k}$ sur k. On cherche à montrer que

— $f_{\tau,\rho} = f_{\tau,\sigma} \circ f_{\sigma,\rho}$ pour tout $\sigma, \tau, \rho \in \mathrm{Iso}_k(K \to \overline{k})$;
— $f_{\tau\omega,\sigma\omega} = (f_{\tau,\sigma})^\omega$ pour tout automorphismes ω de $\overline{k}$ sur k.

Ainsi, on pourra appliquer le théorème 2 (p. 33). On a

$$(f_{\tau,\sigma} \circ f_{\sigma,\rho})^{\rho^{-1}} = (h^\sigma_{\tau\sigma^{-1}} h^\rho_{\sigma\rho^{-1}})^{\rho^{-1}} = h^{\sigma\rho^{-1}}_{\tau\sigma^{-1}} h_{\sigma\rho^{-1}} = h_{\tau\rho^{-1}} = (f_{\tau,\rho})^{\rho^{-1}}$$

De plus on a,

$$f_{\tau\omega,\sigma\omega} = h^{\sigma\omega}_{\tau\omega\omega^{-1}\sigma^{-1}} = (h^\sigma_{\tau\sigma^{-1}})^\omega = (f_{\tau,\sigma})^\omega.$$

Réciproquement, soient σ, τ des éléments du groupe de Galois de K sur k.

$$h_{\sigma\tau} = f^{\sigma\tau} f^{-1} = f^{\sigma\tau} f^{\tau^{-1}} f^\tau f^{-1} = (h_\sigma)^\tau h_\tau.$$

□

3.1.2 Espace de modules

Lorsqu'on étudie certains objets, il est toujours souhaitable de les regrouper selon différents critères, de façon à distinguer des comportements similaires. Les espaces de modules sont des solutions élégantes aux problèmes de classification des courbes à isomorphisme près.

Définition 14. *On appelle* espace de modules *des courbes de genre $\mathtt{g}$ sur k l'ensemble des classes de $\overline{k}$-isomorphisme de courbes (lisses, projectives absolument irréductibles) de genre $\mathtt{g}$. On note $\mathcal{M}_\mathtt{g}(k)$ cet ensemble et $[\mathcal{C}]$ un point de $\mathcal{M}_\mathtt{g}(k)$ avec $\mathcal{C}$ un représentant de la classe d'isomorphisme. Le* groupe d'automorphismes de $[\mathcal{C}]$ *est le groupe d'automorphismes de $\mathcal{C}$.*

De plus, $\mathcal{M}_\mathtt{g}(k)$ est une variété quasi projective. Lorsque $\mathtt{g} = 1$, cet espace est de dimension 1 et lorsque $\mathtt{g} > 1$, cet espace est de dimension $3\,\mathtt{g} - 3$. Le sous-espace de $\mathcal{M}_\mathtt{g}(k)$ des classes de $\overline{k}$-isomoprhisme de courbes hyperelliptiques de genre $\mathtt{g}$ est de dimension $2\,\mathtt{g} - 1$ (cf [MF82]).

Afin de manipuler cet ensemble de manière effective, on associe injectivement à chaque point de l'espace une liste d'éléments de $\overline{k}$ (appelés invariants absolus). Ceci sera l'objet de la section 4. Le cas plus précis du genre 2 sera développé dans la section 5.1.3.2. Inversement, on peut également souhaiter mettre en place une procédure pour inverser cette fonction sur son image,

ce qu'on appellera *reconstruire la courbe* à partir de ses invariants. Ceci sera l'objet du chapitre 6 où l'on verra comment faire cela dans le cas du genre 2, en toute caractéristique différente de 2. Les invariants absolus définissent un certain sous-corps de $\overline{k}$, qui est (dans la plupart des cas) le plus petit corps où l'on peut espérer reconstruire la courbe. Nous étudierons, en particulier dans la cas du genre 2 si cela est possible ou non. La section suivante va exposer quelques définitions et faits généraux sur ce sujet. Quelques résultats spécifiques aux courbes hyperelliptiques seront ensuite donnés.

3.1.3 Strates de l'espace de modules

On s'intéresse aux sous-variétés de $\mathcal{M}_{\mathtt{g}}(k)$ dont les courbes correspondantes ont un groupe d'automorphismes donné. À priori, on aimerait définir une strate comme étant une sous-variété de $\mathcal{M}_{\mathtt{g}}(k)$ dont chaque point a un groupe d'automorphismes donné. Or, ces sous-variétés ne sont pas nécessairement irréductibles. Ce problème a aussi été mentionné et étudié dans [MSSV02], et résolu par les schémas de Hurwitz. Néanmoins, dans ce paragraphe, on priviligie une autre façon de contourner le problème due à Lønsted dans [Løn80, Sec. 6]. En utilisant "une action rigidifiée" des groupes d'automorphismes, l'espace de modules $\mathcal{M}_{\mathtt{g}}(k)$ y est stratifié de manière plus fine. Étant donné un groupe d'automorphismes G, Lønsted définit un sous-schéma de $\mathcal{M}_{\mathtt{g}}(k)$ de la façon suivante.

Définition 15. *Soient l un nombre premier différent de p et $\mathrm{Sp}_{2g}(\mathbb{F}_l)$. Une* strate *de l'espace de modules $\mathcal{M}_{\mathtt{g}}(k)$ est l'ensemble des points $[\mathcal{C}]$ de $\mathcal{M}_{\mathtt{g}}(k)$ tels que le plongement induit de G dans le groupe des morphismes polarisés de $\mathrm{Jac}(\mathcal{C})[l]$ est $\mathrm{Sp}_{2g}(\mathbb{F}_l)$-conjugué à un groupe donné.*

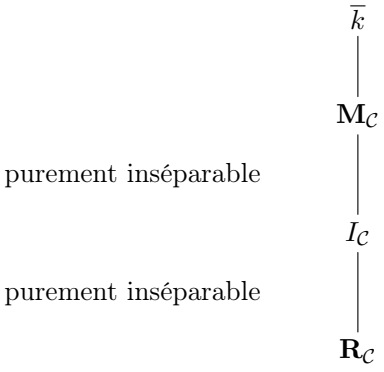
En combinant [Hom81, th.1] avec [Løn80, th.6.5], lorsque $p = 0$ ou $p > 2g + 1$, une telle strate est localement fermée, connexe et est un sous-schéma lisse de $\mathcal{M}_{\mathtt{g}}(k)$. Si k est parfait alors une telle strate connexe est définie sur k si une seule rigidification est possible pour un groupe d'automorphismes donné. Cela n'est pas toujours le cas mais on verra dans la remarque 10 (p. 39) que dans le cas des quartiques planes lisses cette subtilité n'a pas lieu d'être.

3.1.4 Corps de modules et corps de définition

Soit V une variété définie sur $\overline{k}$. Il existe dans la littérature plusieurs définitions de corps de modules. On suit celle de [Hug05] qui s'appuie sur [Koi72] et [Sek85].

Définition 16. *Soit $K \subset \overline{k}$. On dit que K est un* corps de définition *de V s'il existe un* modèle *V_0/K c'est à dire une variété V_0 définie sur K telle que $V_0 \cong_{\overline{k}} V$. Soit $H = \{\sigma \in \mathrm{Aut}(\overline{k}), V \cong V^{\sigma}\}$. Le* corps de modules *de V est le corps fixe $\mathbf{M}_V = \overline{k}^H$.*

[Hug05, p. 14 Th 1.5.8] re-démontre un théorème de Koizumi affirmant que $\mathbf{M}_V$ est une extension purement inséparable de l'intersection de tous les corps de définition de V noté I_V. Quelquefois, I_V est également pris comme définition de corps de modules. On note qu'en général I_V n'est pas un corps de définition pour V. On présentera d'ailleurs des exemples avec les courbes de genre 2 Lorsque V est une courbe $\mathcal{C}$ de genre $\mathtt{g} \geq 2$, il existe une autre définition naturelle de corps de modules en tant que corps résiduel $\mathbf{R}_{\mathcal{C}}$ du point $[\mathcal{C}] \in \mathcal{M}_{\mathtt{g}}(k)$. [Sek85] montre que $I_{\mathcal{C}}$ est une extension purement inséparable de $\mathbf{R}_{\mathcal{C}}$. En résumé :



En conséquence, si l'extension de $\overline{k}$ sur son sous-corps premier est une extension séparable (c'est le cas en caractéristique 0 ou lorsque $\overline{k} = \overline{\mathbb{F}}_p$) les trois notions coïncident.

Cependant, même si on considère des courbes sur des corps finis, l'étude de famille de courbes entraine rapidement l'analyse des extensions non séparables. Dans [LRRS14], on évacue ce problème en considérant la caractéristique p de $\overline{k}$ comme étant nulle ou supérieure à $2\,\mathsf{g}+1$ (en fait $> \mathsf{g}+1$ et $\neq 2\,\mathsf{g}+1$). D'après [Ser68, Cor 1.11], on trouve alors $\mathbf{R}_V = I_V = \mathbf{M}_V$ dans ce cas. On remarque que [Sek85] construit des exemples de familles (hyperelliptiques en caractéristique 2 et non hyperelliptiques en caractéristique 3) pour lesquelles $I_V \neq \mathbf{R}_V$ (Sekiguchi et Koizumi considèrent I_V comme la définition du corps de modules). Lercier et Basson (article en cours) précisent de résultat dans le cas du genre 3 hyperelliptique en caractéristique 2 en montrant que la courbe générique est définie sur une extension de degré 2 purement inséparable de M_V.

Si $p \neq 2$, les résultats de reconstruction obtenus au chapitre 6, permettent de prouver la proposition suivante :

Proposition 11. *Si $\mathcal{C}/k$ est une courbe de genre 2 sur un corps de caractéristique $\neq 2$, alors $I_\mathcal{C} = \mathbf{R}_\mathcal{C}$.*

Démonstration. On remarque que $\mathbf{R}_\mathcal{C}$ correspond au corps $K(g_1, g_2, g_3)$ engendré par les g_2-invariants absolus de $\mathcal{C}$ (voir définition 23 (p. 57)) au dessus du corps premier K. De plus, d'après les résultats de reconstruction du chapitre 6, il existe un modèle $\mathcal{C}$ sur une extension $F/\mathbf{R}_\mathcal{C}$ au plus quadratique. Donc $I_\mathcal{C} \subset F$ par définition et comme $I_\mathcal{C}/\mathbf{R}_\mathcal{C}$ est purement inséparable, $I_\mathcal{C} = \mathbf{R}_\mathcal{C}$. □

Remarque 9. *Il est également difficile de comparer $\mathbf{R}_\mathcal{C}$ et $\mathbf{M}_\mathcal{C}$ en général. En effet, on considère la courbe $\mathcal{C} : y^2 = x^5 - t^{10}x^2 + 4t^{15}$ sur $\mathbb{F}_5(t)$. Le corps $\mathbf{R}_\mathcal{C} = \mathbb{F}_5(g_1, g_2, g_3) = \mathbb{F}_5(t^5)$ et $\mathcal{C}$ est en fait définie sur $\mathbb{F}_5(t^5)$ donc $I_\mathcal{C} = \mathbf{R}_\mathcal{C}$. Cependant, il n'existe pas d'automorphisme de $\overline{\mathbb{F}_5(t)}$ permettant de distinguer $\mathbb{F}_5(t^5)$ et $\mathbb{F}_5(t)$ puisqu'il s'agit d'une extension purement inséparable. Par conséquent, $\mathbf{R}_\mathcal{C} \subsetneq \mathbf{M}_\mathcal{C}$.*

Savoir quand le corps de modules est également un corps de définition est une question profonde. Lorsque $\overline{k}$ est la clôture d'un corps fini (cf [Hug07, Cor. 2.11 p.251]) ou lorsque $\mathcal{C}$ n'a pas d'automorphisme (voir [DE99, Cor. 4.3 p.49]) alors $\mathbf{M}_\mathcal{C}$ est toujours un corps de définition. La plupart des autres résultats découlent de l'argument suivant dû à [DE99].

Supposons que $\overline{k}$ est une extension galoisienne de $\mathbf{M}_\mathcal{C}$. Par définition du corps de modules, pour tout $\sigma \in \mathrm{Gal}_{\overline{k}/\mathbf{M}_\mathcal{C}}$, il existe un $\overline{k}$-isomorphisme $F_\sigma : \mathcal{C} \to \mathcal{C}^\sigma$. On considère la courbe $B = \mathcal{C}/\operatorname{Aut}(\mathcal{C})$. L'isomorphisme F_σ induit un isomorphisme $f_\sigma : B \to \mathcal{C}^\sigma/\operatorname{Aut}(\mathcal{C}^\sigma) =: B^\sigma$ et le diagramme suivant est commutatif.

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{F_\sigma} & \mathcal{C}^\sigma \\ \downarrow & & \downarrow \\ B_\alpha & \xrightarrow{f_\sigma} & B^\sigma \end{array}$$

Comme dans la preuve du [Wei56, Thm. 1 p.510-511], les relations de cocycles de Weil impliquent que la courbe B admette un modèle $\mathcal{B}$ sur $\mathbf{M}_{\mathcal{C}}$ et un $\overline{k}$-isomorphisme $\varphi : B \to \mathcal{B}$ tel que pour tout $\sigma \in \Gamma$, $f_\sigma = (\varphi^{-1})^\sigma \circ \varphi$.

Théorème 3 ([DE99, Cor. 4.3(c) p.49] et [Hug07, Cor. 2.12 p.251])**.** *Si $\mathcal{B}(\mathbf{M}_{\mathcal{C}}) \neq \emptyset$, alors $\mathbf{M}_{\mathcal{C}}$ est un corps de définition de $\mathcal{C}$.*

3.2 De nouvelles notions de famille pour l'espace de modules des courbes

Afin de manipuler les espaces de modules, et en l'absence de "bons invariants", il est utile de représenter les strates (par exemple sous l'action des groupes d'automorphismes) par des familles qui cernent au mieux le lieu en question. Si S est une strate de $\mathcal{M}_{\mathsf{g}}(k)$, alors S est un espace de modules fin (et donc admet une famille universelle [New78, p.25]) si et seulement si le groupe d'automorphismes est trivial [AO00, Sec.14]. Dans ce cas, on a donc théoriquement une très bonne description de la strate S. En pratique, il n'est pas aisé d'obtenir celle-ci et de toute façon dans le cas de groupes d'automorphismes non triviaux, il faut trouver des remplaçants adéquats pour cette notion qui gardent des propriétés suffisamment fortes pour paramétriser de manière effective l'espace de modules. La plus intéressante est la notion de famille *représentative* qui coïncident avec la famille universelle usuelle sur la strate triviale.

Définition 17. *Soient $S \subset \mathcal{M}_{\mathsf{g}}(k)$ une sous-variété de $\mathcal{M}_{\mathsf{g}}(k)$ définie sur k et $\mathcal{F} \to \mathcal{S}$ une famille de courbes telle que les fibres géométriques correspondent au points de la sous-variété S. On note $f_{\mathcal{F}} : \mathcal{S} \to \mathcal{S}$ le morphisme associé. On définit les notions de familles suivantes :*

1. *La famille $\mathcal{F} \to \mathcal{S}$ est* géométriquement surjective *(pour S) si l'application $f_{\mathcal{F}}$ est surjective sur les K-points pour toute extension algébriquement close K de k.*
2. *La famille $\mathcal{F} \to \mathcal{S}$ est* arithmétiquement surjective *(pour S) si l'application $f_{\mathcal{F}}$ est surjective sur les k'-points pour toute extension finie k' de k.*
3. *La famille $\mathcal{F} \to \mathcal{S}$ est* quasi-finie *(pour S) si elle est géométriquement surjective et $f_{\mathcal{F}}$ est quasi-finie.*
4. *La famille $\mathcal{F} \to \mathcal{S}$ est* représentative *(pour S) si l'application $f_{\mathcal{F}}$ est bijective sur les K-points pour toute extension algébriquement close K de k.*

Le concept de famille représentative est relié à la question de savoir si le corps de modules $M_{\mathcal{C}}$ de la courbe $\mathcal{C}$ est un corps de définition.

Proposition 12. *Soit S est une sous-variété de $\mathcal{M}_{\mathsf{g}}(k)$ définie sur k qui admet une famille représentative $\mathcal{F} \to \mathcal{S}$. Si $\mathcal{C}$ est une courbe définie sur une extension algébriquement close K de k telle que le point $[\mathcal{C}]$ de $\mathcal{M}_{\mathsf{g}}(k)$ appartienne à S alors $\mathcal{C}$ descend sur son corps de modules $M_{\mathcal{C}}$. Si k est parfait et $K = \overline{k}$, alors $\mathcal{C}$ correspond à un élément de $\mathcal{S}(M_{\mathcal{C}})$.*

3.3 Les familles représentatives dans le cas des quartiques planes lisses

3.3.1 Groupes d'automorphismes

Théorème 4. *Soit K un corps algébriquement clos dont la caractéristique p vérifie $p = 0$ ou $p \geq 5$ et soit $\mathcal{C}$ une courbe de genre 3 non hyperelliptique définie sur K. Les groupes d'automorphismes possibles de $\mathcal{C}$ ainsi que des familles géométriquement surjectives pour les strates correspondantes sont les suivants :*

1. *$\{1\}$, avec la famille $q_4(x, y, z) = 0$ où q_4 est un polynôme homogène de degré 4 ;*

2. $\mathbf{C}_2$, *avec la famille* $x^4+x^2q_2(y,z)+q_4(y,z)=0$, *où* q_2 *et* q_4 *sont des polynômes homogènes de degré* 2 *et* 4 ;

3. $\mathbf{D}_4$, *avec la famille* $x^4+y^4+z^4+rx^2y^2+sx^2z^2+ty^2z^2=0$;

4. $\mathbf{C}_3$, *avec la famille* $x^3z+y(y-z)(y-rz)(y-sz)=0$;
5. $\mathbf{D}_8$, *avec la famille* $x^4+y^4+z^4+rx^2yz+sy^2z^2=0$;
6. $\mathcal{S}_3$, *avec la famille* $x^3z+y^3z+x^2y^2+axyz^2+bz^4=0$;

7. $\mathbf{C}_6$, *avec la famille* $x^3z+y^4+ry^2z^2+z^4=0$;
8. $\mathbf{G}_{16}$, *avec la famille* $x^4+y^4+z^4+rx^2z^2=0$;
9. $\mathcal{S}_4$, *avec la famille* $x^4+y^4+z^4+r(x^2y^2+x^2z^2+y^2z^2)=0$;

10. $\mathbf{C}_9$, *représenté par la quartique* $x^3y+y^3z+z^4=0$;
11. $\mathbf{G}_{48}$, *représenté par la quartique* $x^4+(x^3-z^3)z=0$;
12. $\mathbf{G}_{96}$, *représenté par la quartique de Fermat* $x^4+y^4+z^4=0$;
13. *(si* $p\neq 7$*)* $\mathbf{G}_{168}$, *représenté par la quartique de Klein* $x^3y+y^3z+z^3x=0$.

On va préciser les générateurs et les normalisateurs des groupes donnés dans ce théorème. Dans cette logique, on fixe d'abord quelques notations puis on utilise [Hug05, lem. 2.3.8].

On considère :

— $\mathrm{GL}_2(K)$ comme un sous-groupe de $\mathrm{PGL}_3(K)$ via l'application :

$$A \to \begin{pmatrix} 1 & 0 \\ 0 & A \end{pmatrix}.$$

— $D(K)$ est le sous-groupe des matrices diagonales dans $\mathrm{PGL}_2(K)$.
— $T(K)$ est le sous-groupe de $D(K)$ des matrices qui ont une valeur différente de 1 sur la diagonale seulement à la première ligne.
— $\widetilde{\mathcal{S}}_3$ est la représentation de $\mathcal{S}_3$ dans $\mathrm{GL}_3(K)$ par l'action de permutation induite sur les coordonnées.
— $\widetilde{\mathcal{S}}_4$ est le relèvement de degré 2 de $\mathcal{S}_4$ sur $\mathrm{GL}_3(K)$ généré par les matrices suivantes :

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_8 & 0 \\ 0 & 0 & \zeta_8 \end{pmatrix}, \ \frac{-1}{i+1}\begin{pmatrix} -(i+1) & 0 & 0 \\ 0 & i & -i \\ 0 & 1 & 1 \end{pmatrix}.$$

Fort de toutes ces notations, on peut énoncer le théorème suivant :

Théorème 5. *Les générateurs des groupes d'automorphismes* G *du théorème 4 (p. 37) ainsi que leur normalisateur* N *dans* $\mathrm{PGL}_3(K)$ *sont les suivants :*

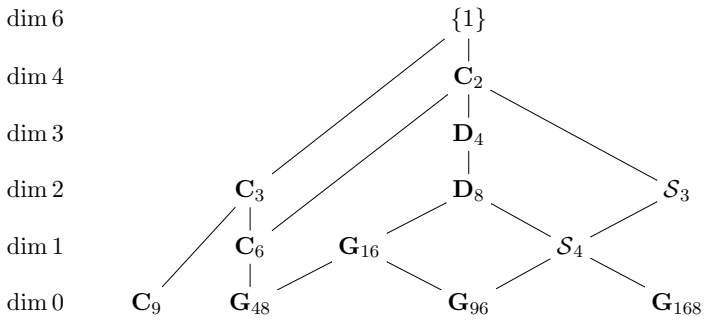
1. $\{1\}$ *est engendré par l'identité,* $N=\mathrm{PGL}_3(K)$.
2. $\mathbf{C}_2 =< \alpha >$ *où* $\alpha(x,y,z)=(-x,y,z)$, $N=\mathrm{GL}_2(K)$.
3. $\mathbf{D}_4 =< \alpha,\beta >$ *où* $\alpha(x,y,z)=(-x,y,z)$ *et* $\beta(x,y,z)=(x,-y,z)$, $N=D(K)\widetilde{\mathcal{S}}_3$.
4. $\mathbf{C}_3 =< \alpha >$ *où* $\alpha(x,y,z)=(\zeta_3 x,y,z)$, $N=\mathrm{GL}_2(K)$.
5. $\mathbf{D}_8 =< \alpha,\beta >$ *où* $\alpha(x,y,z)=(x,\zeta_4 y,-\zeta_4 z)$ *et* $\beta(x,y,z)=(x,z,y)$, $N=T(K)\widetilde{\mathcal{S}}_4$.
6. $\mathcal{S}_3 =< \alpha,\beta >$ *où* $\alpha(x,y,z)=(x,\zeta_3 y,\zeta_3^{-1}z)$ *et* $\beta(x,y,z)=(x,z,y)$, $N=T(K)\widetilde{\mathcal{S}}_3$.
7. $\mathbf{C}_6 =< \alpha >$ *où* $\alpha(x,y,z)=(\zeta_3 x,-y,z)$, $N=D(K)$.
8. $\mathbf{G}_{16} =< \alpha,\beta,\gamma >$ *où* $\alpha(x,y,z)=(\zeta_4 x,y,z)$, $\beta(x,y,z)=(x,-y,z)$ *et* $\gamma(x,y,z)=(x,z,y)$, $N=T(K)\widetilde{\mathcal{S}}_4$.

9. $\mathcal{S}_4 =< \alpha, \beta, \gamma >$ *où* $\alpha(x,y,z) = (x,-y,-z)$, $\beta(x,y,z) = (y,z,x)$ *et* $\gamma(x,y,z) = (y,x,z)$, $N = G$.
10. $\mathbf{C}_9 =< \alpha >$ *où* $\alpha(x,y,z) = (\zeta_9 x, \zeta_9^3 y, \zeta_9^{-3} z)$, $N = D(K)$.
11. $\mathbf{G}_{48} =< \alpha, \beta, \gamma >$ *où* $\alpha(x,y,z) = (x,-\zeta_4 y,-\zeta_4 z)$, $\beta(x,y,z) = (x,\zeta_3 y,z)$ *et* $\gamma(x,y,z) = (x, \frac{y+2z}{\sqrt{3}}, \frac{y-z}{\sqrt{3}})$, N *est* $\mathrm{PGL}_3(K)$*-conjugué à* $T(K)\widetilde{\mathcal{S}}_4$.
12. $\mathbf{G}_{96} =< \alpha, \beta, \gamma, \delta >$ *où* $\alpha(x,y,z) = (\zeta_4 x, y, z)$, $\beta(x,y,z) = (x,\zeta_4 y,z)$, $\gamma(x,y,z) = (y,z,x)$ *et* $\delta(x,y,z) = (y,x,z)$, $N = G$.
13. *(si* $p \neq 7$*)* $\mathbf{G}_{168} =< \alpha, \beta, \gamma >$ *où* $\alpha(x,y,z) = (\zeta_7 x, \zeta_7^2 y, \zeta_7^4 z)$, $\beta(x,y,z) = (y,z,x)$ *et*

$$\begin{aligned}\gamma(x,y,z) = ((&(\zeta_7 - \zeta_7^6)x + (\zeta_7^2 - \zeta_7^5)y + (\zeta_7^4 - \zeta_7^3)z,\\ &(\zeta_7^2 - \zeta_7^5)x + (\zeta_7^4 - \zeta_7^3)y + (\zeta_7 - \zeta_7^6)z,\\ &(\zeta_7^4 - \zeta_7^3)x + (\zeta_7 - \zeta_7^6)y + (\zeta_7^2 - \zeta_7^5)z),\end{aligned}$$

$N = G$.

Grâce à ce théorème, on obtient les inclusions suivantes entre les strates :



Remarque 10. *Comme promis dans le paragraphe 3.1.3, on va indiquer deux rigidifications différentes d'une action d'un groupe fini sur les quartiques planes. On considère le groupe* $\mathbf{C}_3$*. À conjugaison près, ce groupe peu être plongé dans* $\mathrm{PGL}_3(\overline{k})$ *de deux façons différentes : comme une matrice diagonnale avec les entrées proportionnelles à* $(\zeta_3, 1, 1)$ *ou* $(\zeta_3^2, \zeta_3, 1)$*. Cela donne deux rigidifications au sens de Lønsted.*

Cependant, les quartiques planes lisses admettant la seconde rigidification ont toujours une autre involution, donc le groupe d'automorphismes total contient $\mathcal{S}_3$*. C'est cet heureux phénomène qui rend possible une stratification naïve par les groupes d'automorphismes pour les quartiques planes lisses.*

3.3.2 Familles représentatives

Dans ce paragraphe, on explique comment appliquer la descente de Galois aux extensions de corps de fonction. Cela permet de déterminer les familles représentatives pour les strates du théorème 4 (p. 37) avec $|G| > 2$. La proposition 12 (p. 37) montre que l'obstruction à la descente est toujours triviale pour ces strates. Les constructions du théorème 6 (p. 40) conduisent à des familles qui paramétrisent les strates plus efficacement. Considérons le cas $\mathbf{D}_4$. La famille F géométriquement surjective du théorème 4 (p. 37) contient jusqu'à 24 près-images pour l'application $f_{\mathcal{F}}$ et pour un point k-rationnel de $\mathcal{M}_3(k)$, en général, aucune de ces courbes n'est définie sur k. Au contraire, pour les familles ci-dessous, d'après la proposition 12 (p. 37), l'application $f_{\mathcal{F}}$ est bijective et la courbe correspondant à un point k-rationnel de $\mathcal{M}_3(k)$ est défini sur k. Comme dans le théorème 4 (p. 37), on ne spécifie pas les conditions sur les paramètres qui évitent les dégénérescences (i.e singularités ou groupes d'automorphismes plus gros). Cependant, ces dégénérescences ont été prises en compte dans la stratégie d'énumération de [LRRS14].

Théorème 6. *Soit k un corps de caractéristique p satisfaisant $p = 0$ ou $p \geq 7$. Les familles représentatives pour les strates de quartiques planes lisses avec $|G| > 2$ sont les suivantes :*

1. $G \cong \mathbf{D}_4$:

$$\begin{aligned}&(a+3)x^4 + (4a^2 - 8b + 4a)x^3y + (12c + 4b)x^3z + (6a^3 - 18ab + 18c + 2a^2)x^2y^2\\ &+ (12ac + 4ab)x^2yz + (6bc + 2b^2)x^2z^2 + (4a^4 - 16a^2b + 8b^2 + 16ac + 2ab - 6c)xy^3\\ &+ (12a^2c - 24bc + 2a^2b - 4b^2 + 6ac)xy^2z + (36c^2 + 2ab^2 - 4a^2c + 6bc)xyz^2\\ &+ (4b^2c - 8ac^2 + 2abc - 6c^2)xz^3 + (a^5 - 5a^3b + 5ab^2 + 5a^2c - 5bc + b^2 - 2ac)y^4\\ &+ (4a^3c - 12abc + 12c^2 + 4a^2c - 8bc)y^3z + (6ac^2 + a^2b^2 - 2b^3 - 2a^3c + 4abc + 9c^2)y^2z^2\\ &+ (4bc^2 + 4b^2c - 8ac^2)yz^3 + (b^3c - 3abc^2 + 3c^3 + a^2c^2 - 2bc^2)z^4 = 0\end{aligned}$$

   avec

$$\begin{aligned}&x^4 + 2x^2y^2 + 2ax^2yz + (a^2 - 2b)x^2z^2 + ay^4 + 4(a^2 - 2b)y^3z\\ &+ 6(a^3 - 3ab)y^2z^2 + 4(a^4 - 4a^2b + 2b^2)yz^3 + (a^5 - 5a^3b + 5ab^2)z^4 = 0;\end{aligned}$$

2. $G \cong \mathbf{C}_3$: $x^3z + y^4 + ay^2z^2 + ayz^3 + bz^4 = 0$ *avec* $x^3z + y^4 + ayz^3 + az^4 = 0$;
3. $G \cong \mathbf{D}_8$: $ax^4 + y^4 + z^4 + ax^2yz + by^2z^2 = 0$;
4. $G \cong \mathcal{S}_3$: $x^3z + y^3z + x^2y^2 + axyz^2 + bz^4 = 0$;

5. $G \cong \mathbf{C}_6$: $x^3z + ay^4 + ay^2z^2 + z^4 = 0$;
6. $G \cong \mathbf{G}_{16}$: $x^4 + (y^3 + ayz^2 + az^3)z = 0$;
7. $G \cong \mathcal{S}_4$: $x^4 + y^4 + z^4 + a(x^2y^2 + x^2z^2 + y^2z^2) = 0$;

8. $G \cong \mathbf{C}_9$: $x^3y + y^3z + z^4 = 0$;
9. $G \cong \mathbf{G}_{48}$: $x^4 + (y^3 - z^3)z = 0$;
10. $G \cong \mathbf{G}_{96}$: $x^4 + y^4 + z^4 = 0$;
11. *(si $p \neq 7$)* $G \cong \mathbf{G}_{168}$: $x^3y + y^3z + z^3x = 0$;

Soit K une extension algébriquement close de k. Le point clef utilisé dans la preuve suivante est que les courbes des familles du théorème 4 (p. 37) ont toutes le même groupe d'automorphismes G *plongé* comme sous-groupe de $\mathrm{PGL}_3(K)$. À part pour le cas des strates de dimension 0, qui est une simple vérification, on procède de la façon suivante :

1. Le point clef cité précédemment implique que chaque isomorphisme entre deux courbes de la famille est nécessairement induit par un élément du normalisateur N de G dans $\mathrm{PGL}_3(K)$. On considère alors l'action de ce groupe sur les familles du théorème 4 (p. 37).
2. On détermine le sous-groupe N' de N qui envoie la famille sur elle-même. L'action de N' se factorise en une action fidèle de $Q = N'/G$. Par des calculs explicites, il s'avère que Q est fini pour les familles du théorème 4 (p. 37) lorsque $|G| > 2$. Cela montre en particulier que ces familles sont déjà quasi-finies sur ces strates.
3. On peut alors prendre le quotient par l'action finie de Q qui se fait au niveau des corps de fonctions sur K, en utilisant la descente de Galois. Par construction, la famille résultante est représentative.

Démonstration. **Le cas $G \cong \mathbf{D}_4$.** La famille donnée par le théorème 4 (p. 37) est $x^4 + y^4 + z^4 + rx^2y^2 + sy^2z^2 + tz^2x^2 = 0$ et $N = D(K)\widetilde{\mathcal{S}}_3$. L'action du groupe $\widetilde{\mathcal{S}}_3$ induit une permutation sur (r, s, t). L'action d'une matrice diagonale de coefficients λ, μ et 1 donne la courbe $\lambda^4x^4 + \mu^4y^4 + z^4 + \lambda^2\mu^2rx^2y^2 + \mu^2sy^2z^2 + \lambda^2tz^2x^2 = 0$. Si $\lambda^4 = \mu^4 = 1$, on obtient une courbe qui est encore dans la famille. Dans ce cas, les nouvelles valeurs des paramètres r, s et t sont $\mu^2\lambda^2r = \pm r$, $\mu^2s = \pm s$ et

$\lambda^2 t = \pm t$. Cette action supplémentaire est un gênante et on va chercher à l'éliminer en modifiant un peu la famille. On cherche pour cela à "déplacer" les paramètres vers x^4, y^4 et z^4. Dans cette logique, on sépare l'étude selon l'annulation ou non des paramètres. En premier lieu, on remarque que si deux paramètres sont nuls en même temps alors le groupe d'automorphismes est plus large. Par exemple, si s et t sont nuls, alors G contient l'automorphisme $(x, y, z) \to (x, y, \zeta_4 z)$ d'ordre 4. Ensuite, quitte à permuter les coordonnées, on peut supposer que $s \neq 0$ et $t \neq 0$. On se ramène alors aux cas $t = 0$ ou non.

Si $r = 0$, grâce au changement de variables $(x, y, z) \to (\frac{1}{\sqrt{t}}x, \frac{1}{\sqrt{s}}y, z)$ on obtient l'équation :

$$\frac{1}{t^2}x^4 + \frac{1}{s^2}y^4 + z^4 + x^2z^2 + y^2z^2 = 0.$$

Pour plus de simplicité, on la note $rx^4 + sy^4 + z^4 + x^2z^2 + y^2z^2 = 0$.

Si $r \neq 0$, le changement de variables $(x, y, z) \to (\sqrt{s}x, \sqrt{t}y, \sqrt{r}z)$, suivi de la division par rst, appliqué au modèle initial, fournit l'équation :

$$\frac{s}{rt}x^4 + \frac{t}{rs}y^4 + \frac{r}{st}z^4 + x^2y^2 + y^2z^2 + x^2z^2 = 0.$$

Pour plus de simplicité on la note $rx^4 + sy^4 + tz^4 + x^2y^2 + y^2z^2 + x^2z^2 = 0$.

On traite d'abord le cas générique $rx^4 + sy^4 + tz^4 + x^2y^2 + y^2z^2 + x^2z^2 = 0$. ç présent, $N' \cap D(K)$ est inclus dans G. Ainsi, $Q = N'/G$ est isomorphe à $\widetilde{\mathcal{S}}_3$. Le sous-corps des invariants par Q de $M = K(r, s, t)$ est $L = K(a, b, c)$ avec $a = r + s + t$, $b = rs + st + tr$ et $c = rst$. Le cocycle pour cette extension est obtenu par l'envoi d'une permutation de (r, s, t) sur sa matrice de permutation associée en (x, y, z). Un cobord est donné par l'isomorphisme $(x, y, z) \to (x + ry + r^2z, x + sy + s^2z, x + ty + t^2z)$. On note que ce morphisme est inversible dès que r, s et t sont distincts. Cela n'est pas gênant car sinon le groupe d'automorphismes serait plus gros. En transformant l'équation $rx^4 + sy^4 + tz^4 + x^2y^2 + y^2z^2 + x^2z^2 = 0$ par ce cobord, on obtient le résultat voulu.

À présent, on traite le cas $rx^4 + sy^4 + z^4 + x^2z^2 + y^2z^2 = 0$. Là encore $N' \cap D(K)$ est inclu dans G. Cependant, $\widetilde{\mathcal{S}}_3$ induit une permutation sur r et t. Ainsi, $Q = N'/G$ est isomorphe à $\mathcal{S}_2$. Le sous-corps des invariants par Q de $M = K(r, t)$ est $L = K(a, b)$ avec $a = r + t$ et $b = tr$. Le cocycle pour cette extension est donné par l'envoi d'une permutation de (r, t) sur sa matrice de permutation associée en (x, y, z) sur (x, z) laissant fixe y. Un cobord est donné par l'isomorphisme $(x, y, z) \to (y + rz, y + sz, x)$. On note que ce morphisme est inversible dès que r et s sont distincts. Cela n'est pas gênant car sinon le groupe d'automorphismes serait plus gros. En transformant l'équation $rx^4 + sy^4 + z^4 + x^2z^2 + y^2z^2 = 0$ par ce cobord, on obtient le résultat voulu.

Le cas $G \cong \mathbf{C}_3$. On procède de façon un peu différente. Le but est de construire une famille représentative directement à partir de l'action du groupe G sur les monômes de degré 4. Le groupe G est engendré par l'élément α qui peut se représenter comme une matrice diagonale. De cette façon, la famille qu'on va construire ne contiendra que des monômes stables par α, qui sont les suivants :

$$\left\{x^3y, x^3z, y^4, y^3z, y^2z^2, yz^3, z^4\right\}.$$

Remarquons que puisque G conserve la famille à une constante près, on aurait pu aussi considérer les familles constituées des monômes

$$\left\{x^4, xy^3, xy^2z, xyz^2, xz^3\right\} \text{ ou } \left\{x^2y^2, x^2yz, x^2z^2\right\}$$

mais ces deux dernières n'engendrent que des formes réductibles. Pour cette raison, on ne les prendra pas en compte. Ainsi, on part d'une équation :

$$kx^3y + lx^3z + my^4 + ry^3z + sy^2z^2 + tyz^3 + uz^4 = 0.$$

Les éléments k, l, m, r, s, t et u appartiennent à K. À présent, on effectue des changements de variables pour se ramener à une forme avec deux paramètres. Le couple (k, l) doit être différent de $(0, 0)$; sinon G contient l'élément $(x, y, z) \to (\zeta_n x, y, z)\ \forall\, n \in \mathbb{N}$. On effectue le changement de variables $(x, y, z) \to (x, y, ky + lz)$ pour éliminer le monôme x^3y et se ramener à l'équation :

$$x^3z + my^4 + ry^3z + sy^2z^2 + tyz^3 + uz^4 = 0.$$

On peut supposer $m \neq 0$ sinon, la courbe est réductible. Grâce au changement de variables $(x, y, z) \to (x, \frac{1}{\sqrt[4]{m}}y, z)$, on obtient l'équation :

$$x^3z + y^4 + ry^3z + sy^2z^2 + tyz^3 + uz^4 = 0.$$

Puisque la caractéristique du corps K est différente de 3, le changement de variables $(x, y, z) \to (x, y + \frac{r}{3}z, z)$ permet d'éliminer le monôme y^3z et d'avoir :

$$x^3z + y^4 + sy^2z^2 + tyz^3 + uz^4 = 0.$$

À ce stade là, on remarque que si $t = 0$, alors $\eta : (x, y, z) \to (\zeta_4 x, -y, \zeta_4 z) \in G$ et η est d'ordre 4. Cela permet d'affirmer que $t \neq 0$. On sépare l'étude selon que $s = 0$ ou non.

Si $s = 0$, alors $u \neq 0$. En effet, si $u = 0$, alors $\nu : (x, y, z) \to (\zeta_9 x, y, \zeta_9^6 z) \in G$ et ν est d'ordre 9. On effectue alors le changement de variables $(x, y, z) \to (x, \frac{1}{t}y, \frac{1}{u}z)$, on pose $a = \frac{1}{u^3}$ et on se ramène au modèle en dimension 1 voulu.

Si $s \neq 0$, alors on effectue le changement de variables $(x, y, z) \to (x, \frac{1}{s}y, \frac{1}{t}z)$ et on pose $a = \frac{1}{st^2}$ et $b = u$. On obtient le modèle en dimension 2 voulu.

À présent, on vérifie que la famille construite est représentative. Le normalisateur de G est $N = \mathrm{GL}_2(K)$. Soit $A = \begin{pmatrix} e & 0 & 0 \\ 0 & r & s \\ 0 & t & u \end{pmatrix} \in N$. Pour que A conserve la famille, elle doit envoyer le monôme x^3z sur lui-même. On en déduit que $t = 0$ et $e^3u = 1$. De même, $r^4 = 1$. Comme il n'y a pas de terme y^3z dans la famille, $3r^3s = 0$. On en déduit que $s = 0$. L'égalité des coefficients devant les monômes y^2z^2 et yz^3 (resp. yz^3 et z^4) entraine que $r = u$. Par conséquent, $A = \begin{pmatrix} \zeta_3 r & 0 & 0 \\ 0 & r & 0 \\ 0 & 0 & r \end{pmatrix}$. Ainsi, $N' \cong G$. Le groupe Q est donc trivial dans $\mathrm{PGL}_3(K)$ et par suite, la famille construite est représentative.

Le cas $G \cong \mathbf{D}_8$. La famille donnée par le théorème 4 (p. 37) est $x^4+y^4+z^4+rx^2yz+sy^2z^2 = 0$ et $N = T(K)\widetilde{\mathcal{S}}_4$. En faisant agir les générateurs de $\widetilde{\mathcal{S}}_4$ sur la famille précédente, on constate que ce groupe ne conserve pas la structure de la famille. On analyse alors l'action de $T(K)$. L'action d'une matrice diagonale de coefficients λ, 1 et 1 donne la courbe $\lambda^4x^4+y^4+z^4+\lambda^2rx^2yz+sy^2z^2 = 0$. Si $\lambda^4 = 1$, on obtient une courbe qui est encore dans la famille. Dans ce cas, la nouvelle valeur du paramètre r est $\lambda^2 r = \pm r$. La valeur de s est inchangée. Il y a une famille sur $L = K(r, s)$ telle que les fibres (r, s) et $(-r, s)$ soient isomorphes. On veut descendre cette famille sur $K(a, b)$ où $a = r^2$ génère le sous-corps invariant par l'automorphisme $\sigma : r \to -r$ et $b = s$. C'est un problème de descente galoisienne pour le groupe $Q \cong \mathbf{C}_2$ et l'extension de corps $M \supset L$, avec $M = K(r, s)$ et $L = K(a, b)$. La courbe $\mathcal{C}$ sur M qu'on veut descendre sur L est donnée par $x^4 + y^4 + z^4 + rx^2yz + sy^2z^2 = 0$. On considère la courbe $\mathcal{C}^\sigma : x^4 + y^4 + z^4 - rx^2yz + sy^2z^2 = 0$ conjugué par σ et l'isomorphisme $\varphi : \mathcal{C} \to \mathcal{C}^\sigma$ obtenu par $(x, y, z) \to (ix, y, z)$. On n'a pas $\varphi^\sigma\varphi^{-1} = id$. Pour trivialiser ce cocycle, on a besoin d'une extension plus grande que L.

On choisit $M' \supset M$ avec $M' = M(\rho)$ et $\rho^2 = r$. Soit τ un générateur d'ordre 4 du groupe de Galois de l'extension $M' \supset L$. De cette façon, τ se restreint à σ sur l'extension $M \supset L$. On obtient un cocycle de Weil sur l'extension $M' \supset L$ déterminé par l'isomorphisme $\mathcal{C} \to \mathcal{C}^\tau = \mathcal{C}^\sigma$ qui envoie (x, y, z) sur (ix, y, z). Le cobord correspondant est donné par $(x, y, z) \to (\rho x, y, z)$. On effectue la transformation et on obtient :

$$\rho^4x^4 + y^4 + z^4 + r\rho^2x^2yz + sy^2z^2 = ax^4 + y^4 + z^4 + ax^2yz + by^2z^2 = 0.$$

Le cas $G \cong \mathcal{S}_3$. La famille donnée par le théorème 4 (p. 37) est $x^3z+y^3z+x^2y^2+axyz^2+bz^4 = 0$ et $N = T(K)\widetilde{\mathcal{S}}_3$. Après l'action d'une matrice diagonale de coefficients λ, 1 et 1, on obtient la courbe $\lambda^3x^3z + y^3z + \lambda^2x^2y^2 + \lambda axyz^2 + bz^4 = 0$. Pour que ce soit un élément de la famille, il faut que $\lambda^3 = 1$ et $\lambda^2 = 1$, c'est à dire $\lambda = 1$. Ainsi, seul $\widetilde{\mathcal{S}}_3$ conserve la famille. Le groupe Q est donc trivial dans $\mathrm{PGL}_3(K)$. On n'a donc pas besoin d'adapter la vieille famille puisqu'elle est géométriquement surjective et ne contient pas de fibre géométriquement isomorphe.

Le cas $G \cong \mathbf{C}_6$. La famille donnée par le théorème 4 (p. 37) est $x^3z + y^4 + ry^2z^2 + z^4 = 0$ et $N = D(K)$. Après l'action d'une matrice diagonale de coefficients λ, μ et 1, on obtient la courbe $\lambda^3x^3z + \mu^4y^4 + \mu^2ry^2z^2 + z^4 = 0$. Si $\lambda^3 = 1$ $\mu^4 = 1$, on obtient une courbe qui est encore dans la famille. Dans ce cas là, la nouvelle valeur du paramètre r est $\mu^2r = \pm r$. Il y a une famille sur $L = K(r)$ telle que les fibres sur r et $-r$ sont isomorphe et on veut descendre cette famille sur $K(a)$, où $a = r^2$ génère le sous-corps invariant par l'automorphisme $\sigma : r \to -r$. C'est un problème de descente galoisienne pour le groupe $Q \cong \mathbf{C}_2$ et l'extension de corps $M \supset L$, avec $M = K(r)$ et $L = K(a)$. La courbe $\mathcal{C}$ sur M que l'on veut descendre sur L est donnée par $x^3z + y^4 + ry^2z^2 + z^4 = 0$. On considère la courbe $\mathcal{C}^\sigma : x^3z + y^4 - ry^2z^2 + z^4 = 0$ conjugué par σ et l'isomorphisme $\varphi : \mathcal{C} \to \mathcal{C}^\sigma$ donné par $(x, y, z) \to (x, iy, z)$. On n'a pas $\varphi^\sigma\varphi^{-1} = id$. Pour trivialiser ce cocycle, on a besoin d'une extension plus grande de L.

On prend $M' \supset M$ avec $M' = M(\rho)$ et $\rho^2 = r$. Soit τ un générateur d'ordre 4 du groupe de Galois de l'extension $M' \supset L$. De cette façon, τ se restreint à σ sur l'extension $M \supset L$. On obtient un cocycle de Weil sur l'extension $M' \supset L$ déterminé par l'isomorphisme $\mathcal{C} \to \mathcal{C}^\tau = \mathcal{C}^\sigma$ qui envoie (x, y, z) sur (x, iy, z). Le cobord correspondant est donné par $(x, y, z) \to (x, \rho y, z)$. On effectue la transformation et on obtient :

$$x^3z + \rho^4y^4 + r\rho^2y^2z^2 + z^4 = x^3z + ay^4 + ay^2z^2 + z^4 = 0.$$

Le cas $G \cong \mathbf{G}_{16}$. On procède de façon différente. Soit $r \in k$, on écrit $p_r(y, z) = y^4+z^4+rz^2y^2$. La famille donnée par le théorème 4 (p. 37) est $x^4 + p_r(y, z) = 0$. Un isomorphisme entre deux courbes $x^4 + p_r(y, z) = 0$ et $x^4 + p_{r'}(y, z) = 0$ est de la forme $(x, y, z) \to (\lambda x, \ell_1(y, z), \ell_2(y, z))$ avec ℓ_1 et ℓ_2 linéaires, vu la structure du normalisateur. Les courbes sont donc isomorphes si et seulement si les quartiques binaires p_r et $p_{r'}$ sont équivalentes à un scalaire près. On se ramène ainsi au cas des quartiques binaires. Lorsqu'elles n'ont pas de racine multiple, elles sont classées par leur j-invariant. Celui-ci est défini de la façon suivante : $j = 1728\frac{I^3}{I^3-27J^2}$ avec I et J des générateurs de l'algèbre des invariants des quartiques binaires (cf section 5.2.3). Le j-invariant de p_r est :

$$j = 16\frac{(r^2 + 12)^3}{(r - 2)^2(r + 2)^2}.$$

Ainsi, le j-invariant de p_r est bien défini lorsque $r \neq \pm 2$. Or, pour ces valeurs de r, la quartique $x^4 + p_r(y, z) = 0$ est singulière. Ainsi, on peut totalement classer p_r avec son j-invariant. Soit $a \in k$, on considère la quartique binaire $q_a = z(y^3 + ayz^2 + az^3)$. Lorsque $a \neq 0$ ou $a \neq -27/4$, cette quartique correspond à une courbe elliptique de j-invariant :

$$j = \frac{6912a}{4a + 27}.$$

On peut aussi exprimer a en fonction de j :

$$a = \frac{27j}{4(1728 - j)}.$$

Dans ce cas, à toutes valeurs de $j \neq 0$ ou $j \neq 1728$ correspond une quartique de la forme q_a. De plus, deux quartiques binaires sont équivalentes si et seulement si elles ont le même j-invariants. Ainsi, q_a et q'_a sont équivalentes si et seulement si $a = a'$. Pour finir, il reste à comprendre pourquoi la courbe elliptique construite à partir de p_r ne peut pas avoir de j-invariant égal à 0 ou 1728.

— Le cas $j = 1728$ correspond à $r = \pm 6$ ou $r = 0$. Si $r = 0$, la quartique plane $x^4+p_r(y,z) = x^4 + y^4 + z^4 = 0$ a pour groupe d'automorphismes $\mathbf{G}_{96}$. On sait que les quartiques binaires sont classifiées par leur j-invariants. De plus, les courbes $x^4 + p_r(y,z) = 0$ et $x^4 + p_{r'}(y,z) = 0$ sont isomorphes si et seulement si les quartiques binaires p_r et $p_{r'}$ sont équivalentes à un scalaire près. En conséquence, $r = \pm 6$ correspond aussi a une quartique plane lisse qui a pour groupe d'automorphismes $\mathbf{G}_{96}$.

— Le cas $j = 0$. La quartique binaire $(y^3 - z^3)z$ a ce j-invariant. Ainsi, puisque p_r est équivalente à $(y^3-z^3)z$ (à une transformation linéaire près), $x^4+p'_r y, z = 0$ est équivalente à $x^4 + (y^3 - z^3)z = 0$ qui a pour groupe d'automorphismes $\mathbf{G}_{48}$.

Dans les deux cas, on retombe sur des quartiques ayant plus de 16 automorphismes. On peut alors écarter ces deux cas.

Le cas $G \cong \mathcal{S}_4$. La famille $\mathcal{F}$ donnée par le théorème 4 (p. 37) est $x^4 + y^4 + z^4 + r(x^2y^2 + x^2z^2 + y^2z^2) = 0$ et $N = G$. Le groupe Q est donc trivial dans $\mathrm{PGL}_3(K)$, ainsi on n'a pas besoin d'adapter la famille originelle puisqu'elle est géométriquement surjective et que le morphisme $f_{\mathcal{F}}$ est injectif. □

D'après la proposition 12 (p. 37), s'il existe une famille représentative sur k pour une strate donnée, alors le corps de modules est un corps de définition pour toutes les courbes de la strate. Dans [AQ12], il est prouvé qu'il existe des $\mathbb{R}$-points dans la strate $\mathbf{C}_2$ pour lesquels la courbe correspondante ne peut pas être construite sur $\mathbb{R}$. En fait, on suspecte que cet argument puisse être adapté pour démontrer que les familles représentatives pour cette strate n'existe pas même si k est un corps fini. Pour pallier à cela, on construit dans [LRRS14] une famille arithmétiquement surjective sur les corps finis.

Proposition 13. *Soient $\mathcal{C}$ une quartique plane lisse, sur un corps fini k de caractéristique différente de 2, dont le groupe d'automorphismes est $\mathbf{C}_2$ et α un élément qui n'est pas un carré dans k. Alors $\mathcal{C}$ est k-isomorphe à une courbe de la liste suivante :*

$$x^4 + \epsilon x^2y^2 + ay^4 + \mu y^3z + by^2z^2 + cyz^3 + dz^4 = 0 \qquad \text{avec } \epsilon = 1, \alpha \text{ et } \mu = 0, 1$$
$$x^4 + x^2yz + ay^4 + \epsilon y^3z + by^2z^2 + cyz^3 + dz^4 = 0 \qquad \text{avec } \epsilon = 0, 1, \alpha$$
$$x^4 + x^2(y^2 - \alpha z^2) + ay^4 + by^3z + cy^2z^2 + dyz^3 + ez^4 = 0 \qquad .$$

Démonstration. Puisque le groupe d'automorphismes de $\mathcal{C}$ ne contient qu'une involution, elle est définie sur k. Ainsi, en choisissant une base dans laquelle cette involution est une matrice diagonale, on peut supposer qu'elle est donnée par $(x, y, z) \to (x, -y, z)$. Ce résultat montre que la famille $x^4 + x^2q_2(y,z) + q_4(y,z)$ du théorème 4 (p. 37) est arithmétiquement surjective. De plus, $q_2(y,z) \neq 0$; sinon, d'autres automorphismes sur K existeraient. Pour conclure, il faut distinguer les cas selon la factorisation de $q_2(y,z)$ sur k.

— Si q_2 a une racine multiple, alors on peut supposer que $q_2(y,z) = ry^2$ avec $r = 1$ ou $r = \alpha$. On pose $q_4(y,z) = ay^4 + by^3z + cy^2z^2 + dyz^3 + ez^4$. Si $b = 0$, alors la démonstration est terminée. Si $b \neq 0$, alors on le normalise à 1 en utilisant le changement de variable $z \to \frac{1}{b}z$.

— Si q_2 se factorise sur k, alors on peut supposer que $q_2(y,z) = yz$. Si $b = 0$, alors la démonstration est terminée. Si $b \neq 0$, alors on effectue le changement de variable $y \to \lambda y$ et $z \to \lambda z$. cela transforme by^3z en $b\lambda^2y^3z$. De fait, on peut supposer que $b = 1$ ou α.

— Si q_2 est irréductible sur k, alors on normalise $q_2(y,z)$ en $y^2 - \alpha z^2$. Cela donne la dernière famille à 5 paramètres.

□

On a vu au début de la section 3.2 qu'une famille universelle existe pour la strate qui a un groupe d'automorphismes trivial. De plus, comme $\mathcal{M}_3(k)$ est rationnel (cf [Kat96]), cette famille dépend de 6 paramètres rationnels. Cependant, aucune famille représentative (et donc universelle) ne semble avoir été décrite. On se contente du résultat ci-dessous dû à Bergström.

Proposition 14. *Soit $\mathcal{C}$ une quartique plane lisse sur k qui admet un point rationnel sur un corps de caractéristique $\neq 2$. $\mathcal{C}$ est isomorphe à une courbe qui a une des formes suivantes :*

$$\begin{aligned}
m_1x^4 + m_2x^3y + m_4x^2y^2 + m_6x^2z^2 + m_7xy^3 + xy^2z + m_{11}y^4 + m_{12}y^3z + y^2z^2 + yz^3 = 0,\\
m_1x^4 + m_2x^3y + m_4x^2y^2 + m_6x^2z^2 + xy^3 + m_{11}y^4 + m_{12}y^3z + y^2z^2 + yz^3 = 0,\\
m_1x^4 + m_2x^3y + m_4x^2y^2 + m_6x^2z^2 + m_{11}y^4 + m_{12}y^3z + y^2z^2 + yz^3 = 0,\\
m_1x^4 + m_2x^3y + m_4x^2y^2 + m_6x^2z^2 + xy^3 + xy^2z + m_{11}y^4 + m_{12}y^3z + yz^3 = 0,\\
m_1x^4 + m_2x^3y + m_4x^2y^2 + m_6x^2z^2 + xy^2z + m_{11}y^4 + m_{12}y^3z + yz^3 = 0,\\
x^4 + m_2x^3y + m_4x^2y^2 + m_6x^2z^2 + m_7xy^3 + m_{11}y^4 + m_{12}y^3z + yz^3 = 0,\\
m_2x^3y + m_4x^2y^2 + m_6x^2z^2 + m_7xy^3 + m_{11}y^4 + m_{12}y^3z + yz^3 = 0,\\
x^3z + m_4x^2y^2 + m_7xy^3 + m_8xy^2z + xyz^2 + m_{11}y^4 + m_{12}y^3z + m_{13}y^2z^2 + yz^3 = 0,\\
x^3z + m_4x^2y^2 + m_7xy^3 + m_8xy^2z + m_{11}y^4 + m_{12}y^3z + m_{13}y^2z^2 + yz^3 = 0,\\
x^4 + m_4x^2y^2 + m_5x^2yz + m_7xy^3 + m_8xy^2z + m_{11}y^4 + m_{12}y^3z + yz^3 = 0.
\end{aligned}$$

Les coefficients m_i appartiennent à k.

Démonstration. On note $m_1, \ldots, m_{15}$ les coefficients de la quartique $\mathcal{C}$ avec les monômes ordonnés de la façon suivante :

$$\{x^4, x^3y, x^3z, x^2y^2, x^2yz, x^2z^2, xy^3, xy^2z, xyz^2, xz^3, y^4, y^3z, y^2z^2, yz^3, z^4\} \tag{3.3.1}$$

La courbe $\mathcal{C}$ a un point rationnel P. Ainsi, quitte à translater le point P sur le point $(0:0:1)$ puis effectuer une rotation de centre $(0:0:1)$, on peut supposer que $P = (0:0:1)$ et que la tangente en P à la courbe est $y = 0$. Il en découle que $m_{15} = m_{10} = 0$ et $m_{14} \neq 0$. Quitte à diviser l'équation de $\mathcal{C}$ par m_{14}, on peut supposer que $m_{14} = 1$. La preuve se divise alors en plusieurs cas.

Cas 1 : $m_6 \neq 0$. On considère le terme $m_6x^2(z^2 + m_3/m_6xz)$. Ainsi, grâce au changement de variables $z \to z + m_3/(2m_6)x$, on peut supposer que $m_3 = 0$ sans modifier les conditions précédentes. À partir de cette nouvelle équation, on considère le terme $m_6x^2(z^2 + m_5/m_6yz)$. Ainsi, grâce au changement de variables $z \to z + m_5/(2m_6)y$, on peut supposer que $m_5 = 0$ sans modifier les conditions précédentes. À partir de cette dernière équation, on considère le terme $m_6z^2(x^2 + m_9/m_6yx)$. Ainsi, grâce au changement de variables $x \to x + m_9/(2m_6)y$, on peut supposer que $m_9 = 0$ sans modifier les conditions précédentes. On insiste sur le fait que l'ordre des changements de variables est crucial. Si on ne le respecte pas, on réintroduit des coefficients non nuls éliminés auparavant. À présent, l'étude s'organise en fonction de la nullité de m_8 ou m_{13}.

1. Si m_8 et m_{13} sont tout deux non nuls, alors on peut choisir $m_{13} = m_8 = 1$. Pour cela, on effectue le changement de variables $(x, y, z) \to (m_{13}x, m_8y, m_{13}m_8z)$. Les coefficients respectifs de xy^2z, y^2z^2 et yz^3 deviennent tous égaux à $m_{13}^3m_8^4$. On divise alors par $m_{13}^3m_8^4$ et on obtient le premier modèle.
2. Si $m_8 = 0$, $m_{13} \neq 0$ et $m_7 \neq 0$, alors on peut transformer m_{13} et m_7 pour obtenir $m_{13} = m_7 = 1$. Pour cela, on effectue le changement de variables $(x, y, z) \to (m_{13}x, m_7y, m_{13}m_7z)$. Les coefficients respectifs de xy^3, y^2z^2 et yz^3 deviennent tous égaux à $m_{13}^3m_7^4$. On divise alors par $m_{13}^3m_7^4$.
3. Si $m_8 = 0$, $m_{13} \neq 0$ et $m_7 = 0$, alors on peut poser $m_{13} = 1$. Pour cela, on effectue le changement de variables $z \to m_{13}z$ et on divise par m_{13}^3.
4. Si $m_8 \neq 0$, $m_{13} = 0$ et $m_7 \neq 0$, alors on peut poser $m_8 = m_7 = 1$. Pour cela, on effectue le changement de variables $(x, y, z) \to (m_7^2x, m_8^3y, m_8^2m_7z)$. Les coefficients respectifs de xy^2z, xy^3 et yz^3 deviennent tous égaux à $m_8^9m_7^3$. On divise alors par $m_8^9m_7^3$.

5. Si $m_8 \neq 0$ et $m_{13} = m_7 = 0$, alors on peut poser $m_8 = 1$. Pour cela, on effectue le changement de variables $(x, y, z) \to (x, m_8 y, m_8 z)$ et on divise par m_8^4.
6. Si $m_{13} = m_8 = 0$ et $m_1 \neq 0$, alors on peut poser $m_1 = 1$. Pour cela, on effectue le changement de variables $(x, y, z) \to (m_1 x, m_1^2 y, m_1 z)$ et on divise par m_1^5.
7. Si $m_{13} = m_8 = m_1 = 0$, alors on a le septième modèle de la proposition.

Cas 2 : $m_6 = 0$ et $m_3 \neq 0$. On considère le terme $m_3 x^3(z + m_1/m_3 x)$. Ainsi, grâce au changement de variables $z \to z + m_1/m_3 x$ on peut supposer que $m_1 = 0$ sans modifier les conditions précédentes. À partir de cette nouvelle équation, on considère le terme $m_3 x^3(z + m_2/m_3 y)$. Ainsi, grâce au changement de variables $z \to z+m_2/m_3 y$, on peut supposer que $m_2 = 0$ sans modifier les conditions précédentes. À partir de cette dernière équation, on considère le terme $m_3 x^2 z(x+m_5/m_3 y)$. Ainsi, grâce au changement de variables $x \to x+m_5/m_3 y$, on peut supposer que $m_5 = 0$ sans modifier les conditions précédentes. Là encore, l'ordre des transformations est très important.

8. Si $m_9 \neq 0$, on peut normaliser m_3 et m_9 à 1. Pour cela, on effectue le changement de variables $(x, y, z) \to (m_9^2 x, m_3 y, m_9^3 z)$. Les coefficients respectifs de $x^3 z$, xyz^2 et yz^3 deviennent tous égaux à $m_3 m_9^9$. On divise alors par $m_3 m_9^9$.
9. Si $m_9 = 0$, on normalise m_3 â 1. Pour cela, on effectue le changement de variables $(x, y, z) \to (x m_3, m_3^2 y, m_3 z)$ et on divise par m_3^5.

Cas 3 : $m_6 = 0$ et $m_3 = 0$.à

10. Si $m_1 \neq 0$, alors on peut le normaliser à 1. Pour cela, on effectue le changement de variables $(x, y, z) \to (x m_1, m_1^2 y, m_1 z)$ et on divise par m_1^5. On suppose alors que $m_9 = m_{13} = m_2 = 0$. Pour cela, on considère le terme $y(m_9 x z^2 + z^3)$. Ainsi, grâce au changement de variables $z \to z + \frac{m_9}{3} x$ on peut supposer que $m_9 = 0$ sans modifier les conditions précédentes. À partir de cette nouvelle équation, on considère le terme $y(z^3 + m_{13} y z^2)$. Ainsi, grâce au changement de variables $z \to z + \frac{m_{13}}{3} y$, on peut supposer que $m_{13} = 0$ sans modifier les conditions précédentes. À partir de cette nouvelle équation, on considère le terme $x^4 + m_2 x^3 y$. Ainsi, grâce au changement de variables $x \to x + \frac{m_2}{4} y$, on peut supposer que $m_2 = 0$ sans modifier les conditions précédentes.

La preuve est ainsi terminée car il reste le cas $m_1 = m_3 = m_6 = m_{10} = m_{15} = 0$ qui correspond à une quartique réductible. □

Bergström a aussi déterminé des modèles sans point rationnel, mais ils dépendent de 9 paramètres. En utilisant la borne de Hasse-Weil-Serre, on montre que lorsque k est un corps fini de cardinal > 29, les modèles de la proposition 14 (p. 44) constituent une famille arithmétiquement surjective de dimension 7, c'est à dire une de moins que la dimension de l'espace de modules.

Sur les corps fini k de caractéristique > 7 avec $|k| \leq 29$ il y a toujours des courbes sans point rationnel (cf [HLT05]). Les expériences de [LRRS14] ont montré qu'à l'exception d'un cas particulier, toutes ces courbes ont un groupe d'automorphismes non trivial. De cette façon, elles apparaissent déjà dans les familles non génèriques. La quartique plane lisse exceptionnelle sans point sur $\mathbb{F}_{11}$ est la suivante :

$$7x^4 + 3x^3y + 10x^3z + 10x^2y^2 + 10x^2yz + 6x^2z^2 + 7xy^2z \\ +xyz^2 + 4xz^3 + 9y^4 + 5y^3z + 8y^2z^2 + 9yz^3 + 9z^4 = 0.$$

Troisième partie

Espace de modules en genre 2

Chapitre 4

Introduction aux invariants et covariants.

4.1 Motivation

La théorie des invariants a des racines profondes. En 1773, J.L Lagrange a remarqué que le déterminant d'une forme quadratique binaire est invariant par les transformations linéaires du type $(x, y) \to (x + \lambda y, y)$. Aux alentours des années 1800, Carl F. Gauss s'est intéressé au problème général de l'invariance d'une forme binaire à coefficients entiers sous l'action du groupe spécial linéaire. En 1843, George Boole a posé les bases de la théorie des invariants. Dans le seconde partie du 19e siècle, la théorie des invariants s'est enrichie, notamment grâce à Sir Arthur Cayley, James J. Sylvester, Felix Klein. Elle connait un point culminant avec la preuve de Paul Gordan : celui-ci prouve, en exhibant un algorithme et sa preuve de terminaison, que l'algèbre des invariants des formes binaires (sous l'action de $\mathrm{SL}_2(\mathbb{C})$) est de type fini. Cependant, la recherche classique menée jusqu'à alors sur les invariants s'est arrêtée brutalement à la fin du 19e siècle. Cette rupture est due à la preuve de David Hilbert : il a démontré par raisonnement pur et non effectif que l'algèbre des invariants des formes n-aires (sous l'action de $\mathrm{SL}_n(\mathbb{C})$) est de type fini. Cette preuve n'a pas eu qu'un effet sur la théorie des invariants mais aussi un effet sur les mathématiques en général. En effet, elle est à l'origine des approches algébriques abstraites qui ont caractérisées une grande partie des mathématiques du XX^e siècle et qui ont complètement discrédité l'approche calculatoire, autrefois dominante. Cependant, à partir des années 1955, de nombreux travaux de mécanique des milieux continus ont abordés ces questions de calculs effectifs. Puis, vers les années 1970, des résultats complets ont été établis essentiellement par des procédés géométriques élémentaires. Dans les années 80, du fait de l'émergence de l'informatique, il y a eu un regain d'interêt pour les questions relatives aux calculs effectifs sur les algèbres d'invariants ou de covariants, en particulier la recherche d'un systèmes de générateurs pour celles-ci. Pour les formes binaires, qui sont notre principal intérêt ici, les approches ont essentiellement repris et amélioré une méthode plus tardive due à Hilbert (qui l'avait exhibée suite aux critiques envers ses raisonnements "théologiques"). Ainsi, Brouwer et Popoviciu ont obtenu un système de générateurs d'invariants de forme binaire de degré 9 et 10. Olive et Lercier ont réussi à calculer une famille génératrice pour les degrés 9 et 10. Ils s'appuient quant à eux sur une relecture de la méthode originelle de Gordan.
Il est à noter que tout ces travaux sont valables sur un corps de caractéristique 0. Le problème des petites caractéristiques (par rapport au degré de la forme) n'a, à notre connaissance, été abordé que récemment dans la thèse de Basson [Bas15]. Nous apporterons dans le chapitre 5 quelques nouveaux exemples et résultats à ce sujet.

4.2 Définitions

Soient k un corps algébriquement clos de caractéristique p ainsi que n et m deux entiers > 1. On note $V = k^m$ l'espace vectoriel avec la base $(x_1, \ldots, x_m)$, et $S^n(V)$ l'espace vectoriel, de dimension $n+1$, des formes homogènes m-aires de degré n en $(x_1, \ldots, x_m)$. Dans le cas $m = 2$, on parle de forme binaire et on note (x, z) la base de V. Lorsque $n = 0$, on pose $S^0(V) = k$. L'action d'un sous-groupe G de $\mathrm{GL}_m(k)$ sur V est donnée par :

$$M.(x_1, \ldots, x_m) = \Big(\sum_{j=1}^{m} a_{ij} x_j \Big)_{i=1\ldots m} = \Big(\sum_{j=1}^{m} a_{1j} x_j, \ldots, \sum_{j=1}^{m} a_{mj} x_j \Big),$$

pour tout $M = (a_{ij})_{ij} \in G$ et $(x_1, \ldots, x_m) \in V$. On en déduit une action de G sur $S^n(V)$:

$$(M.f)(x_1, \ldots, x_m) = f(M^{-1}.(x_1, \ldots, x_m)) \text{ pour tout } f \in S^n(V) \text{ et } M \in G.$$

On introduit les notions d'invariants et plus généralement de covariants d'une forme m-aire.

Définition 18. *Soient r et n deux entiers strictement positifs et G un sous-groupe de $\mathrm{GL}_m(k)$.*

- *Une fonction polynomiale homogène $q : S^n(V) \to S^r(V)$ de degré d est un* covariant *de degré d et d'ordre r s'il existe $\omega \in \mathbb{Z}$ tel que pour tout $M \in G$ et tout $f \in S^n(V)$, on a :*

$$q(M.f) = \det(M)^{-\omega} \cdot M.q(f).$$

  L'entier ω est appelé le poids *du covariant q.*
- *On appelle* invariant *(relatif) les covariants d'ordre* 0.
- *On appelle* invariant absolu *le quotient de deux invariants de même degré.*

Dans la suite, on identifiera un covariant (qui est ici une application) avec son image sur une forme f de coefficients génériques. Il s'agira donc d'un polynôme $q(f, (x_1, \ldots, x_n))$ en les coefficients des formes homogènes m-aires de degré n et en les x_i tel qu'il existe $\omega \in \mathbb{Z}$ pour lequel

$$q(M.f, M.(x_1, \ldots, x_n)) = \det(M)^{-\omega} \cdot q(f, (x_1, \ldots, x_n))$$

pour tout $M \in G$.

Exemple 7. *Pour tout sous-groupe G de $\mathrm{GL}_m(k)$:*

- *Si I est un invariant de f, alors pour tout $M \in G$, $I(M.f) = \det(M)^{\omega} I(f)$.*
- *$f \in S^n(V)$ est un covariant de degré 1 et d'ordre n.*
- *Si $m = 2$, alors le discriminant d'une forme binaire $f = \prod_{i=1}^{n} (\alpha_i x, \beta_i z)$ de degré n, en caractéristique $p \neq 2$, est un invariant de degré $2(n-1)$, défini par :*

$$\Delta(f) = \prod_{i<j} (\alpha_i \beta_j - \alpha_j \beta_i)^2.$$

On définit la notion de système générateur.

Définition 19. *Soient f une forme binaire et $\{q_1(f), \ldots, q_n(f)\}$ des covariants (resp. invariants) de f. On dit que $\{q_1(f), \ldots, q_n(f)\}$ est un* système générateur *de l'algèbre des covariants (resp. invariants) si on peut exprimer tout covariant q (resp. invariant) de f comme un polynôme en les $q_1(f), \ldots, q_n(f)$. Le système est* minimal *si on perd cette propriété en retirant un élément de la liste.*

Dans la littérature sur les formes binaires, l'action de $\mathrm{GL}_2(k)$ est souvent remplacée par l'action de $\mathrm{SL}_2(k)$. Nous allons voir ci-dessous que les notions de covariants sont identiques pour ces deux groupes. Tout d'abord, pour qu'un covariant de degré d et d'ordre r soit défini, $r - nd$ doit être pair (considérer l'action de la matrice $-I_2$). En lien avec notre problème de classification des courbes hyperelliptiques à isomorphisme près, on doit considérer l'action

de $\mathrm{GL}_2(k)$. Lorsque k est algébriquement clos, l'action de $\mathrm{PGL}_2(k)$ s'identifie avec l'action de $\mathrm{PSL}_2(k) = \mathrm{SL}_2(k)/\{Id, -Id\}$. En analysant l'action de $\mathrm{SL}_2(k)$, les déterminants valent 1. Ainsi, le poids des covariants n'est plus important. On considère alors l'algèbre des covariants, $\mathcal{C}_n$, (resp. des invariants, $\mathcal{I}_n$) pour les formes binaires de degré n sous l'action de $\mathrm{SL}_2(k)$. Nous avons le lemme suivant :

Lemme 3. *Les notions d'invariants et de covariants coincident pour ces deux groupes.*

Démonstration. Tout covariant sous l'action de $\mathrm{GL}_2(k)$ est un covariant pour celle de $\mathrm{SL}_2(k)$. Bien que moins évidente, la réciproque est vraie : si q est un covariant de degré d et d'ordre r sous l'action de $\mathrm{SL}_2(k)$, alors

$$q(\lambda I_2.f) = q(\lambda^{-n} f) \text{ pour une matrice scalaire } \lambda I_2.$$

D'autre part, q est un polynôme homogène de degré d en les coefficients de f d'où :

$$q(\lambda^{-n} f) = \lambda^{-nd} q(f).$$

Pour $M \in \mathrm{GL}_2(k)$, on a $M' = M/\sqrt{\det M} \in \mathrm{SL}_2(k)$. On en déduit que :

$$\begin{aligned} q(M.f) &= q\Big((\sqrt{\det M} I_2).(M'.f)\Big) = (\sqrt{\det M})^{-nd} q(M'.f) \\ &= (\sqrt{\det M})^{-nd} M'.q(f) = (\sqrt{\det M})^{-nd+r} (\sqrt{\det M})^{-r} M'.q(f). \end{aligned}$$

Enfin, puisque $M'.q(f)$ est un polynôme homogène de degré r, on obtient :

$$(\sqrt{\det M})^{-r} M'.q(f) = (\sqrt{\det M} I_2).(M'.q(f)) = (\sqrt{\det M} I_2.M').q(f) = M.q(f).$$

Au final, on a :

$$q(M.f) = (\det M)^{-\frac{nd-r}{2}} M.q(f).$$

Autrement dit, q est un covariant pour $\mathrm{GL}_2(k)$ de poids $(nd-r)/2$. □

4.3 Invariants et courbes hyperelliptiques

On considère une courbe $\mathcal{C}$ hyperelliptique, hyperelliptiquement définie sur k (k étant algébriquement clos, ceci n'est pas une restriction [1]), de genre $\mathsf{g} \geq 2$, d'équation affine $y^2 = f(x)$ où f est un polynôme séparable de degré $2\,\mathsf{g}+1$ ou $2\,\mathsf{g}+2$. En homogénéisant les coordonnées projectives pondérées de poids $(1, \mathsf{g}+1, 1)$, on obtient une équation $y^2 = f(x, z)$. Le polynôme f est vu comme un polynôme de degré $2\,\mathsf{g}+2$; on prend en compte une "racine à l'infini" lorsque $\deg(f) = 2\,\mathsf{g}+1$. Un isomorphisme entre $\mathcal{C}$ et $\mathcal{C}'$ est donné par un couple (M, e) [2] où $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$ et $e \in k^*$. On associe l'isomorphisme $(x, y, z) \to (ax + bz, ey, cx + dz)$ à un tel couple. La représentation d'un tel isomorphisme est unique à l'équivalence près $(M, e) \cong (\lambda M, \lambda^{\mathsf{g}+1} e)$ pour $\lambda \in k^*$. Comme k est algébriquement clos, on peut toujours supposer que $e = 1$. Ainsi, deux courbes hyperelliptiques sont isomorphes sur k si et seulement si leur polynôme sont $\mathrm{GL}_2(k)$-équivalents. De plus d'après un résultat de [MF82, p. 78], les polynômes hyperelliptiques f et f' de $\mathcal{C}$ et $\mathcal{C}'$ sont $\mathrm{GL}_2(k)$-équivalents si et seulement s'il existe $\lambda \in k$ tel que $I(f) = \lambda^d I(f')$, pour tout $I \in \mathcal{I}_{2\,\mathsf{g}+2}$ homogène de degré d. Ce constat motive la définition suivante :

Définition 20. *On appelle* invariant de la courbe $\mathcal{C}$ *d'équation* $y^2 = f(x, z)$, *les invariants de la forme binaire* f.

1. cf section 2.1.1
2. cf [LRS12, sec. Application to isomorphisms of hyperelliptic curves.]

Proposition 15. *Deux courbes hyperelliptiques $\mathcal{C}$ et $\mathcal{C}'$ sont isomorphe sur k si et seulement si elles ont les mêmes invariants absolus.*

Ceci n'est bien sûr plus vrai si k n'est pas algébriquement clos sinon, les algorithmes sur les tordues présentés plus haut n'auraient pas d'intérêt.

Démonstration de la proposition 15 (p. 52). Puisque $\mathcal{C}$ et $\mathcal{C}'$ sont définies sur k qui est algébriquement clos, elles sont hyperelliptiquement définies sur k. Supposons que $\mathcal{C}$ et $\mathcal{C}'$ soient isomorphe alors leur formes binaires associées f et f' sont équivalentes. On rappelle que f et f' sont des formes binaire de degré $2\,\mathtt{g}+2$. Ainsi, il existe une matrice $M \in \mathrm{GL}_2(k)$ et un scalaire $\lambda \in k$ tels que $f' = \lambda M.f$. Soit j un invariant absolu de des formes binaires de degré $2\,\mathtt{g}+2$. Alors il existe I et $J \in \mathcal{I}_{2\,\mathtt{g}+2}$ de même degrés d tels que $j = \frac{I}{J}$. Ainsi,

$$j(f') = j(\lambda M.f) = \frac{I(\lambda M.f)}{J(\lambda M.f)} = \frac{\lambda^{(2\,\mathtt{g}+2)d}\det(M)^{-(g+1)d} I(f)}{\lambda^{(2\,\mathtt{g}+2)d}\det(M)^{-(g+1)d} J(f)} = j(f).$$

Donc $\mathcal{C}$ et $\mathcal{C}'$ ont les mêmes invariants absolu.

Réciproquement soit $\{I_{d_1}, \ldots, I_{d_n}\}$ un système générateur de l'algèbre des invariants $\mathcal{I}_{2\,\mathtt{g}+2}$ où I_{d_i} sont de degrés d_i pour tout $i \in \{1, \ldots, n\}$. Soit $i \in \{1, \ldots, n\}$, on chercher à montrer qu'il existe $\lambda \in k$ tel que $I(f) = \lambda^{d_i} I_{d_i}(f')$. Soit D le discriminant de la forme binaire de degré $2\,\mathtt{g}+2$. On note d son degré. Puisque f et f' sont des polynômes hyperelliptiques, $D(f)$ (resp ; $D(f')$) est non nul. Pour tout $i \in \{1, \ldots, n\}$, $\frac{I_{d_i}(f)}{D(f)}$ (resp $\frac{I_{d_i}(f')}{D(f')}$) est un invariant absolu de f (resp. f'). Ainsi,

$$\frac{I_{d_i}(f)}{D(f)} = \frac{I_{d_i}(f')}{D(f')}.$$

On pose $\lambda = \sqrt[d]{\frac{D(f)}{D(f')}}$. Ainsi, on obtient $I_{d_i}(f) = \lambda^d I_{d_i}(f')$. □

Lorsque le discriminant D de degré d est un des éléments d'un système générateur minimal $\{I_{d_1}, \ldots, I_{d_n}\}$ alors

$$\{\frac{I_{d_1}^{d/\operatorname{pgcd}(d_1,d)}}{D^{d_1/\operatorname{pgcd}(d_1 d)}}, \ldots, \frac{I_{d_n}^{d/\operatorname{pgcd}(d_n,d)}}{D^{d_n/\operatorname{pgcd}(d_n,d)}}\}$$

est une liste d'invariants absolus pour toutes les courbes hyperelliptiques. C'est le cas en genre 2 (section 5.1.3). En genre 3, le discriminant ne fait plus partie d'un système générateur minimal et on travaille donc avec des invariants absolus en notation "projective". L'article [LR12, sec 1.4] présente un algorithme permettant de trouver un représentant canonique de la classe des invariants.

Remarque 11. *Lorsque $m = 3$, on parle de forme ternaire. L'algèbre des invariants n'est connue que pour les formes de degré 2,3 et 4. Nous n'utiliserons dans la suite que le résultat en degré 4. Un système de générateurs de l'algèbre des invariants est donné par les invariants de Dixmier-Ohno. Dixmier a d'abord calculé des invariants primaires (i.e. algébriquement indépendants) et Ohno a enrichi ce travail par un système générateur. Ces résultats ont été implémentés en* `magma` *par Kohel. À une forme ternaire f de degré 4, on associe naturellement une quartique plane $C : f = 0$ de $\mathbb{P}^2$. La caractérisation des isomorphismes (voir section 1.3) pour les courbes planes lisses de degré supérieur à 4 montre que deux quartiques planes lisses $C : f = 0$ et $C' : f' = 0$ sont isomorphes sur k si et seulement s'il existe $M \in \mathrm{GL}_3(\overline{k})$ tel que $M.f = f'$. Ceci est utilisé dans l'annexe C pour l'énumération des classes d'isomorphisme en genre 3.*

Chapitre 5

Calcul d'invariants et de covariants à partir de la courbe

à présent, on va présenter des méthodes de calcul explicite d'invariants. Dans ce but, on note k un corps algébriquement clos de caractéristique $p \neq 2$ et $\mathcal{C}$ une courbe hyperelliptique d'équation affine $y^2 = f(x)$.

5.1 Résultats classiques

5.1.1 Caractéristique nulle

En caractéristique nulle, l'algèbre des covariants $\mathcal{C}_n$ et celle des invariants $\mathcal{I}_n$ ont été étudiées dès la moitié du XIX^{me} siècle. Sous le nom de Überschiebung, Clebsch et Gordan ont introduit l'opération principale permettant de créer des nouveaux covariants. Dans cette étude, on appellera "transvectant" cet opérateur. Soient :

— i et j deux entiers distincts,
— (x_i, z_i) et (x_j, z_j) des bases de deux copies V_i et V_j de $V = k^2$,
— Ω_{ij} l'opérateur différentiel

$$\Omega_{ij} = \frac{\partial}{\partial x_i}\frac{\partial}{\partial z_j} - \frac{\partial}{\partial x_j}\frac{\partial}{\partial z_i}.$$

Cet opérateur est appelé l'opérateur différentiel de Cayley. Soient $r_i, r_j > 0$ des entiers, $f_i \in S^{r_i}(V) = S^{r_i}(V_i)$ et $f_j \in S^{r_j}(V) = S^{r_j}(V_j)$. On définit l'opérateur différentiel [1] suivant :

Définition 21. *Le* transvectant *d'indice h, noté $(,)_h$, est l'application $S^{r_i}(V_i) \times S^{r_j}(V_j) \to S^{r_i+r_j-2h}(V)$ définie par :*

$$(f_i, f_j)_h = \frac{(r_j-h)!(r_i-h)!}{r_i!r_j!}\Big(\Omega_{ij}^h\big(f_i(x_i,z_i).f_j(x_j,z_j)\big)\Big)_{(x_i,z_i)=(x_j,z_j)=(x,z)}.$$

Exemple 8. *Soit $f = a_2x^2 + a_1xz + a_0x^2$, on calcule le transvectant d'indice 2 de f avec elle-même :*

$$\begin{aligned}
(f,f)_2 &= \frac{1}{4}\Big((\partial_{x_i}f\partial_{z_j}f - \partial_{x_j}f\partial_{z_i}f)^2\Big)_{(x_i,z_i)=(x_j,z_j)=(x,z)} \\
&= \frac{1}{4}\Big(\partial^2_{x_i^2}f\partial^2_{z_j^2}f + \partial^2_{x_j^2}f\partial^2_{z_i^2}f - 2\partial^2_{x_iz_i}f\partial^2_{x_jz_j}f\Big)_{(x_i,z_i)=(x_j,z_j)=(x,z)} \\
&= \frac{1}{2}(\partial^2_{x^2}f\partial^2_{z^2}f - (\partial^2_{xz})^2) \\
&= -\frac{1}{2}(a_1^2 - 4a_0a_2).
\end{aligned}$$

1. où la composition est notée multiplicativement

On se rend compte que ce transvectant correspond au discriminant de la forme quadratique binaire f, à un scalaire près.

De façon générale, le transvectant permet d'engendrer un covariant à partir de 2 covariants initiaux, comme l'énonce la proposition suivante.

Proposition 16. *Le transvectant d'indice h de deux covariants de degré d_1, d_2 et d'ordre r_1, r_2 est un covariant de degré $d_1 + d_2$ et d'ordre $r_1 + r_2 - 2h$.*

Ce résultat se retrouve bien dans l'exemple précédent.

Réciproquement, il est remarquable que tout covariant d'une forme f s'obtienne par des calculs de transvectant successifs à partir de f, pour des ordres de transvection inférieurs au degré de la forme f. De cette observation, Gordan déduit son résultat de finitude en exibant des relations algébriques entre les transvectants.

Théorème 7. *[Gor68]. Les $\mathbb{C}$-algèbres $\mathcal{C}_n$ et $\mathcal{I}_n$ sont de type fini.*

à partir du covariant fondamental f, la méthode de Gordan consiste à itérer l'opération de transvection sur f, en caractéristique 0. Le but est alors de créer un système de générateurs pour les invariants et les covariants. Par cette approche, des familles finies de générateurs des algèbres $\mathcal{C}_n$ et $\mathcal{I}_n$ pour $n = 2, \ldots, 6$ et pour $\mathcal{I}_8$ ont été déterminées lors de la seconde moitié du XIX^{me} siècle. L'algèbre des covariants $\mathcal{C}_6$ est engendré par 21 covariants calculés par transvectants sucessifs (cf. [Cle72, p.296]) et 5 invariants A, B, C D et R. Ces derniers peuvent être calculer de la façon illustrée dans la figure 5.1 (p. 55).

Remarque 12. *Pour les degrés supérieurs, Shioda a effectué une description complète de l'algébre $\mathcal{I}_8$ en 1967. Suite aux travaux de Dixmier (1985), Lazard (1988) et Bedratyuk (2005), des générateurs fondamentaux de $\mathcal{I}_7$ ont été donnés. Les générateurs pour les degrés 9 et 10 ont été construits par Brouwer et Popoviciu en 2010. En ce qui concerne les algèbres de covariants des formes binaires de degré 9 et 10, Lercier et Olive ont fourni des familles génératrices minimales en 2014 en améliorant la méthode de Gordan.*

5.1.2 Caractéristique non nulle

Les résultats évoqués précédemment ont été obtenus pour des formes définies sur $\mathbb{C}$ et reposent essentiellement sur le caractère linéairement réductif du groupe algébrique $\mathrm{SL}_2(\mathbb{C})$. Bien que la situation soit plus délicate en caractéristique positive, certains résultats valables en toute caractéristique existent. En effet, un résultat de Geyer (1974) établit que l'algèbre $\mathcal{I}_n$ sur un corps de caractéristique p est essentiellement identique à celle sur $\mathbb{C}$ pour $p > n$. Il n'est pas très compliqué de retrouver $\mathcal{I}_4$ en caractéristique 3 (cf. [Bas15, sec. 2.10.2]). Igusa (1960) définit 5 invariants qui conviennent en toute caractéristique pour décrire l'algèbre $\mathcal{I}_6$. Il se base sur les invariants de Clebsch des sextiques binaires sur $\mathbb{C}$ connus depuis le XIX$^{\mathrm{e}}$ siècle. Dans sa thèse, Basson a déterminé un système générateur de séparants (voir définition 27 (p. 61)) pour $\mathcal{I}_8$ pour les caractéristiques $2, 3$ et 7 et en a conjecturé un pour $p = 5$. Le cas des covariants est un peu plus délicats. Par exemple, le cas de $\mathcal{C}_6$ en petite caractéristique est encore ouvert. En effet, nos calculs ont fait apparaître un covariant d'ordre 2 et de degré 1 en caractéristique 5, ainsi qu'un covariant d'ordre 4 et de degré 1 en caractéristique 3. Ils ne sont pas la réduction d'un covariant sur $\mathbb{C}$.

Remarque 13. *Le résultat de Geyer pour $p > n$ ne permet malheureusement pas d'affirmer qu'un système de générateurs valable en caractéristique 0 (engendré par la méthode de Gordan) le reste ne caractéristique p. Ainsi en degré 8, des arguments supplémentaires sont nécessaires dans [LR12] pour montrer que le système générateur de Shioda le reste en caractéristique > 7.*

Dans la section 5.2, on montrera que, dans le cas de $\mathcal{I}_6$, les résultats de Geyer sont encore valables en caractéristique 3 et 5 ce qui permet de retrouver les résultats d'Igusa pour $\mathcal{I}_6$. Nous

FIGURE 5.1 – Générateurs pour l'algèbre $\mathcal{C}_6$ en caractéristique 0

ordre / degré	0	2	4	6	8	10	12
1				f			
2	$A = (f,f)_6$		$i = (f,f)_4$		$H = (f,f)_2$		
3		$y_1 = (f,i)_4$		$p = (f,i)_2$	$(f,i)_1$		$T = (f,H)_1)_1$
4	$B = (i,i)_4$		$(f,y_1)_2$	$(f,y_1)_1$		$(H,i)_1$	
5		$y_2 = (i,y_1)_2$	$(i,y_1)_1$		$(H,y_1)_1$		
6	$C = (i,(i,i)_2)_4$			$(p,y_1)_1$ $((f,i)_1,y_1)_2$			
7		$y_3 = (i,y_2)_2$	$(f,y_1^2)_3$				
8		$y_4 = (y_1,y_2)_1$					
9			$((f,i)_1,y_1^2)_4$				
10	$D = (y_3,y_1)_2$	$y_5 = (y_3,y_1)_1$					
12		$y_6 = (y_2,y_3)_1$					
15	$R = ((f,i)_1,y_1^4)_8$						

avons également tenté d'appliquer la méthode de Geyer pour les covariants $\mathcal{C}_6$ mais les calculs restent prohibitifs. Limitant nos ambitions au cas du degré 4, nous avons alors obtenu des résultats nouveaux pour l'algèbre des covariants en caractéristique 3.

5.1.3 Le cas du genre 2

On va définir les invariants qui serviront dans le chapitre 6 pour la reconstruction de courbes à partir de leurs invariants. On va notamment définir les invariants d'Igusa ainsi que les invariants absolus de Cardonna Quer que nous appellerons les $\mathtt{g}_2$-invariants.

5.1.3.1 Les invariants d'Igusa

On définit un système générateur de $\mathcal{I}_6$ valable en toute caractéristique diffférente de 2. Les résultats sont présentés sans preuve car les démonstrations ont été développées dans l'article [Igu60]. Bien qu'on ne traite pas ce point, Igusa a aussi défini des invariants valables en caractéristique 2.

Soit f une forme sextique. On écrit f de la façon suivante : $f = u_0 \prod(x - x_i)$. Igusa ([Igu60, p.620]) définit les invariants de f comme des expressions symétriques en les racines suivantes :

$$\begin{aligned}
A' =& u_0^2 \sum (x_1 - x_2)^2 (x_3 - x_4)^2 (x_5 - x_6)^2 \\
B' =& u_0^4 \sum (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 (x_4 - x_5)^2 (x_4 - x_6)^2 (x_5 - x_6)^2 \\
C' =& u_0^6 \sum (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2 (x_4 - x_5)^2 (x_4 - x_6)^2 (x_5 - x_6)^2 (x_1 - x_4)^2 (x_2 - x_5)^2 (x_4 - x_6)^2 \\
D' =& u_{10} \prod_{i<j} (x_i - x_j)^2.
\end{aligned}$$

Les trois premières sommes sont telles que les expressions sont symétriques : la première somme a 15 facteurs, la seconde 10 et la troisième 60. Ces invariants peuvent être exprimés en fonction des coefficients de f grâce aux formules suivantes (cf. [Mes91, p. 319]) :

$$\begin{aligned}
A' =& -120A \\
B' =& -720A^2 + 6750B \\
C' =& \quad 8640A^3 - 108000AB + 202500C \\
D' =& -62208A^5 + 972000A^3B + 1620000A^2C - 3037500AB^2 - 6075000BC - 4556250D.
\end{aligned}$$

Les éléments A, B, C et D sont ceux de la figure 5.1 (p. 55) présentée précédemment. Enfin, des facteurs parasites, en petite caractéristique, sont éliminés en considèrant des nouveaux invariants de même degré obtenus par combinaisons linéaire. Ainsi, les invariants d'Igusa ([Igu60, p.621,622]) sont définis de la façon suivante :

Définition 22. *Soit $\mathcal{C}$ une courbe hyperelliptique de genre 2 d'équation $y^2 = f(x)$ Les* invariants d'Igusa *de $\mathcal{C}$ s'expriment de la façon suivante :*

$$\begin{aligned}
J_2(\mathcal{C}) =& 2^{-3} A' \\
J_4(\mathcal{C}) =& 2^{-5} \cdot 3^{-1} (4J_2^2 - B') \\
J_6(\mathcal{C}) =& 2^{-6} 3^{-2} (8J_2^3 - 160 J_2 J_4 - C') \\
J_8(\mathcal{C}) =& 2^{-2} (J_2 J_6 - J_4^2) \\
J_{10}(\mathcal{C}) =& 2^{-12} D'.
\end{aligned}$$

Ces résultats ont servi à implémenter la fonction `formal_igusa_invariants` de l'annexe A.2.

5.1.3.2 Les g_2-invariants

Cette partie s'inspire des résultats de [CQ05]. Comme dans cet article, on définit un triplet d'invariants absolus algébriquement indépendants (les g_2-invariants). Ceux-ci permettent de paramétriser l'espace de modules et par suite, de reconstruire une courbe $\mathcal{C}$ de genre 2 ayant ces invariants. Ce point sera l'objet du chapitre 6.

Définition 23. *On appelle* g_2-invariants *de* $\mathcal{C}$*, les invariants absolus définis à partir des invariants d'Igusa de* $\mathcal{C}$ *de la façon suivante :*

1. *Si* $J_2(\mathcal{C}) \neq 0$ *alors*

$$g_1(\mathcal{C}) = \frac{J_2^5(\mathcal{C})}{J_{10}(\mathcal{C})},\ g_2(\mathcal{C}) = \frac{J_2^3(\mathcal{C})J_4(\mathcal{C})}{J_{10}(\mathcal{C})} \text{ et } g_3(\mathcal{C}) = \frac{J_2^2(\mathcal{C})J_6(\mathcal{C})}{J_{10}(\mathcal{C})}.$$

2. *Si* $J_2(\mathcal{C}) = 0$ *et* $J_4(\mathcal{C}) \neq 0$ *alors*

$$g_1(\mathcal{C}) = 0,\ g_2(\mathcal{C}) = \frac{J_4^5(\mathcal{C})}{J_{10}^2(\mathcal{C})} \text{ et } g_3(\mathcal{C}) = \frac{J_4(\mathcal{C})J_6(\mathcal{C})}{J_{10}(\mathcal{C})}.$$

3. *Si* $J_2(\mathcal{C}) = 0$ *et* $J_4(\mathcal{C}) = 0$ *alors*

$$g_1(\mathcal{C}) = 0,\ g_2(\mathcal{C}) = 0 \text{ et } g_3(\mathcal{C}) = \frac{J_6^5(\mathcal{C})}{J_{10}^3(\mathcal{C})}.$$

Grâce à la proposition 15 (p. 52), il est naturel de définir l'application suivante :

$$\begin{aligned} \varphi : \mathcal{M}_2(k) &\to k^3. \\ [\mathcal{C}] &\to (g_1(\mathcal{C}), g_2(\mathcal{C}), g_3(\mathcal{C})) \end{aligned}$$

Cette application n'est pas à proprement parler introduite dans [CQ05]. Nous l'avons introduite afin de rendre explicite le plongement de $\mathcal{M}_2(k)$ dans k^3.

Proposition 17. *φ est une bijection.*

Avant d'expliquer cette proposition, on va démontrer le lemme suivant :

Lemme 4. *Soit $\mathcal{C}$ une courbe de genre 2. Les invariants absolus de $\mathcal{C}$ peuvent s'exprimer comme fractions rationnelles des invariants d'Igusa de $\mathcal{C}$.*

Démonstration. Soient $I(\mathcal{C})$ un invariant absolu de $\mathcal{C}$, $J_2(\mathcal{C})$, $J_4(\mathcal{C})$, $J_6(\mathcal{C})$ et $J_{10}(\mathcal{C})$ les invariants d'Igusa de $\mathcal{C}$ et $R(\mathcal{C})$ un invariant de degré 15. Sachant que $J_2(\mathcal{C})$, $J_4(\mathcal{C})$, $J_6(\mathcal{C})$, $J_{10}(\mathcal{C})$ et $R(\mathcal{C})$ génèrent tous les invariants de $\mathcal{C}$, $I(\mathcal{C})$ peut s'exprimer comme une fraction rationnelle de $J_2(\mathcal{C})$, $J_4(\mathcal{C})$, $J_6(\mathcal{C})$, $J_{10}(\mathcal{C})$ et $R(\mathcal{C})$. Or, $R(\mathcal{C})$ est le seul invariant de degré impair de la liste. En conséquence, il ne peut apparaitre qu'avec une puissance paire dans $I(\mathcal{C})$. De plus, $R(\mathcal{C})^2$ peut être exprimé comme polynôme homogène en les $J_2(\mathcal{C})$, $J_4(\mathcal{C})$, $J_6(\mathcal{C})$ et $J_{10}(\mathcal{C})$ (cf. chapitre 6). Ainsi, $I(\mathcal{C})$ s'écrit comme une fraction rationnelle de $J_2(\mathcal{C})$, $J_4(\mathcal{C})$, $J_6(\mathcal{C})$ et $J_{10}(\mathcal{C})$. □

Démonstration de la proposition 17 (p. 57). On va démontrer l'injectivité de cette application. La surjectivité fait l'objet du chapitre 6. Soient $\mathcal{C}$ et $\mathcal{C}'$ deux courbes de genre 2 telles que

$$(g_1(\mathcal{C}), g_2(\mathcal{C}), g_3(\mathcal{C})) = (g_1(\mathcal{C}'), g_2(\mathcal{C}'), g_3(\mathcal{C}')).$$

Pour prouver que $[\mathcal{C}] = [\mathcal{C}']$, on montre que $\mathcal{C}$ et $\mathcal{C}'$ ont les mêmes invariants absolus. D'après le lemme 4 (p. 57), les invariants absolus de $\mathcal{C}$ peuvent s'exprimer comme fractions rationnelles des invariants d'Igusa de $\mathcal{C}$. Ainsi, il suffit de déterminer $\lambda \in \overline{k}$ tel que $J_i(\mathcal{C}) = \lambda^i J_i(\mathcal{C}')$ pour

$i \in \{2,4,6,10\}$. Les autres cas se traitant de façon analogue, on développe seulement le premier cas :

$$g_1(\mathcal{C}) = \frac{J_2^5(\mathcal{C})}{J_{10}(\mathcal{C})},\ g_2(\mathcal{C}) = \frac{J_2^3(\mathcal{C})J_4(\mathcal{C})}{J_{10}(\mathcal{C})} \text{ et } g_3(\mathcal{C}) = \frac{J_2^2(\mathcal{C})J_6(\mathcal{C})}{J_{10}(\mathcal{C})}.$$

On pose :

$$\lambda = \sqrt[10]{\frac{J_{10}(\mathcal{C})}{J_{10}(\mathcal{C}')}}.$$

Comme $g_1(\mathcal{C}) = g_1(\mathcal{C}')$, on obtient :

$$\sqrt[5]{\frac{J_{10}(\mathcal{C})}{J_{10}(\mathcal{C}')}} = \frac{J_2(\mathcal{C})}{J_2(\mathcal{C}')}.$$

Ainsi, $J_2(\mathcal{C}) = \lambda^2 J_2(\mathcal{C}')$ et $J_{10}(\mathcal{C}) = \lambda^{10} J_{10}(\mathcal{C}')$. Sachant que $g_2(\mathcal{C}) = g_2(\mathcal{C}')$ et $g_3(\mathcal{C}) = g_3(\mathcal{C}')$, les égalités $J_4(\mathcal{C}) = \lambda^4 J_4(\mathcal{C}')$ et $J_6(\mathcal{C}) = \lambda^6 J_6(\mathcal{C}')$ se vérifient aisément. L'injectivité de l'application est alors établie. □

Grâce à cette proposition, $\mathcal{M}_2(k)$ s'injecte dans k^3 via les $\mathtt{g}_2$-invariants. à première vue, il n'est pas évident que des invariants absolus définis sur k garantissent qu'on puisse trouver un ensemble de générateurs correspondants $J_2,\ J_4,\ J_6,\ J_{10},\ R \in k$ engendrant ces $\mathtt{g}_2$-invariants. Le lemme suivant prouve l'existence de tels invariants.

Lemme 5. *Pour tout point $[\mathcal{C}] \in \mathcal{M}_2(k)$, il existe des invariants définis sur k qui donnent les $\mathtt{g}_2$-invariants de $[\mathcal{C}]$.*

Démonstration. Soit :

$$(J_2, J_4, J_6, J_{10}) = \begin{cases} (g_1, g_1g_2, g_1^2g_3, g_1^4), & \text{si } g_1 \neq 0, \\ (0, g_2, g_2g_3, g_2^2), & \text{si } g_1 = 0,\ g_2 \neq 0, \\ (0, 0, g_3^2, g_3^3), & \text{si } g_1 = g_2 = 0, g_3 \neq 0, \\ (0, 0, 0, 1), & \text{si } g_1 = g_2 = g_3 = 0. \end{cases}$$

Avec ce choix, on obtient les bonnes valeurs des $\mathtt{g}_2$-invariants de $[\mathcal{C}]$. On peut aussi choisir R de telle sorte qu'il soit défini sur k. Puisque R^2 s'exprime comme combinaison algébrique des J_i (cf. proposition35 (p. 97) pour l'expression exacte), R est de la forme $\sqrt{d}R_0$ avec $R_0, d \in k$. Soit $r = \sqrt{d}$, on construit un autre ensemble d'invariants équivalent au premier et définis sur k :

$$\begin{aligned}(J_2', J_4', J_6', J_{10}', R') &= (r^2J_2, r^4J_4, r^6J_6, r^{10}J_{10}, r^{15}R) \\ &= (dJ_2, d^2J_4, d^3J_6, d^5J_{10}, d^6R_0).\end{aligned}$$

□

La fonction `g2_to_Igusa_invariants` de l'annexe A.2 est une implémentation `sage` de cette méthode.

5.2 Approche de Geyer-Sturmfels

Exceptés les quartiques (cf. [Bas15, sec 2.10.2]) et les invariants d'Igusa pour les sextiques, on ne connait pas de système générateur pour les invariants en toute caractéristique. Grâce à des réductions astucieuses et de nombreux calculs, Basson a exposé dans sa thèse un système de "séparant"[2] qu'il conjecture être générateur en caractéristique 3 et 7 pour les octiques. Quant aux caractéristiques ≥ 11, elles sont connues par les résultats de [LR12]. Afin d'obtenir de nouveaux

2. *i.e.* : qui sépare les orbites (cf définition 27 (p. 61))

résultats pour les covariants, on va mettre en place une méthode de calcul totalement différente en suivant [Gey74] et [Stu08]. On va ainsi obtenir des résultats pour les covariants des quartiques en caractéristique 3 et retrouver les résultats d'Igusa pour les invariants en caractéristique ≥ 3. Par contre, on se heurtera à deux écueils : comme pour Basson, en petite caractéristique, notre méthode ne fournit qu'un système de séparants. Plus limitant encore, dès le cas des sextiques, le temps de calcul pour les covariants devient prohibitif et on n'est pas en mesure de faire aboutir les calculs par la force brute.

5.2.1 Définitions et résultats

On va modifier légèrement les résultats de Sturmfels [Stu08, Chap 3, sec 6] afin qu'ils soient valables en toute caractéristique. Dans le cas des invariants, il s'agit exactement de la méthode de Geyer [Gey74]. Soient k un corps algébriquement clos de caractéristique p et $n > 1$ un entier positif. On considère la forme binaire :

$$\begin{aligned} f(x,z) &= \sum_{k=0}^{n} a_k x^k z^{n-k} \\ &= (\mu_1 x - \nu_1 z)(\mu_2 x - \nu_2 z)\dots(\mu_n x - \nu_n z). \end{aligned}$$

Les "racines" (μ_i, ν_i) peuvent être vues comme des points $(\mu_i, \nu_i) \in \mathbb{P}^1$.

Remarque 14. *Pour Sturmfels, $f(x,z) = \sum_{k=0}^{n} \mathbf{C}_n^k a_k x^k z^{n-k}$. Néanmoins, cette écriture ne fonctionne pas en toute caractéristique.*

L'étude des covariants de n-points de $\mathbb{P}^1$ sur l'action de $\mathrm{GL}_2(k)$ est un sujet classique et on va rappeler ci-dessous les résultats principaux. Le principal avantage de ce travail est qu'il existe un système de générateurs explicite de covariants *indépendants* de la caractéristique. Les covariants pour les formes binaires proviennent alors de la sous-algèbre symétrisée par $\mathcal{S}_n$.

Définition 24. *Soient M un monôme appartenant à $k[\mu_1, \nu_1, \mu_2, \nu_2, \dots, \mu_n, \nu_n,\ x,\ z]$ tel que :*

$$M = \mu_1^{u_1}\mu_2^{u_2}\cdots\mu_n^{u_n}\nu_1^{v_1}\nu_2^{v_2}\cdots\nu_n^{v_n}x^{w_1}z^{w_2}$$

et P un polynôme appartenant à $k[\mu_1, \nu_1, \mu_2, \nu_2, \dots, \mu_n, \nu_n,\ x,\ z]$. On dit que :

- *M est* régulier de degré d *si $u_1 + v_1 = u_2 + v_2 = \cdots = u_n + v_n = d$. L'entier d est appelé le* degré de régularité *de M.*
- *P est* régulier de degré d *si tous ses monômes sont réguliers de degré d. Lorsque P est régulier pour un certain degré d, on dira que P est* régulier.
- *P est* symétrique *si, pour toute permutation $\sigma \in S_n$, il vérifie :*

$$P(\mu_1, \nu_1, \mu_2, \nu_2, \dots, \mu_n, \nu_n,\ x,\ z) = P(\mu_{\sigma(1)}, \nu_{\sigma(1)}, \mu_{\sigma(2)}, \nu_{\sigma(2)}, \dots, \mu_{\sigma(n)}, \nu_{\sigma(n)},\ x,\ z).$$

Un monôme régulier est dit réductible *s'il peut s'exprimer comme le produit de deux monômes réguliers de degré de régularité supérieur ou égal à 1.*

On définit l'action de $\mathrm{GL}_2(k)$ sur $k[\mu_1, \nu_1, \mu_2, \nu_2, \dots, \mu_n, \nu_n,\ x,\ z]$ de la façon suivante : soit $M \in \mathrm{GL}_2(k)$,

$$\begin{pmatrix} \nu_i \\ \mu_i \end{pmatrix} \to \begin{pmatrix} \overline{\nu}_i \\ \overline{\mu}_i \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} \nu_i \\ \mu_i \end{pmatrix}$$

$$\begin{pmatrix} x \\ z \end{pmatrix} \to \begin{pmatrix} \overline{x}_i \\ \overline{z}_i \end{pmatrix} = M^{-1} \cdot \begin{pmatrix} x \\ z \end{pmatrix}.$$

Définition 25. *Un polynôme P régulier est un* covariant (de n points) *s'il existe $w \in \mathbb{Z}$ tel que :*

$$P(\overline{\mu}_1, \overline{\nu}_1, \overline{\mu}_2, \overline{\nu}_2, \dots, \overline{\mu}_n, \overline{\nu}_n,\ \overline{x},\ \overline{z}) = \det(M)^w P(\mu_1, \nu_1, \mu_2, \nu_2, \dots, \mu_n, \nu_n,\ x,\ z).$$

On dira que P est un invariant s'il ne dépend pas de x et z.

Il est facile de définir des quantités covariantes.

Définition 26. *Soit $1 \leq i < j \leq n$, on appelle* crochet *les quantités suivantes :*

$$[ij] := \mu_i\nu_j - \nu_i\mu_j,$$
$$[iu] := \mu_i x - \nu_i z.$$

Le sous-anneau $\mathcal{B}(n)$ engendré par ces crochets dans $k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n,\ x,\ z]$, est appelé *l'anneau crochet*. On note également $\mathcal{B}_{reg}(n)$ le sous-anneau de $\mathcal{B}(n)$ des polynômes en les crochets qui sont réguliers de degré d pour $d \geq 0$. Ce dernier est engendré par les monômes de la forme :

$$\prod_{i<j}[ij]^{m_{ij}},$$

où les entiers m_{ij} vérifient $d = \sum_{j=1}^{i-1} m_{ji} + \sum_{j=i+1}^{n} m_{ij}$. En fait, on a un résultat plus fort :

Théorème 8. *(lemme de Kempe ([Stu08, th. 3.7.3 p. 132])) L'anneau $\mathcal{B}_{reg}(n)$ est engendré par les monômes de degré de régularité 1 ou 2.*

Remarque 15. *D'après [HMSV09, th.2.3 p.7], si on se restreint aux invariants et si n est pair, on peut engendrer ce sous-anneau en degré de régularité 1.*

Le résultat suivant est une conséquence du premier théorème fondamental (cf [Wey39]).

Théorème 9. *L'anneau des polynômes covariants réguliers est égal à $\mathcal{B}_{reg}(n)$.*

Lorsque le groupe qui agit est $\mathrm{GL}_2(\mathbb{C})$, le théorème 3.2.1 et le lemme 3.6.5 de [Stu08] fournissent une démonstration. Lorsque le groupe est quelconque, la preuve se trouve dans [dCP76]. On notera aussi que [Gey74, Satz 5] donne une démonstration élémentaire dans le cas de $\mathrm{GL}_2(k)$.

Dans la section 5.2.4, on présentera un exemple de calcul de générateurs pour $\mathcal{B}_{reg}(n)$ et son sous-anneau des invariants. Il reste à décrire la dernière étape pour obtenir les covariants des formes binaires. Soit :

$$\begin{aligned}\Psi : k[a_0, a_1, \ldots, a_n,\ x,\ z] &\to k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n,\ x,\ z]\\ a_{n-k} &\to (-1)^n \mu_1 \cdots \mu_n \cdot \sigma_k(\frac{\nu_1}{\mu_1}, \ldots, \frac{\nu_n}{\mu_n}).\end{aligned}$$

σ_k représente la k-ième fonction polynôme symétrique élémentaire en n variables.

Remarque 16. *Sturmfels définit Ψ de la façon suivante :*

$$\begin{aligned}\Psi : k[a_0, a_1, \ldots, a_n,\ x,\ z] &\to k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n,\ x,\ z]\\ a_{n-k} &\to \frac{(-1)^n}{n!} \mu_1 \cdots \mu_n \cdot \sigma_k(\frac{\nu_1}{\mu_1}, \ldots, \frac{\nu_n}{\mu_n})\end{aligned}$$

mais le $\frac{1}{n!}$ ne compense pas le facteur $\binom{k}{n}$ de son expression de f.

Le théorème suivant (issu de [Stu08, th3.6.6]) est une conséquence élémentaire du théorème précédent. On note $\mathcal{B}_{reg,sym}(n)$ le sous-anneau de $\mathcal{B}_{reg}(n)$ des polynômes en les crochets qui sont symétriques.

Théorème 10. *L'application Ψ est un isomorphisme entre l'anneau des covariants de $k[a_0, \ldots, a_n, x, z]$ et le sous-anneau $\mathcal{B}_{reg,sym}(n)$ des fonctions polynomiales crochets régulières et symétriques de $k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n,\ x,\ z]$. Si $C(a_0, \ldots, a_n)$ est un covariant de degré d et d'ordre r alors $\Psi(C)$ est une fonction polynomiale crochet symétrique telle que :*

1. *à l'intérieur de chaque monôme de $\Psi(C)$, les indices 1, 2,..., n apparaissent d fois,*
2. *à l'intérieur de chaque monôme de $\Psi(C)$, la lettre u apparaisse r fois.*

On souhaite alors calculer $\mathcal{C}_n$ comme $\mathcal{B}_{reg}(n)^{\mathcal{S}_n}$. Si on note $b_1, \ldots, b_t$ un système de générateurs de monômes crochets pour $\mathcal{B}_{reg}(n)$, on a un morphisme surjectif :

$$\begin{array}{ccc} k[x_1, \ldots, x_t] & \to & \mathcal{B}_{reg}(n). \\ x_i & \to & b_i \end{array}$$

Le noyau I de ce morphisme est engendré par les relations suivantes.

Proposition 18. *Soient $1 \leq i < j < k < l \leq n$, on a :*

$$[ik][jl] = [ij][kl] + [il][jk],$$

$$[ik][ju] = [ij][ku] + [iu][jk].$$

Ces relations sont appelées les syzygies.

L'action de $\mathcal{S}_n$ sur les b_i induit une représentation G_n de $\mathcal{S}_n$ dans $\mathrm{GL}_t(k)$. Il existe des algorithmes permettant de calculer $k[x_1, \ldots, x_t]^{G_n} = R_n$ (cf [DK02]). Ces derniers étant aussi valables dans le cas modulaire (c'est à dire avec $p \mid |G_n|$), on les utilise "naivement" à travers leurs implémentations `Magma`. Pour autant, comme indiqué précédemment, ce procédé engendre une limitation dès que $n = 6$. Il reste à préciser le lien entre R_n et $\mathcal{C}_n$.

Lorsque p ne divise pas $|\mathcal{S}_n|$, $\mathcal{S}_n$ est un groupe linéairement réductif (cf [DK02, Def 2.2.1]) et l'existence des opérateurs de Reynolds (cf [DK02, Th 2.2.5]) permet de préserver la surjectivité du morphisme $k[x_1, \ldots, x_n] \to \mathcal{B}_{reg}(n)$ lors du passage au symétrisé.

Proposition 19. *([Stu08, lem.3.7.2]) L'image d'un système générateur de R_n par la surjection canonique $k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]/I = \mathcal{B}_{reg}(n)$ est un système générateur de $\mathcal{C}_n = \mathcal{B}_{reg}(n)^{\mathcal{S}_n}$.*

En particulier, si $p > n$, on obtient une généralisation du résultat de Geyer.

Proposition 20. *Pour $p > n$, l'anneau des covariants $\mathcal{C}_n$ est la réduction modulo p de l'anneau des covariants en caractéristique 0. En particulier les séries de Poincaré bi-graduées sont identiques.*

Lorsque $p \mid |\mathcal{S}_n|$, $\mathcal{S}_n$ n'est plus qu'un groupe réductif (cf. [DK02, sec 2.2.2]) et le résultat précédent n'est plus valable dans le cas général. Pour palier à cela, on introduit concept suivant :

Définition 27. *Soit X une variété affine et G un groupe d'automorphisme de $k[X]$. Un sous-ensemble $S \subseteq k[X]^G$ est dit* séparant *si, pour chaque paire de points (x, y) de X, on a la propriété suivante : s'il existe un élément $f \in k[X]^G$ tel que $f(x) \neq f(y)$, alors il existe un élément g de G tel que $g(x) \neq g(y)$.*

La relation avec l'anneau des invariants est la suivante (cf [DK02, prop.2.3.10]) :

Proposition 21. *On suppose que X est irréductible et $k[X]^G$ est de type fini. Soit $A \subseteq k[X]^G$ une sous-algèbre séparante de type finie.* $\mathrm{Frac}(k[X]^G)$ *est alors une extension finie purement inséparable de* $\mathrm{Frac}(A)$*. En particulier, si la caractéristique de k est nulle alors :*

$$\mathrm{Frac}(A) = \mathrm{Frac}(k[X]^G).$$

La définition 27 présente l'avantage de préserver la surjectivité lors du passage aux invariants.

Théorème 11 ([DK02, p. 59])**.** *Soit G un groupe algébrique linéaire. Les assertions suivantes sont équivalentes.*

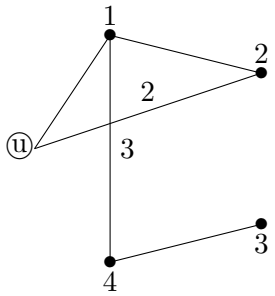
- *G est réductif.*
- *Si G agit régulièrement sur une variété affine X et si $Y \subseteq X$ est une sous-variété G-stable, alors l'application de restriction $k[X] \to k[Y]$ envoie un sous-ensemble séparant de $k[X]^G$ sur un sous-ensembles séparants de $k[Y]^G$.*

Ainsi R_n est l'algèbre des séparants des covariants des formes binaires de degré n mais on n'a pas nécessairement égalité. On verra que le cas des quartiques en caractéristique 3 illustre cette inclusion stricte.

Afin d'exhiber plus facilement un système de générateurs de $\mathcal{B}_{reg}(n)$ les monômes vont être représentés par des graphes valués tels que les sommets forment un polygône régulier. On représente :

— un monôme de $\mathcal{B}(n)$ par un graphe à n sommets numérotés de 1 à n et un sommet appelé ⓤ,
— le crochet $[ij]$ par une arête reliant le sommet i au sommet j avec $i < j \in \{1, \dots, n\}$,
— le crochet $[iu]$ par une arête reliant ⓤ au sommet i.

à titre d'exemple, le produit de crochets $[12][14]^3[34][1u][2u]^2 \in \mathcal{B}(4)$ est représenté par le graphe suivant :



Les résultats précédents font émerger 5 remarques très utiles. Le point suivant découle de la définition de $\mathcal{B}_{reg}(n)$.

Point 1. *Chaque monôme d'ordre m et de degré de régularité d est représenté par un graphe ayant m connexions avec ⓤ et chaque sommet numeroté a une valence d.*

De plus, d'après le théorème 8 (p. 60), l'algèbre des covariants de n points est engendré par des éléments de degré de régularité au plus 2. Également, d'après la remarque 15 (p. 60), les invariants de n points sont engendrés par les degrés de régularité 1, d'où le point suivant :

Point 2. *Les sommets numérotés ont une valence au plus* 2. *Pour les invariants, ils ont une valence* 1.

De part sa définition, si un graphe s'exprime comme union de sous-graphes correspondants à des graphes de degré et d'ordre inférieurs déjà calculés, le covariant associé est réductible.

Point 3. *On exclut les graphes ayant un sous-graphe déjà calculé.*

Lorsque les sommets sont placés sur un polygone régulier, la proposition 18 (p. 61) entraîne le point suivant (voir [KR84, th.6.2 p.72] pour une démonstration) :

Point 4. *On considère uniquement les graphes n'ayant pas de croisement d'arêtes.*

Grâce au point 2, le nombre d'arêtes adjacentes à ⓤ possède une borne supérieure grossière. De plus, lorsque n est pair, le point 1 impose une autre condition sur les arêtes adjacentes à ⓤ.

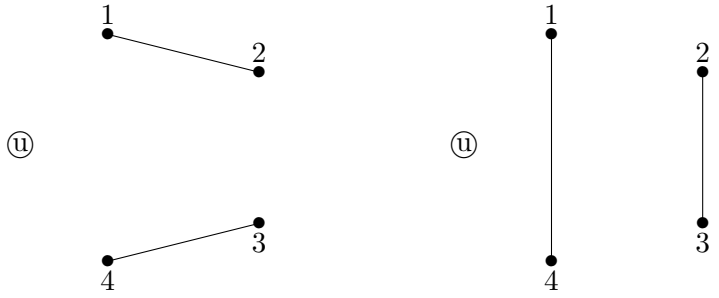
Point 5. ⓤ *a au plus* $2n$ *arêtes adjacentes.*
Lorsque n est pair, ⓤ *a un nombre pair d'arêtes adjacentes.*

5.2.2 Calcul de $\mathcal{B}_{reg}(4)$ avec l'approche graphique

On va exploiter les cinq points de la section 5.2.1 pour construire un système de générateurs de $\mathcal{B}_{reg}(4)$. Le point 5 (p. 62) permet de considérer seulement les ordres 0, 2, 4, 6 et 8. Grâce au point 2 (p. 62), on retient uniquement les graphes dont les sommets numérotés ont une valence 1 ou 2.

5.2.2.1 Formes quartiques, ordre 0

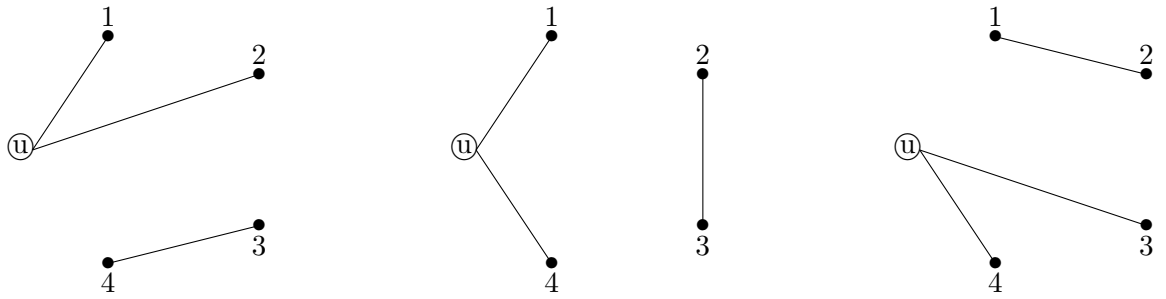
Tout d'abord, grâce à la seconde partie du point 2 (p. 62), on considère uniquement les graphes de degré de régularité 1. Ensuite, l'utilisation du point 1 (p. 62) réduit le système de générateurs à 3 graphes. Enfin, le point 4 (p. 62) permet de simplifier ce système aux 2 graphes présentés ci-dessous.



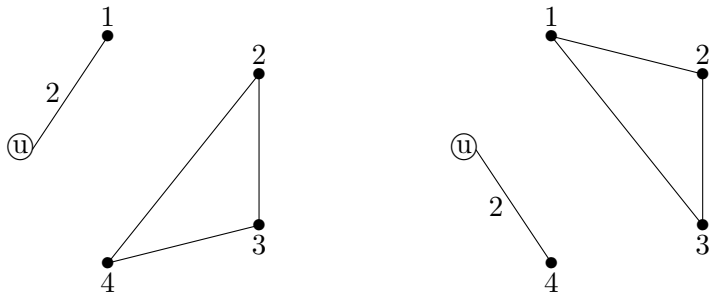
On les appelle respectivement t_0 et t_1. Ces deux graphes représentent deux covariants de 4 points qui engendrent l'algèbre des invariants de 4 points.

5.2.2.2 Formes quartiques, ordre 2

On étudie d'abord les graphes dont les sommets numérotés ont une valence 1. L'utilisation du point 1 (p. 62) réduit le système à 6 graphes. Le point 4 (p. 62) permet de simplifier ce système aux 3 graphes donnés ci-dessous.



On les appelle respectivement u_0, u_1 et u_2. à présent, on étudie les graphes dont les sommets numérotés ont une valence 2. L'utilisation du point 1 (p. 62) réduit le système à considérer à 11 graphes. Ensuite, le point 4 (p. 62) permet de simplifier ce système à 6 graphes. Enfin, le point 3 (p. 62) permet de réduire ce système aux deux graphes suivants :

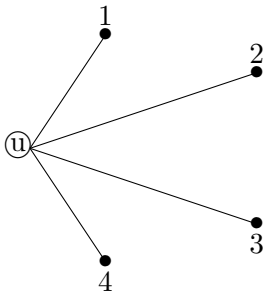


On les appelle respectivement U_0 et U_1. Grâce à la proposition 18 (p. 61), il est possible d'exprimer U_0 et U_1 en fonction des graphes déjà calculés de la façon suivante :

$$\begin{aligned} U_0 &= t_1 u_0 - t_0 u_1, \\ U_1 &= t_1 u_2 - t_0 u_1. \end{aligned}$$

5.2.2.3 Formes quartiques, ordre 4

Le seul graphe dont les sommets numérotés ont tous une valence 1 et dont le sommet ⓤ a une valence 4 est celui correspondant à la forme f. Il s'agit du graphe suivant :



Il y a 36 graphes dont les sommets numérotés ont tous une valence 2 et le sommet ⓤ a une valence 4. Cependant, ils sont tous le produit de deux graphes de valence 1 sur les sommets numérotés. Ils correspondent donc à des covariants de 4 points réductibles.

5.2.2.4 Formes quartiques, ordre ≥ 6

Il n'y a pas de graphe de valence 1 sur les sommets numérotés. De plus, de la même façon que précédement, tous les graphes (de degré 2) construits sont réductibles. En résumé, on a calculé 6 générateurs de l'algèbre des covariants de 4 points. Il s'agit des éléments t_0, t_1, u_0, u_1, u_2 et f. à présent, on va faire agir le groupe $\mathcal{S}_4$ sur ces covariants pour retrouver un système séparant de l'algèbre des covariants d'une forme binaire en caractéristique 3.

5.2.3 Covariants de formes quartiques

Dans le paragraphe précédent, on a vu que l'algèbre des covariants de 4 points est engendré par t_0, t_1, u_0, u_1, u_2 et f. On va faire agir le groupe $\mathcal{S}_4$ puis, à l'aide de la fonction `InvariantRing` de `Magma`, on va calculer un système séparant de l'algèbre des covariants $\mathcal{C}_4$. Sachant que $\mathcal{S}_4$ est engendré par $\sigma = (1234)$ et $\tau = (12)$, l'action de $\mathcal{S}_4$ sur t_0, t_1, u_0, u_1, u_2 et f est donnée par les égalités suivantes :

$$\begin{array}{llll} t_0^\tau = -t_0 & et & t_0^\sigma = -t_1, \\ t_1^\tau = t_1 + t_0 & et & t_1^\sigma = -t_0, \\ u_0^\tau = u_0 & et & u_0^\sigma = -(u_0 + u_1 + u_2), \\ u_1^\tau = u_1 + u_2 & et & u_1^\sigma = u_0, \\ u_2^\tau = -u_2 & et & u_2^\sigma = u_1, \\ f^\tau = f & et & f^\sigma = f. \end{array}$$

Grâce au code `Magma`

```
FF:= Rationals();
M1:= Matrix(FF,[
               [0,-1,0,0,0,0],
               [-1,0,0,0,0,0],
               [0,0,-1,-1,-1,0],
               [0,0,1,0,0,0],
               [0,0,0,1,0,0],
               [0,0,0,0,0,1]
               ]);
// representation de l'action du cycle (123456)

M2:=Matrix(FF,[
               [-1,0,0,0,0,0],
```

```
                [1,1,0,0,0,0],
                [0,0,1,0,0,0],
                [0,0,0,1,1,0],
                [0,0,0,0,-1,0],
                [0,0,0,0,0,1]
                ]);
// representation de l'action du cycle (12)

GT :=  MatrixGroup<6, FF| [M1,M2]>;
// Groupe genere par les matrices M1 et M2
R:=InvariantRing(GT);
// Anneau des invariants du groupe G sur un ensemble de 6 points
F:=FundamentalInvariants(R);
// Invariants qui engendrent l'anneau R
```

on trouve que les fonctions invariantes qui engendrent $\mathbb{C}[t_0, t_1, u_0, u_1, u_2, f]^{\mathtt{GT}}$ sont donnés par les équations suivantes :

$$
\begin{aligned}
C_1 =& f,\\
C_2 =& t_0^2 + t_0t_1 + t_1^2,\\
C_3 =& u_0^2 + 4/3u_0u_1 + 2/3u_0u_2 + 4/3u_1^2 + 4/3u_1u_2 + u_2^2,\\
C_4 =& t_0^3 + 3/2t_0^2t_1 - 3/2t_0t_1^2 - t_1^3,\\
C_5 =& t_0u_0u_1 + 2t_0u_0u_2 + t_0u_1^2 + t_0u_1u_2 + 2t_1u_0u_1 + t_1u_0u_2 + 2t_1u_1^2 + 2t_1u_1u_2,\\
C_6 =& u_0^3 + 2u_0^2u_1 + u_0^2u_2 - u_0u_2^2 - 2u_1u_2^2 - u_2^3,\\
C_7 =& t_0^2u_0u_1 + 2t_0^2u_0u_2 + t_0^2u_1^2 + t_0^2u_1u_2 - 2t_0t_1u_0u_1 + 2t_0t_1u_0u_2 - 2t_0t_1u_1^2\\
&- 2t_0t_1u_1u_2 - 2t_1^2u_0u_1 - t_1^2u_0u_2 - 2t_1^2u_1^2 - 2t_1^2u_1u_2,\\
C_8 =& u_0^2u_1^2 + u_0^2u_1u_2 + u_0^2u_2^2 + 2u_0u_1^3 + 3u_0u_1^2u_2 + u_0u_1u_2^2 + u_1^4 + 2u_1^3u_2 + u_1^2u_2^2,\\
C_9 =& t_0u_0^3u_1 + 2t_0u_0^3u_2 + 3/2t_0u_0^2u_1^2 + 6t_0u_0^2u_1u_2 + 3t_0u_0^2u_2^2 + t_0u_0u_1^3 + 6t_0u_0u_1^2u_2\\
&+ 6t_0u_0u_1u_2^2 + 2t_0u_0u_2^3 + 1/2t_0u_1^4 + t_0u_1^3u_2 + 3/2t_0u_1^2u_2^2 + t_0u_1u_2^3 + 2t_1u_0^3u_1\\
&+ t_1u_0^3u_2 + 3t_1u_0^2u_1^2 + 3t_1u_0^2u_1u_2 + 3/2t_1u_0^2u_2^2 + 2t_1u_0u_1^3 + 3t_1u_0u_1^2u_2 + 3t_1u_0u_1u_2^2\\
&+ t_1u_0u_2^3 + t_1u_1^4 + 2t_1u_1^3u_2 + 3t_1u_1^2u_2^2 + 2t_1u_1u_2^3.
\end{aligned}
$$

On évalue ces fonctions en t_0, t_1, u_0, u_1, u_2 et f puis on réduit le système construit grâce à la fonction `MinimalAlgebraGenerators` de `Magma`. On obtient alors les covariants suivants :

$$
\begin{aligned}
c_{0,2} =& -3a_1a_3 + a_2^2 + 12a_4a_0,\\
c_{0,3} =& -27/2a_1^2a_4 + 9/2a_1a_2a_3 - a_2^3 + 36a_2a_4a_0 - 27/2a_3^2a_0,\\
c_{4,1} =& a_0z^4 + a_1xz^3 + a_2x^2z^2 + a_3x^3z + a_4x^4,\\
c_{4,2} =& (a_1^2 - 8/3a_2a_0)z^4 + (4/3a_1a_2 - 8a_3a_0)xz^3 + (4/3a_2^2 - 2a_1a_3 - 16a_4a_0)x^2z^2\\
&+ (4/3a_2a_3 - 8a_1a_4)x^3z + (a_3^2 - 8/3a_2a_4)x^4,\\
c_{6,3} =& (a_1^3 - 4a_1a_0a_2 + 8a_0a_3)z^6 + (2a_1^2a_2 + 4a_0a_1a_3 - 8a_0a_2^2 + 32a_0^2a_4)xz^5 +\\
&(5a_1^2a_3 + 40a_0a_1a_4 - 20a_0a_2a_3)x^2z^4 + (20a_1^2a_4 - 20a_0a_3^2)x^3z^3 +\\
&(20a_1a_2a_4 - 5a_1a_3^2 - 40a_0a_3a_4)x^4z^2 + (8a_2^2a_4 - 4a_1a_3a_4 - 2a_2a_3^2 - 32a_0a_4^2)x^5z +\\
&(4a_2a_3a_4 - 8a_1a_4^2 - a_3^3)x^6.
\end{aligned}
$$

On retrouve bien les covariants classiques de la caractéristique nulle.

On applique le même méthode en caractéristique 3. Les fonctions invariantes qui engendrent $\overline{\mathbb{F}}_3[t_0,t_1,u_0,u_1,u_2,f]^{\mathtt{GT}}$ sont donnés par les équations suivantes :

$$
\begin{aligned}
C_1 =& t_0 + 2t_1,\\
C_2 =& f,\\
C_3 =& u_0u_1 + 2u_0u_2 + u_1^2 + u_1u_2,\\
C_4 =& u_0^3 + 2u_0^2u_1 + u_0^2u_2 + 2u_0u_2^2 + u_1u_2^2 + 2u_2^3,\\
C_5 =& t_0^2u_0^2 + 2t_0^2u_0u_1 + 2t_0^2u_0u_2 + 2t_0^2u_1^2 + 2t_0^2u_1u_2 + t_0^2u_2^2 + t_0t_1u_0^2 + 2t_0t_1u_0u_2\\
&+ t_0t_1u_2^2 + t_1^2u_0^2 + t_1^2u_2^2,\\
C_6 =& u_0^3u_1 + 2u_0^3u_2 + u_0u_1^3 + 2u_0u_2^3 + 2u_1^4 + u_1^3u_2 + u_1u_2^3,\\
C_7 =& t_0^4t_1^2 + 2t_0^3t_1^3 + t_0^2t_1^4,\\
C_8 =& t_0^3t_1u_0u_1 + t_0^3t_1u_1^2 + t_0^3t_1u_1u_2 + t_0^2t_1^2u_0u_1 + 2t_0^2t_1^2u_0u_2 + t_0^2t_1^2u_1^2\\
&+ t_0^2t_1^2u_1u_2 + 2t_0t_1^3u_0u_2,\\
C_9 =& t_0^2u_0^4 + 2t_0^2u_0^3u_2 + 2t_0^2u_0^2u_1^2 + 2t_0^2u_0^2u_1u_2 + 2t_0^2u_0^2u_2^2 + t_0^2u_0u_1^3 +\\
&2t_0^2u_0u_1u_2^2 + 2t_0^2u_0u_2^3 + 2t_0^2u_1^4 + t_0^2u_1^3u_2 + 2t_0^2u_1^2u_2^2 + t_0^2u_2^4 + t_0t_1u_0^4 +\\
&2t_0t_1u_0^3u_1 + 2t_0t_1u_0^3u_2 + 2t_0t_1u_0^2u_1^2 + 2t_0t_1u_0^2u_1u_2 + 2t_0t_1u_0^2u_2^2 + 2t_0t_1u_0u_1u_2^2 +\\
&2t_0t_1u_0u_2^3 + 2t_0t_1u_1^2u_2^2 + 2t_0t_1u_1u_2^3 + t_0t_1u_2^4 + t_1^2u_0^4 + 2t_1^2u_0^3u_1 + t_1^2u_0^3u_2 +\\
&2t_1^2u_0^2u_1^2 + 2t_1^2u_0^2u_1u_2 + 2t_1^2u_0^2u_2^2 + 2t_1^2u_0u_1u_2^2 + t_1^2u_0u_2^3 +\\
&2t_1^2u_1^2u_2^2 + 2t_1^2u_1u_2^3 + t_1^2u_2^4,\\
C_{10} =& t_0u_0^5u_1 + 2t_0u_0^5u_2 + t_0u_0^4u_2^2 + t_0u_0^3u_1^3 + t_0u_0^3u_1^2u_2 + 2t_0u_0^3u_1u_2^2 +\\
&t_0u_0^3u_2^3 + 2t_0u_0^2u_0^4 + 2t_0u_0^2u_1u_2^3 + t_0u_0^2u_2^4 + t_0u_0u_1^4u_2 + t_0u_0u_1^2u_2^3 +\\
&2t_0u_0u_2^5 + 2t_0u_1^4u_2^2 + t_0u_1^3u_2^3 + t_0u_1u_2^5 + 2t_1u_0^5u_1 + t_1u_0^5u_2 + 2t_1u_0^4u_2^2 +\\
&2t_1u_0^3u_1^3 + 2t_1u_0^3u_1u_2^2 + 2t_1u_0^3u_2^3 + t_1u_0^2u_1^4 + 2t_1u_0^2u_1^3u_2 + 2t_1u_0^2u_1u_2^3 +\\
&2t_1u_0^2u_2^4 + 2t_1u_0u_1^3u_2^2 + t_1u_0u_2^5 + t_1u_1^4u_2^2 + 2t_1u_1^3u_2^3 + 2t_1u_1u_2^5,\\
C_{11} =& t_0^3t_1u_0^3u_1 + t_0^3t_1u_0u_1^3 + 2t_0^3t_1u_1^4 + t_0^3t_1u_1^3u_2 + t_0^3t_1u_1u_2^3 + t_0^2t_1^2u_0^3u_1 +\\
&2t_0^2t_1^2u_0^3u_2 + t_0^2t_1^2u_0u_1^3 + 2t_0^2t_1^2u_0u_2^3 + 2t_0^2t_1^2u_1^4 + t_0^2t_1^2u_1^3u_2 +\\
&t_0^2t_1^2u_1u_2^3 + 2t_0t_1^3u_0^3u_2 + 2t_0t_1^3u_0u_2^3,\\
C_{12} =& t_0^2t_1u_0^3u_1^2u_2 + t_0^2t_1u_0^3u_1u_2^2 + 2t_0^2t_1u_0^2u_1^3u_2 + t_0^2t_1u_0^2u_1u_2^3 + t_0^2t_1u_0u_1^4u_2 +\\
&2t_0^2t_1u_0u_1^3u_2^2 + t_0^2t_1u_0u_1^2u_2^3 + t_0t_1^2u_0^3u_1^2u_2 + t_0t_1^2u_0^3u_1u_2^2 + 2t_0t_1^2u_0^2u_1^3u_2 +\\
&at_0t_1^2u_0^2u_1u_2^3 + t_0t_1^2u_0u_1^4u_2 + 2t_0t_1^2u_0u_1^3u_2^2 + t_0t_1^2u_0u_1^2u_2^3,\\
C_{13} =& t_0^4t_1u_0^5u_1 + 2t_0^4t_1u_0^4u_1^2 + 2t_0^4t_1u_0^4u_1u_2 + 2t_0^4t_1u_0^3u_1^3 + t_0^4t_1u_0^3u_1^2u_2 +\\
&t_0^4t_1u_0^2u_1^4 + t_0^4t_1u_0^2u_1^3u_2 + t_0^4t_1u_0u_1^4u_2 + t_0^4t_1u_0u_1^3u_2^2 + t_0^4t_1u_0u_1^2u_2^3 +\\
&2t_0^4t_1u_0u_1u_2^4 + t_0^4t_1u_1^4u_2^2 + 2t_0^4t_1u_1^3u_2^3 + 2t_0^4t_1u_1^2u_2^4 + t_0^4t_1u_1u_2^5 +\\
&2t_0^3t_1^2u_0^5u_2 + 2t_0^3t_1^2u_0^3u_2^3 + 2t_0^3t_1^2u_0u_2^5 + 2t_0^2t_1^3u_0^5u_1 + t_0^2t_1^3u_0^4u_1^2 +\\
&t_0^2t_1^3u_0^4u_1u_2 + t_0^2t_1^3u_0^3u_1^3 + t_0^2t_1^3u_0^3u_1^2u_2 + 2t_0^2t_1^3u_0^3u_1u_2^2 + 2t_0^2t_1^3u_0^2u_1^4 +\\
&2t_0^2t_1^3u_0^2u_1^3u_2^2 + t_0^2t_1^3u_0u_1^4u_2 + t_0^2t_1^3u_0u_1^2u_2^3 + t_0^2t_1^3u_0u_1u_2^4 +\\
&2t_0^2t_1^3u_1^4u_2^2 + t_0^2t_1^3u_1^3u_2^3 + t_0^2t_1^3u_1^2u_2^4 + 2t_0^2t_1^3u_1u_2^5 + t_0t_1^4u_0^5u_2 +\\
&2t_0t_1^4u_0^3u_1^2u_2 + 2t_0t_1^4u_0^3u_1u_2^2 + t_0t_1^4u_0^3u_2^3 + t_0t_1^4u_0^2u_1^3u_2 + 2t_0t_1^4u_0^2u_1u_2^3 +\\
&2t_0t_1^4u_0u_1^4u_2 + t_0t_1^4u_0u_1^3u_2^2 + 2t_0t_1^4u_0u_1^2u_2^3 + t_0t_1^4u_0u_2^5.
\end{aligned}
$$

On évalue ces fonctions en t_0, t_1, u_0, u_1, u_2 et f puis on réduit le système construit grâce à la fonction `MinimalAlgebraGenerators` de `Magma`. On note

$$\begin{aligned} c_{4,3} =&(a_0a_4^2 + 2a_1a_3a_4 + 2a_2^2a_4 + a_2a_3^2)x^4 + (a_0a_3a_4 + a_1a_2a_4 + 2a_1a_3^2)x^3z + \\ &(a_0a_1a_4 + a_0a_2a_3 + 2a_1^2a_3)xz^3 + (a_0^2a_4 + 2a_0a_1a_3 + 2a_0a_2^2 + a_1^2a_2)z^4 \end{aligned}$$

un covariant de degré 3 et d'ordre 4 en caractéristique 3. On obtient alors le système de covariants séparants suivants :

$$\begin{aligned} c_{0,1} =&a_2, \\ c_{0,6} =&a_0^3a_4^3 + a_0^2a_2^2a_4^2 + a_0a_1a_2^2a_3a_4 + a_0a_2^4a_4 + 2a_0a_2^3a_3^2 + 2a_1^3a_3^3 + 2a_1^2a_2^3a_4 + a_1^2a_2^2a_3^2, \\ c_{4,1} =&\ a_0z^4 + a_1xz^3 + a_2x^2z^2 + a_3x^3z + a_4x^4, \\ c_{4,4} =&a_2c_{4,3}, \\ c_{6,3} =&(2a_0^2a_3 + 2a_0a_1a_2 + a_1^3) + (2a_0^2a_4 + a_0a_1a_3 + a_0a_2^2 + 2a_1^2a_2)x + (a_0a_1a_4 + a_0a_2a_3 + 2a_1^2a_3)x^2 + \\ &(a_0a_3^2 + 2a_1^2a_4)x^3 + (2a_0a_3a_4 + 2a_1a_2a_4 + a_1a_3^2)x^4 + (a_0a_4^2 + 2a_1a_3a_4 + 2a_2^2a_4 + a_2a_3^2)x^5 + \\ &(a_1a_4^2 + a_2a_3a_4 + 2a_3^3)x^6, \\ c_{8,4} =&c_{4,1}(c_{4,3} - a_2^2c_{4,1}), \\ c_{8,6} =&(c_{4,3} - a_2^2c_{4,1})c_{4,3}. \end{aligned}$$

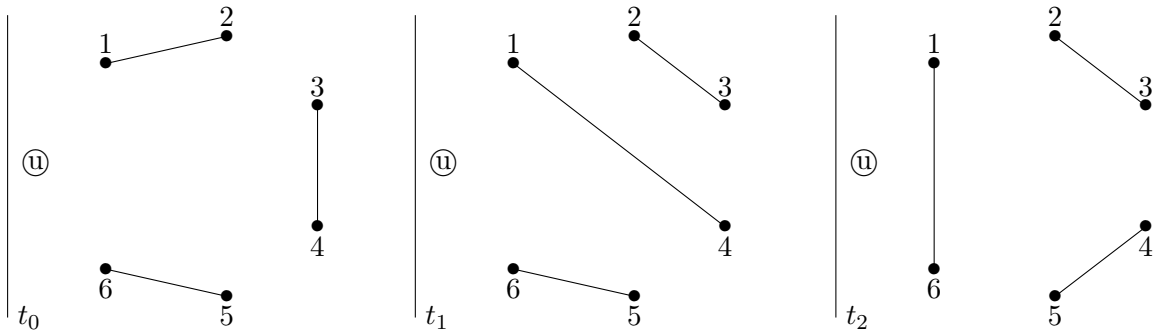
On retrouve bien les résultats de la thèse de Basson pour les invariants. Ce système n'est pas un système générateur de l'algèbre des covariants car il ne permet pas de trouver $c_{4,3}$ comme polynôme des autres $c_{2i,j}$. Ce cas de figure fournit un exemple où un sous-ensemble séparant n'est pas sysème générateur de l'algèbre des covariants. On constate que $\{c_{0,1}, c_{0,6}, c_{4,1}, c_{4,3}, c_{6,3}\}$ est également un système séparant de l'algèbre $\mathcal{C}_4$ et on peut se demander si ce dernier est également un système générateur. Le théorème [DK02, Th.2.3.12] permettrait en théorie de tester cette hypothèse mais en pratique les calculs n'aboutissent pas.

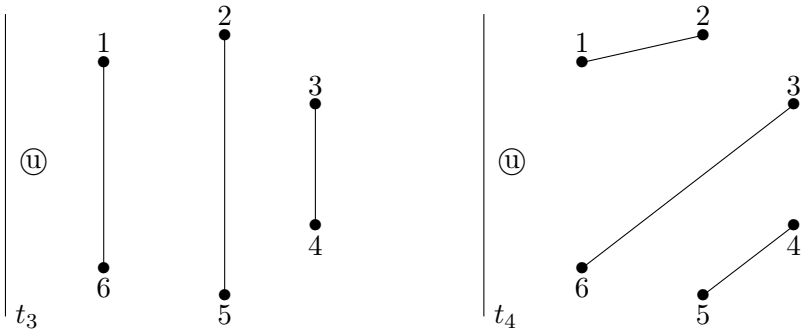
5.2.4 Calcul de $\mathcal{B}_{reg}(6)$ avec l'approche graphique

On va exploiter les 5 points de la section 5.2.1 pour construire un système de générateurs de $\mathcal{B}_{reg}(6)$. Le point 5 (p. 62) permet de séparer les cas selon l'ordre du covariant de 6 points. Il permet de considérer seulement les ordres 0, 2, 4, 6, 8, 10 et 12.

5.2.4.1 Formes sextiques, ordre 0

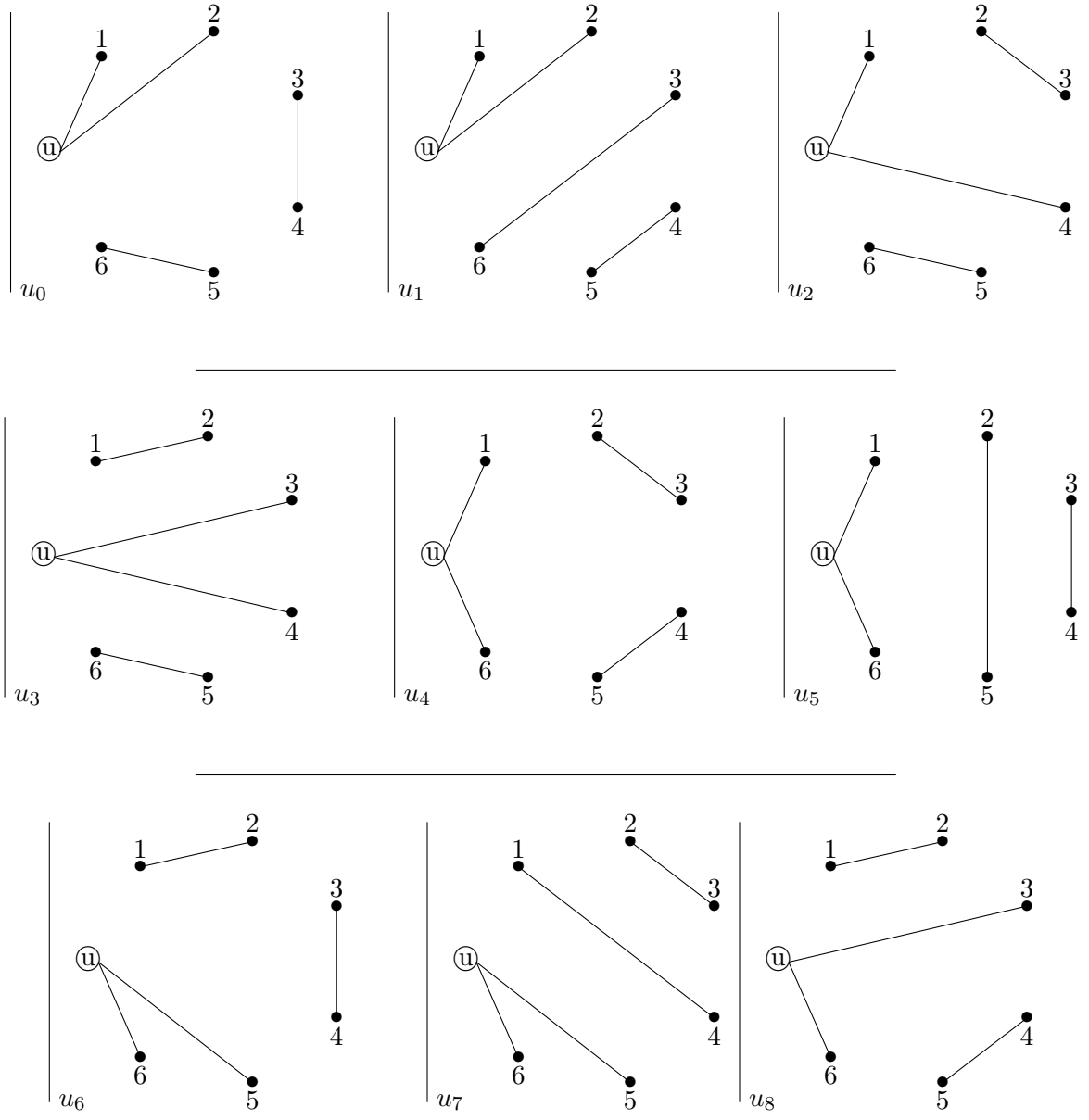
Tout d'abord, grâce au point 2 (p. 62), on considère uniquement les graphes de degré de régularité 1. Ensuite, l'utilisation du point 1 (p. 62) réduit le système de générateurs à 15 graphes. Enfin, le point 4 (p. 62) permet de se ramener aux 5 graphes donnés ci-dessous.





5.2.4.2 Formes sextiques, ordre 2

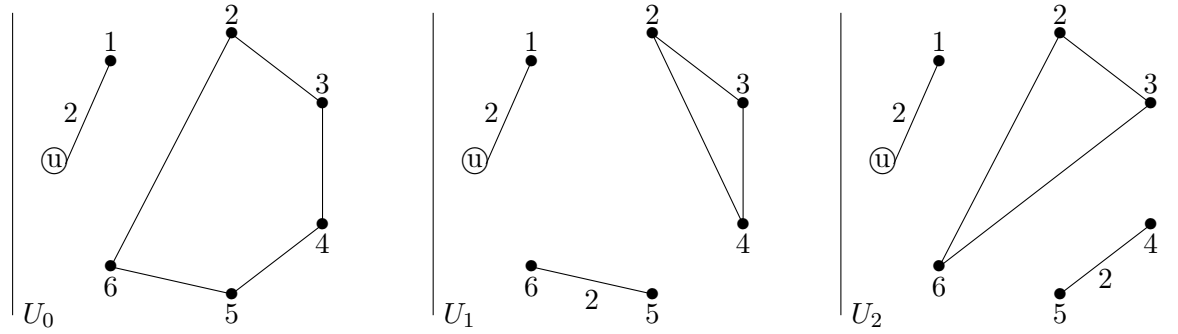
Grâce aux points 1 à 5 (p. 62), on obtient 27 graphes satisfaisant ces propriétés. Les 9 graphes de degré de régularité 1 sont présentés ci-dessous.

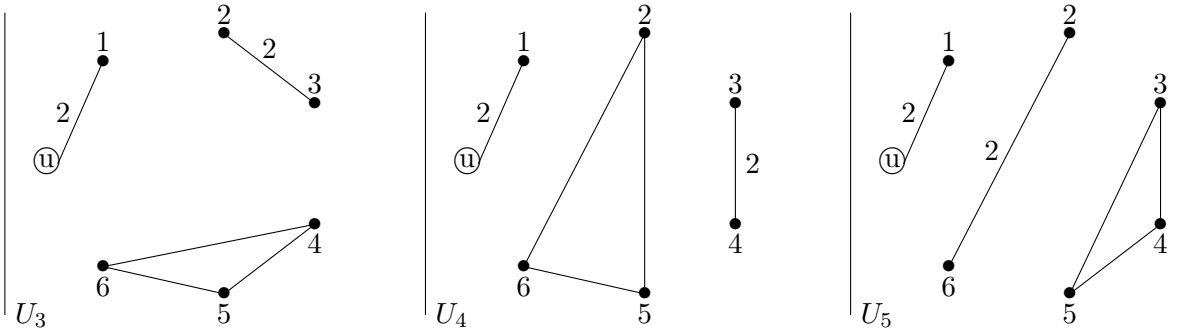


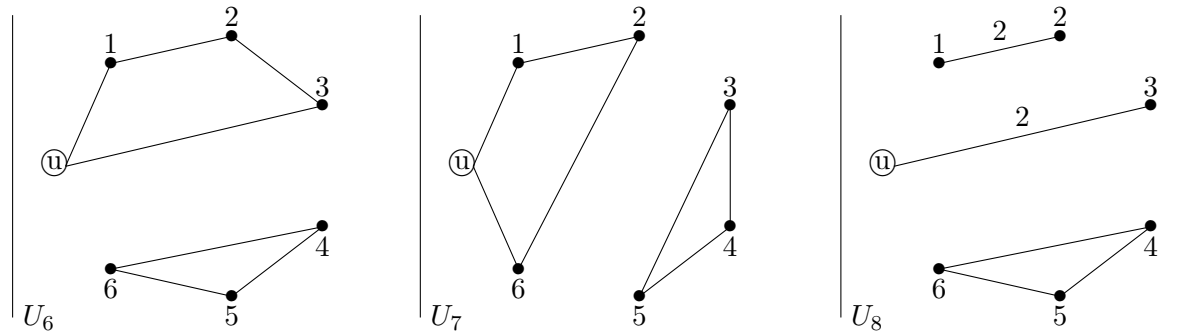
Pour le degré de régularité 2, il y a :
— 4 graphes composés d'un triangle de trois chiffres consécutifs et d'un quadrilatère,
— 2 graphes composés d'un pentagone et d'une double arête reliée à ⓤ,

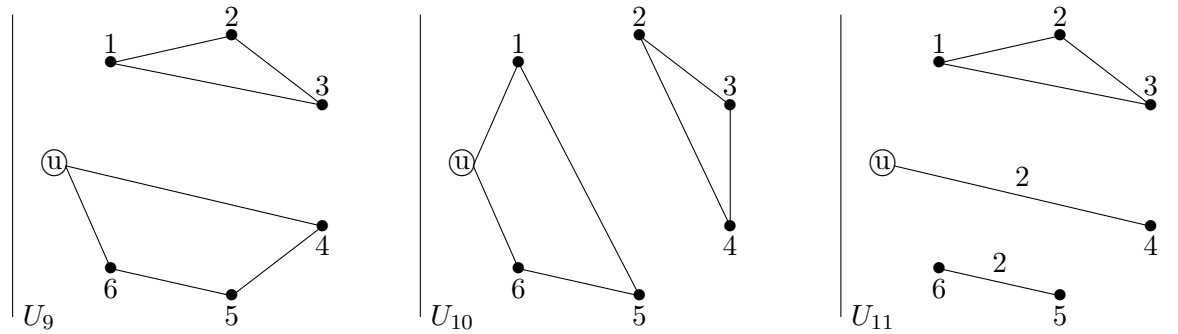
— 12 graphes composés d'un triangle reliant des sommets numérotés et de deux doubles arêtes disjointes.

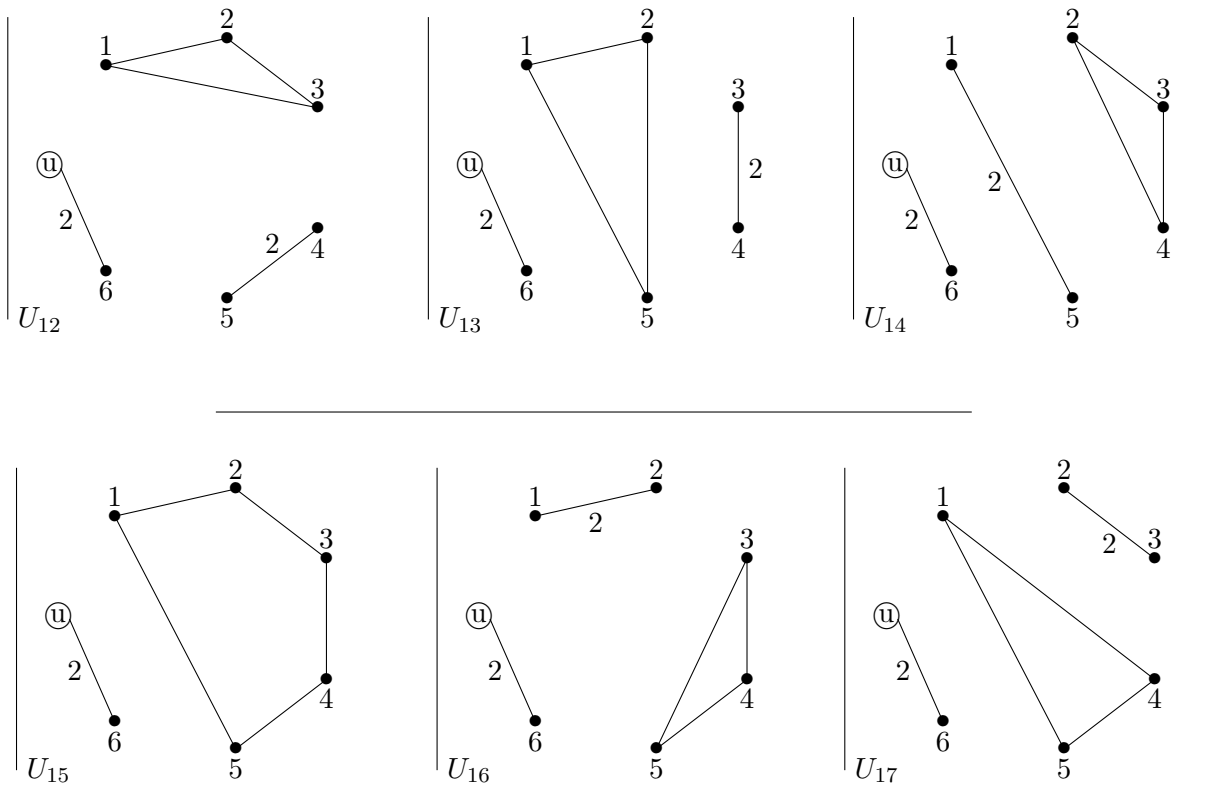
Ces graphes sont les suivants :









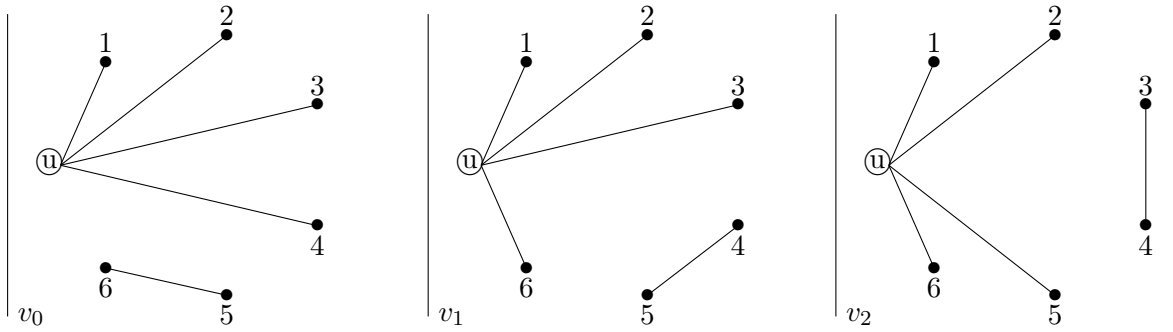


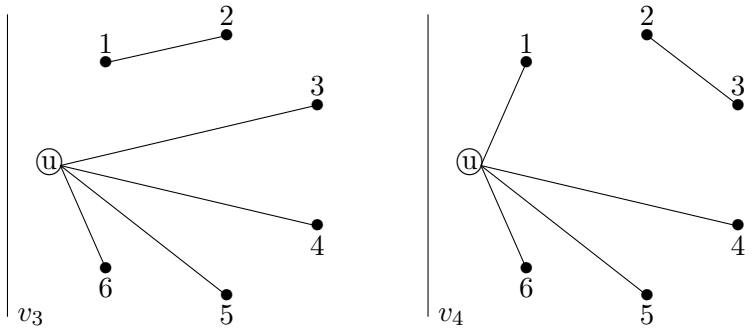
Ces 18 graphes correspondent à 18 covariants de 6 points réductibles et peuvent s'exprimer en fonction des u_i et t_j de la façon suivante :

$$\begin{aligned}
U_0 =& u_0t_2 - u_4t_0\\
U_1 =& u_0t_1 - u_2t_0\\
U_2 =& u_1t_2 - u_4t_4\\
U_3 =& u_2t_2 - u_4t_1\\
U_4 =& u_0t_3 - u_5t_0\\
U_5 =& u_4t_0 - u_5t_4 + u_1t_3 - u_0t_2\\
U_6 =& u_2t_4 - u_4t_0\\
U_7 =& u_5t_4 - u_4t_0\\
U_8 =& u_3t_4 - u_8t_0\\
U_9 =& u_8t_1 - u_4t_0\\
U_{10} =& u_5t_1 - u_4t_0\\
U_{11} =& u_3t_1 - u_2t_0\\
U_{12} =& u_8t_2 - u_4t_4\\
U_{13} =& u_6t_3 - u_5t_0\\
U_{14} =& u_4t_0 - u_5t_1 + u_7t_3 - u_6t_2\\
U_{15} =& u_6t_2 - u_4t_0\\
U_{16} =& u_6t_4 - u_8t_0\\
U_{17} =& u_7t_2 - u_4t_1
\end{aligned}$$

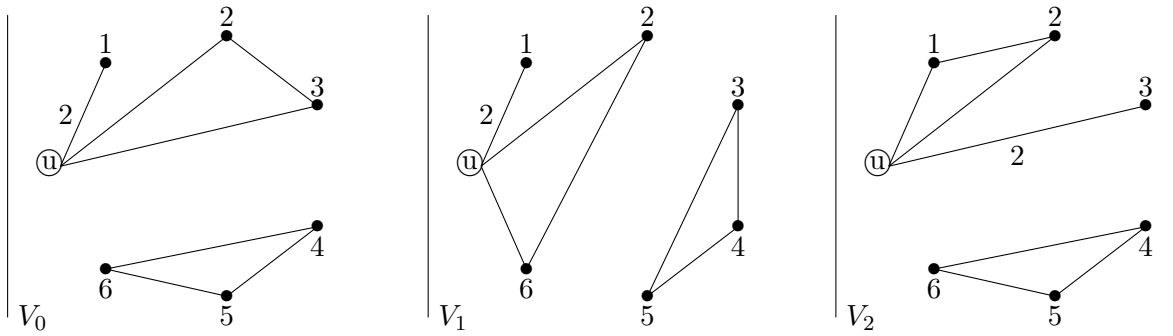
5.2.4.3 Formes sextiques, ordre 4

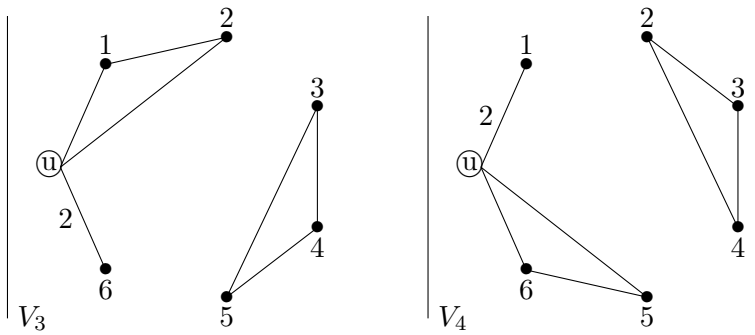
Grâce aux points 1 à 5 (p. 62), on construit 5 graphes de degré de régularité 1 et 8 de degré de régularité 2. Ci-dessous les 5 graphes de degré 1.

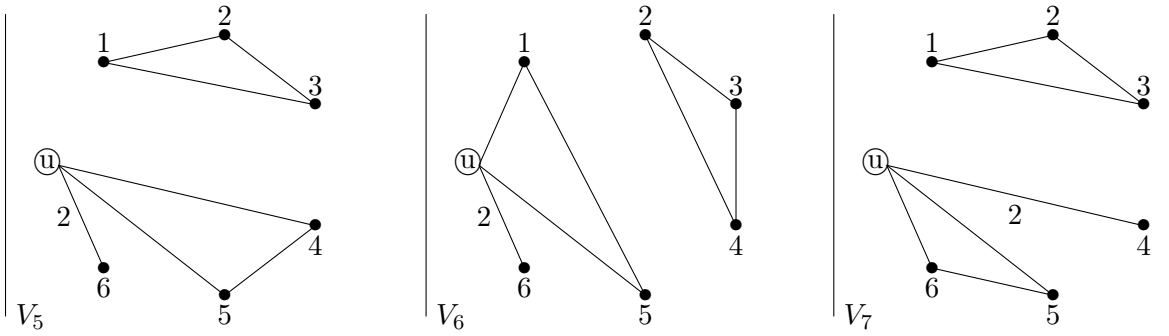




Pour le degré de régularité 2, les 8 graphes sont les suivants :





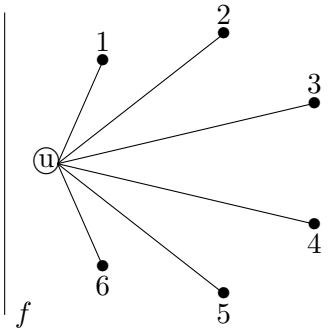


Ces covariants de 6 points sont réductibles, comme le montrent les relations suivantes :

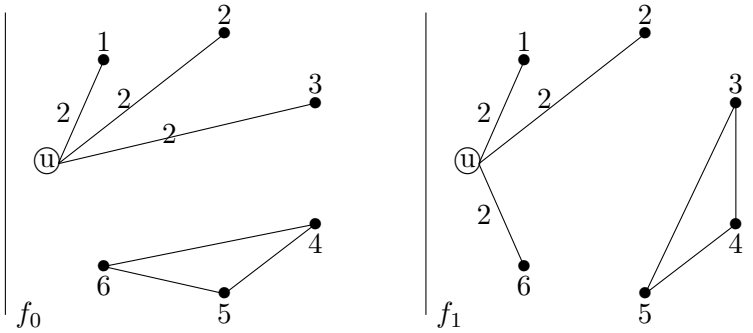
$$\begin{aligned}
V_0 =& v_0t_2 - v_1t_1\\
V_1 =& v_1(t_0 + t_3) - v_2(t_2 + t_4)\\
V_2 =& v_0t_4 - v_1t_0\\
V_3 =& v_2t_4 - v_1t_0\\
V_4 =& v_2t_1 - v_4t_0\\
V_5 =& v_3t_2 - v_4t_4\\
V_6 =& v_4(t_0 + t_3) - v_2(t_2 + t_1)\\
V_7 =& v_4t_0 - v_3t_1
\end{aligned}$$

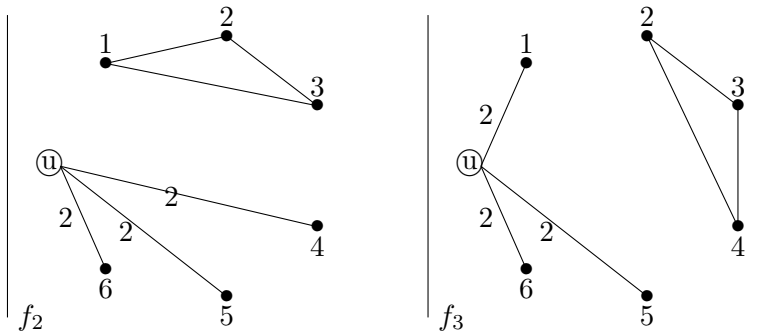
5.2.4.4 Forme sextique : ordre 6

Un seul covariant de 6 points d'ordre 6 et de degré 1 satisfait les points 1 à 5 (p. 62). Il correspond à la forme f et sa représentation graphique est :



4 covariants de 6 points de degré 2 et d'ordre 6 satisfont aussi les points 1 à 5 (p. 62). Ci-dessous les graphes associés.





Ces graphes correspondent à 4 covariants de 6 points réductibles. Voici leur expression en fonction de covariants de degré inférieur :

$$\begin{aligned} f_0 &= v_0u_1 - u_0v_1 \\ f_1 &= v_2u_1 - v_1u_0 \\ f_2 &= v_3u_7 - v_4u_6 \\ f_3 &= u_7v_2 - u_6v_4 \end{aligned}$$

5.2.4.5 Forme sextique : ordre ≥ 8

Pour les ordres supérieurs, aucun graphe ne vérifie simultanément les points 1 à 5 (p. 62).

En résumé, on a calculé 20 générateurs de l'algèbre des covariants de 6 points. Il s'agit de tous les éléments de degré de régularité 1 calculés.

Remarque 17. *Il est curieux que l'on ai seulement des générateurs de degré de régularité* 1 *comme dans le cas des invariants. C'est également le cas pour les covariants des quartiques. On peut se demander s'il est possible d'améliorer le résultat de Kempe cité dans le théorème 8 (p. 60).*

À présent, on va faire agir le groupe $\mathcal{S}_6$ sur ces covariants pour tenter de retrouver l'algèbre des covariants d'une forme binaire. Dans ce but, on va d'abord chercher à retrouver l'algèbre des invariants.

5.2.5 Invariants de formes sextiques

On cherche à identifier un système d'invariants séparant de $\mathcal{I}_6$ à partir des invariants t_0, t_1, t_2, t_3 et t_4 de 6 points en caractéristique 3 et 5. Pour cela, on va faire agir le groupe $\mathcal{S}_6$ sur l'algèbre construite sur ces invariants. Sachant que $\mathcal{S}_6$ est généré par la transposition $\tau = (12)$ et le 6-cycle $\sigma = (123456)$, l'action de $\mathcal{S}_6$ sur les racines est entièrement décrite par :

$$\begin{array}{lll} t_0^\tau = -t_0 & et & t_0^\sigma = -t_2 \\ t_1^\tau = t_1 + t_0 & et & t_1^\sigma = -t_3 \\ t_2^\tau = t_2 + t_4 & et & t_2^\sigma = -t_0 \\ t_3^\tau = t_0 + t_3 & et & t_3^\sigma = -t_4 \\ t_4^\tau = -t_4 & et & t_4^\sigma = -t_1 \end{array}$$

On commence par étudier le cas de la caractéristique 3. Grâce aux fonctions `PrimaryInvariants` et `SecondaryInvariants` de `magma` on obtient 5 invariants primaires I_2, I_4, I_6, I_6' et I_{10} de degré respectivement 2, 4, 6, 6 et 10 ainsi que 3 invariants secondaires I_8, I_{18} et I_{23} de degré respectivement 8, 18 et 23. On ne les écrit pas pas car leur expression en fonction de t_0, t_1, t_2, t_3 et t_4 est très longue. Ensuite on exprime ces invariants comme combinaison linéaire des invariants d'Igusa (J_2, J_4, J_6 et J_{10}) et de $\mathcal{R}$. On fait ceci grâce à une stratégie dévaluation similaire à

[LR12]. Ensuite, on vérifie formellement que notre combinason linéaire est la bonne. Au final on obtient :

$$\begin{aligned}
I_2 &= J_2,\\
I_4 &= J_2^2 - J_4,\\
I_6 &= 0,\\
I_6' &= J_4J_2 - J_6,\\
I_{10} &= J_2^5 - J_2^3J_4 - J_2^2J_6 - J_2J_4^2 - J_4J_6 + J_{10},\\
I_8 &= J_2^4 - J_2^2J_4 + J_2J_6 + J_4^2,\\
I_{18} &= 0,\\
I_{23} &= 2\,\mathcal{R}\,J_2^2J_4.
\end{aligned}$$

On se réfère à l'annexe B.3.4 pour le détail du calcul. On ne retrouve pas directement dans ce cas un système générateur de l'algèbre des invariants. En effet, on est obligé de factoriser I_{23} pour retrouver l'invariant $\mathcal{R}$ de degré 15. Ceci est en accord avec le fait qu'on obtient a priori simplement un ensemble de séparants.

Par le même raisonnement, en caractéristique 5, on obtient 5 invariants primaires I_2, I_4, I_6, I_6' et I_{10} de degré respectivement 2, 4, 6, 6 et 10 ainsi que 3 invariants secondaires I_8, I_{15} et I_{23} de degré respectivement 8, 18 et 15. Leurs expression en fonction des invariants d'Igusa sont les suivantes :

$$\begin{aligned}
I_2 &= J_2,\\
I_4 &= J_4,\\
I_6 &= J_2^3 + J_2J_4 + 3J_6,\\
I_6' &= J_2J_4 + J_6,\\
I_{10} &= 4J_{10},\\
I_8 &= J_2^4 + 4J_2^2J_4 + J_2J_6 + 3J_4^2,\\
I_{15} &= 3\,\mathcal{R},\\
I_{23} &= 3\,\mathcal{R}(J_2^4 + 3J_2^2J_4 + J_2J_6 + 2J_4^2),
\end{aligned}$$

On se réfère à l'annexe B.3.4 pour le détail du calcul. Dans ce cas l'ensemble séparant est un système générateur de $\mathcal{I}_6$. On retrouve ainsi dans ce cas exactement les résultats d'Igusa.

5.2.6 Covariants de formes sextiques

Afin de construire un système générateur pour l'algèbre des covariants, on souhaiterait généraliser la méthode précédente pour le calcul des covariants. On a vu que les covariants de 6 points sont engendrés par 20 covariants de 6 points. Ces derniers sont donnés par tous les éléments de degré de régularité 1 qu'on a calculé (à l'exeption de u_3, u_{10}, u_{11} et v_3). On va faire agir le groupe $\mathcal{S}_6$ sur l'algèbre engendré par ces covariants et identifier les invariants sous cette action. On sait que $\mathcal{S}_6$ est engendré par la transposition $\tau = (12)$ et le 6-cycle $\sigma = (123456)$. Par l'action de τ

et σ sur les racines, on obtient ainsi :

$$\begin{array}{lll}
t_0^\tau = -t_0 & et & t_0^\sigma = -t_2 \\
t_1^\tau = t_1 + t_0 & et & t_1^\sigma = -t_3 \\
t_2^\tau = t_2 + t_4 & et & t_2^\sigma = -t_0 \\
t_3^\tau = t_0 + t_3 & et & t_3^\sigma = -t_4 \\
t_4^\tau = -t_4 & et & t_4^\sigma = -t_1 \\
u_0^\tau = u_0 & et & u_0^\sigma = -u_1 - u_4 - u_8 \\
u_1^\tau = u_1 & et & u_1^\sigma = -u_0 - u_2 - u_3 \\
u_2^\tau = u_2 + u_3 & et & u_2^\sigma = -u_0 - u_5 - u_6 \\
u_3^\tau = -u_3 & et & u_3^\sigma = -u_2 - u_4 - u_7 \\
u_4^\tau = u_4 + u_8 & et & u_4^\sigma = u_0 \\
u_5^\tau = u_5 + u_6 & et & u_5^\sigma = u_1 \\
u_6^\tau = -u_6 & et & u_6^\sigma = u_4 \\
u_7^\tau = u_6 + u_7 & et & u_7^\sigma = u_5 \\
u_8^\tau = -u_8 & et & u_8^\sigma = u_2 \\
v_0^\tau = v_0 & et & v_0^\sigma = -v_0 - v_1 - v_2 - v_3 - v_4 \\
v_1^\tau = v_1 & et & v_1^\sigma = v_0 \\
v_2^\tau = v_2 & et & v_2^\sigma = v_1 \\
v_3^\tau = -v_3 & et & v_3^\sigma = v_4 \\
v_4^\tau = v_3 + v_4 & et & v_4^\sigma = v_2 \\
f^\tau = f & et & f^\sigma = f
\end{array}$$

Déterminer les générateurs de l'algèbre des invariants sous cette action est coûteux et n'aboutit pas par une utilisation basique des fonctions existante de `Magma`. Toutefois, on peut quand même produire certains résultats partiels en petite caractéristique. On retrouve ainsi le covariant c d'ordre 2 et de degré 1 en caractéristique 5 de la section 6.6.2.3, comme l'indique l'égalité suivante :

$$c := a_4x^2 + 3a_3xz + a_2z^2 = 2u_0 + u_1 + 3u_2 + 4u_3 + u_4 + 3u_5 + 2u_6 + u_7 + 3u_8.$$

D'autre part, on construit un covariant d'ordre 4 et de degré 1 en caractéristique 3 qui n'est pas la réduction d'un covariant en caractéristique 0 :

$$q = 2v_0 + v_1 + v_3 + 2v_4 = 2a_1z^4 + a_2xz^3 + 2a_4x^3z + a_5x^4.$$

5.3 Une nouvelle méthode de construction de covariants en caractéristique impaire

Nous introduisons ici une nouvelle opération pour construire des covariants en petite caractéristique. Pour montrer la validité de notre démarche, notre première idée était d'utiliser la caractérisation différentielle des covariants, comme dans [Hil93, p.43]. Il s'avère cependant que le résultat de Hilbert (théorème 12 (p. 80)), démontré originellement en caractéristique 0 admet des contre-exemples en petite caractéristique, comme nous le verrons dans la section 5.3.2. Nous avons donc abordé la preuve de la proposition 13 (p. 80) directement. Dans la suite f est une forme binaire définie sur corps k

$$f = \sum_{i=0}^{n} a_i x^i z^{n-i}$$

5.3.1 Définitions et propriétés

Soient :
— $k[a_0, \ldots, a_n]_d$ l'algèbre des polynômes homogènes de degré d,
— $\mathbb{T}$ le sous-groupe des matrices diagonales de $\mathrm{SL}_2(k)$,
— Γ le sous-groupe des matrices triangulaires supérieures et de diagonale égale à 1 de $\mathrm{SL}_2(k)$,
— Γ^* le sous-groupe des matrices triangulaires inférieures et de diagonale égale à 1 de $\mathrm{SL}_2(k)$.
Ces sous-groupes sont importants car ils engendrent $\mathrm{SL}_2(k)$ et permettent ainsi de décomposer les questions d'invariance sous l'action de ce groupe.

Dans la suite I désigne un élément non nul de $k[a_0, \ldots, a_n]$.

Définition 28. *Soit $M = a_0^{\rho_0} a_1^{\rho_1} \ldots, a_n^{\rho_n}$, on définit le poids de M par*

$$w = \sum_{i=0}^{n} i\rho_i.$$

On dit que I est isobare *si tous ses monômes ont le même poids.*

On va définir deux opérateurs différentiels sur I qui conservent le degré.

Définition 29. *Les opérateurs $\boldsymbol{\Delta}$ et $\boldsymbol{D}$ sont donnés par :*

$$\boldsymbol{\Delta} = \sum_{i=1}^{n} i a_i \frac{\partial}{\partial a_{i-1}}$$

$$\boldsymbol{D} = \sum_{i=0}^{n-1} (n-i) a_i \frac{\partial}{\partial a_{i+1}}.$$

Remarque 18. *Si I est isobare de poids p en les coefficients de f, alors $\boldsymbol{\Delta} I$ est isobare de poids $p+1$.*
Si I est isobare de poids p en les coefficients de f, alors $\boldsymbol{D} I$ est isobare de poids $p-1$.

Ces affirmations se démontrent assez facilement en posant les calculs.

Remarque 19. *Puisque $\boldsymbol{\Delta}$ et $\boldsymbol{D}$ sont des opérateurs différentiels linéaires, pour tout I_1, $I_2 \in K[a_0, \ldots a_n]$*

1.
$$\boldsymbol{\Delta}(I_1 + I_2) = \boldsymbol{\Delta} I_1 + \boldsymbol{\Delta} I_2,$$
$$\boldsymbol{D}(I_1 + I_2) = \boldsymbol{D} I_1 + \boldsymbol{D} I_2,$$

2.
$$\boldsymbol{\Delta}(I_1 I_2) = (\boldsymbol{\Delta} I_1) I_2 + I_1 \boldsymbol{\Delta} I_2,$$
$$\boldsymbol{D}(I_1 I_2) = (\boldsymbol{D} I_1) I_2 + I_1 \boldsymbol{D} I_2.$$

Ces égalités amènent la proposition suivante :

Proposition 22. *Si I est isobare de poids w et homogène de degré d, alors*

$$(\boldsymbol{D}\boldsymbol{\Delta} - \boldsymbol{\Delta}\boldsymbol{D}) I = (nd - 2w) I. \tag{5.3.1}$$

Démonstration. On va présenter les trois principales idées de la preuve.

1. Le résultat est clairement vrai si I est constant. Si I est l'un des a_i, alors
$$(\mathbf{D}\boldsymbol{\Delta} - \boldsymbol{\Delta}\mathbf{D})a_i =$$
$$(i+1)\mathbf{D}a_{i+1} - (n-i-1)\boldsymbol{\Delta}a_{i-1} = (i+1(n-i) - (n-i-1)i)a_i = (n-2i)a_i.$$
Le résultat est alors démontré car a_i est de poids i et de degré 1.
2. En utilisant les formules de la remarque 19 (p. 76), on montre que le résultat est vrai pour le produit $a_i a_j$. Par récurrence immédiate, cela reste vrai pour les monômes.
3. Si on choisit deux monômes de même poids et de même degré, la somme vérifie encore l'identité car le coefficient $nd-2w$ est le même pour les deux termes. Ainsi, par récurrence immédiate, n'importe quel polynôme isobare et homogène verifie l'identité (5.3.1).

□

Plus généralement, avec les mêmes hypothèses, on a le résultat suivant :

Proposition 23. *Soit $l > 0$ un entier naturel.*
$$(\boldsymbol{D}^l\boldsymbol{\Delta} - \boldsymbol{\Delta}\boldsymbol{D}^l) = l(nd - 2w + l - 1)\boldsymbol{D}^{l-1}, \tag{5.3.2}$$
$$(\boldsymbol{D}\boldsymbol{\Delta}^l - \boldsymbol{\Delta}^l\boldsymbol{D}) = l(nd - 2w - l + 1)\boldsymbol{\Delta}^{l-1}. \tag{5.3.3}$$

Démonstration. Les résultat (5.3.2) et (5.3.3) se traitent de façon analogue. Par conséquence, on va uniquement détailler le (5.3.2). Ce résultat se démontre par récurrence sur l'entier l. La proposition 22 (p. 76) assure la validité du résultat au rang initial.
Soit l tel que (5.3.2) soit vérifié. On applique d'abord l'opérateur $\mathbf{D}$ à (5.3.2) :
$$\mathbf{D}^{l+1}\boldsymbol{\Delta} - \mathbf{D}\boldsymbol{\Delta}\mathbf{D}^l = l(nd - 2w + l - 1)\mathbf{D}^l.$$
Puis, la formule (5.3.1) à $\mathbf{D}^l$. Grâce à la remarque 18 (p. 76), on obtient :
$$\mathbf{D}\boldsymbol{\Delta}\mathbf{D}^l - \boldsymbol{\Delta}\mathbf{D}^{l+1} = (nd - 2(w-l))\mathbf{D}^l.$$
Ainsi, par somme :
$$\begin{aligned}\mathbf{D}^{l+1}\boldsymbol{\Delta} - \boldsymbol{\Delta}\mathbf{D}^{l+1} &= (l(nd - 2w + l - 1) + (nd - 2(w-l)))\mathbf{D}^l \\ &= (l+1)(nd - 2w + (l+1) - 1)\mathbf{D}^l.\end{aligned}$$

□

5.3.2 Conditions nécessaires et suffisantes pour avoir un covariant

Soit $C \in k[a_0, \ldots, a_n][x, z]$ un polynôme homogène en (x, z) de degré m tel que
$$C = \sum_{i=0}^{m} C_i x^i z^{m-i}$$
avec $C_i \in k[a_0, \ldots, a_n]$ homogènes de même degré d. Le but est de donner une condition nécessaire et suffisante pour que C soit un covariant sous l'action de $\mathrm{SL}_2(k)$. Pour cela, on exploite la notion de poids ainsi que les opérateurs $\boldsymbol{\Delta}$ et $\mathbf{D}$. Ce travail s'effectue en trois temps en adaptant la preuve que Hilbert a donnée en caractéristique 0. D'abord, on montre une condition nécessaire et suffisante pour que C soit un covariant sous l'action de $\mathbb{T}$ (lemme 6 (p. 78)). Ce résultat est valide en caractéristique quelconque. Par contre les résultats d'invariance sous l'action de Γ et sous celle de Γ^* admettent des contre-exemples en petite caractéristique et le résultat final n'est donc pas valable en toute caractéristique.

Soit $M \in \mathrm{SL}_2(k)$. On a $f(M.(x,z)) = \sum_{i=0}^{n} a'_i x^i z^{n-i}$. Dans la suite on notera $X = (x, z)$, $X' = M^{-1}(x, z)$ et $a' = (a'_0, \ldots, a'_n)$.

Lemme 6. *C est un covariant sous l'action de $\mathbb{T}$ si et seulement si les C_i sont isobares de poids $w+i$ et $nd-2w=m$.*

Démonstration. Si $M=\left(\begin{smallmatrix}\lambda^{-1} & 0\\ 0 & \lambda\end{smallmatrix}\right)\in\mathbb{T}$, alors $a'_i=\lambda^{n-2i}a_i$ et $C_l(a')=\sum_{i=1}^{l}\prod_{j=0}^{n}{a'_j}^{\epsilon_{i,j,l}}$ (resp. $C_l(a)=\sum_{i=1}^{l}\prod_{j=0}^{n}{a_j}^{\epsilon_{i,j,l}}$) avec $l\in\{0,\dots,m\}$. On a

$$\begin{aligned}C_l(a')=\sum_{i=1}^{l}\prod_{j=0}^{n}\lambda^{(n-2j)\epsilon_{i,j,l}}{a_j}^{\epsilon_{i,j,l}}&=\sum_{i=1}^{l}\lambda^{\sum_{j=0}^{n}(n-2j)\epsilon_{i,j,l}}\prod_{j=0}^{n}{a_j}^{\epsilon_{i,j,l}}\\&=\sum_{i=1}^{l}\lambda^{nd-2\sum_{j=0}^{n}j\epsilon_{i,j,l}}\prod_{j=0}^{n}{a_j}^{\epsilon_{i,j,l}}.\end{aligned}$$

Puisque M agit aussi sur (x,z) par $M^{-1}.(x,z)$, on obtient

$$M.C(a,X)=C(a'_0,\dots,a'_n,\lambda x,\lambda^{-1}z)=\sum_{l=0}^{m}\lambda^{2l-m}C_l(a')x^lz^{m-l}.$$

On suppose que C soit un covariant, alors $M.C=C$, donc pour tout $l\in\{0,\dots,m\}$

$$C(a)=\lambda^{2l-m}C_l(a').$$

Cela entraine que pour tout l et pour tout i

$$nd-2\sum_{j=0}^{n}j\epsilon_{i,j,l}+2l-m=0.$$

En particulier, $\sum_{j=0}^{n}j\epsilon_{i,j,l}-l$ ne dépend ni de l ni de i. Ainsi, on peut bien définir w en posant $w=\sum_{j=0}^{n}j\epsilon_{i,j,l}-l$. On obtient alors $nd-2w=m$. De plus, l'entier w est le poids de C_0. Le poids de C_l est $\sum_{j=0}^{n}j\epsilon_{i,j,l}=w+l$.
Réciproquement on cherche à montrer que $C_l(a)=\lambda^{2l-m}C_l(a')$. Puisque le poids de C_l est $\sum_{j=0}^{n}j\epsilon_{i,j,l}$, on a $w=\sum_{j=0}^{n}j\epsilon_{i,j,l}-l$. De plus, $nd-2w=m$, d'où :

$$nd-2\sum_{j=0}^{n}j\epsilon_{i,j,l}+2l-m=0.$$

Ceci entraine que :

$$C_l(a)=\lambda^{2l-m}C_l(a').$$

Ainsi, C est un covariant sous l'action de $\mathbb{T}$. □

Puisqu'à partir de C_0, on retrouve le poids des C_i du covariant C, on dit que C est de poids w.

Malheureusement les opérateurs différentiels se comportent mal en caractéristique p et le résultat de Hilbert suivant n'est valable qu'en caractéristique p nulle ou large.

Lemme 7. *Supposons $p=0$ ou $p>nd+m$. Le polynôme C est un covariant sous Γ si et seulement si*

$$\mathbf{\Delta}C=z\frac{\partial C}{\partial x}.$$

Démonstration. Si $M=\left(\begin{smallmatrix}1 & \mu\\ 0 & 1\end{smallmatrix}\right)\in\Gamma$, alors $f(M.(x,z))=\sum_{i=0}^{n}a'_ix^iz^{n-i}$ avec

$$a'_i=\sum_{j=i}^{n}\mu^{j-i}a_j\binom{j}{j-i}.$$

On a $X' = (x', z') = (x - \mu z, z)$. Clairement $C(a', X')$ est un polynôme en μ de degré au plus $nd + m$ en μ. On dérive a'_{i-1} par rapport à μ

$$\frac{\partial a'_{i-1}}{\partial \mu} = \sum_{j=i-1}^{n} (j - i + 1)\mu^{j-i} a_j \binom{j}{j-i+1} = \sum_{j=i}^{n} i\mu^{j-i} a_j \binom{j}{j-i} = i a'_i.$$

On dérive C par rapport à μ

$$\frac{\partial C(a', X')}{\partial \mu} = \sum_{i=0}^{n} \Big(\frac{\partial C(a', X')}{\partial a'_i} \frac{\partial a'_i}{\partial \mu} \Big) + \frac{\partial C(a', X')}{\partial x'} \frac{\partial x'}{\partial \mu} + \frac{\partial C(a', z')}{\partial z'} \frac{\partial z'}{\partial \mu}.$$

Comme a'_n et z' ne dépendent pas de μ et grâce aux deux formules précédentes, on obtient :

$$\frac{\partial C(a', X')}{\partial \mu} = \sum_{i=0}^{n-1} \frac{\partial C(a', X')}{\partial a'_i} (i+1) a'_{i+1} - \frac{\partial C(a', X')}{\partial x'} z = \mathbf{\Delta} C(a', X') - \frac{\partial C(a', X')}{\partial x'} z.$$

De plus, $\frac{\partial x}{\partial x'} = 1$ entraine que :

$$\frac{\partial C(a', X')}{\partial \mu} = \mathbf{\Delta} C(a', X') - \frac{\partial C(a', X')}{\partial x} z.$$

On suppose que C soit un covariant, alors $C(a', X') = C(a, X)$, d'où :

$$\frac{\partial C(a', X')}{\partial \mu} = 0.$$

Ainsi,

$$\mathbf{\Delta} C(a, X) = \frac{\partial C(a, X)}{\partial x} z.$$

Réciproquement, puisque $\mathbf{\Delta} C(a', X') = \frac{\partial C(a', X')}{\partial x} z$:

$$\frac{\partial C(a', X')}{\partial \mu} = 0.$$

$C(a', X')$, ne dépend donc pas de μ. En remplaçant μ par 0, on obtient $C(a', X') = C(a, X)$ et le résultat est démontré. □

Le résultat suivant se démontre de manière analogue.

Lemme 8. *Supposons $p = 0$ ou $p > nd + m$. C est un covariant sous Γ^* si et seulement si*

$$\boldsymbol{D} C = x \frac{\partial C}{\partial z}.$$

Enfin, puisque $\mathrm{SL}_2(k)$ est engendré par $\mathbb{T}$, Γ et Γ^*, ces trois dernières propositions justifient le résultat ci-dessous.

Théorème 12. *Supposons $p = 0$ ou $p > nd + m$. Le polynôme $C = \sum_{i=0}^{m} C_i x^i z^{m-i}$ est un covariant de la forme f sous l'action de $\mathrm{SL}_2(k)$ si et seulement si les conditions suivantes sont satisfaites :*

1. *$C_0, \ldots, C_m$ sont des fonctions homogènes de degré d et isobares de poids $w, w+1, \ldots, w+m$ avec $nd - 2w = m$,*
2. *$\boldsymbol{D} C = x \frac{\partial C}{\partial z}$,*

3. $\mathbf{\Delta}C = z\frac{\partial C}{\partial x}$.

Remarque 20. *Ce résultat n'est pas vrai en petite caractéristique. Considérons* $f = \sum_{i=0}^{16} a_i x^i z^{16-i}$ *une forme binaire de degré* $n = 16$ *en caractéristique* 3. *On pose* $C = a_{11}x^6$ *un polynôme homogène de degré* $m = 6$. *Le polynôme* C *n'est pas un covariant de* f *car pour* $M = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(k)$ *on a*

$$C(M.f, M.(x,z)) = (x+2z)^6(a_{11}+a_{14}) \neq C.$$

Or

1. $C_0, \ldots, C_m$ *sont des fonctions homogènes de degré* 1 *et isobares de poids* $w = 5, 6, \ldots, 11$ *avec* $nd - 2w = 16 \cdot 1 - 2 \cdot 5 = 6 = m$,
2. $\boldsymbol{D}C = 6a_{10}x^6 = 0 = x\frac{\partial C}{\partial z}$,
3. $\mathbf{\Delta}C = 12a_6x^6 = 0 = z\frac{\partial C}{\partial x}$.

5.3.2.1 Une nouvelle opération sur les covariants en caractéristique positive

Théorème 13. *Soient* $\mathcal{Q} = \sum_{i=0}^{m_0} \mathcal{Q}_i x^i z^{m_0-i}$ *un covariant de* f *d'ordre* m_0, *de degré* d_0 *et de poids* ω_0 *et* l *un entier plus petit que* $m_0/2$ *et* p. *Le polynôme*

$$C = \frac{1}{z^l}\frac{\partial^l \mathcal{Q}}{\partial x^l}$$

est un covariant de f *si et seulement si* $m_0 - l + 1$ *est congru à* 0 *modulo* p. *Lorsque* C *est un covariant non nul, il est d'ordre* $m_0 - 2l$ *et de degré* d_0.

Avant de montrer ce résultat, on énonce un lemme technique.

Lemme 9. *On reprend les notations de la section 5.3.2 et on note* $g : (a, X) \to (a', (x, \mu x + z))$. *Si* $\mathcal{Q}$ *est un covariant et* l *un entier naturel alors*

$$\frac{\partial^l \mathcal{Q}}{\partial x^l} \circ g = \sum_{i=0}^{l} \binom{l}{i} \cdot (-\mu)^{l-i} \cdot \frac{\partial^l \mathcal{Q}(x,z)}{\partial x^i \partial^{l-i} z}.$$

Démonstration. La preuve de ce lemme se fait par récurrence sur l en considérant les quantités $\frac{\partial}{\partial x}(\frac{\partial^l \mathcal{Q}}{\partial x^l} \circ g)$ et $\frac{\partial}{\partial z}(\frac{\partial^l \mathcal{Q}}{\partial x^l} \circ g)$. □

Pour montrer que C est un covariant sous l'action de $\mathrm{SL}_2(k)$, on va considérer l'action de $\mathbb{T}$, Γ et Γ^*. On écrit $C = \sum_{i=0}^{m} C_i x^i z^{m-i}$.

Action de $\mathbb{T}$. Par définition, C, $C_0, \ldots, C_m$ sont des fonctions homogènes de degré d_0 et isobares de poids $l + \omega_0, l + \omega_0 + 1, \ldots, l + \omega_0 + m$. On exprime C en fonction des coefficients de $\mathcal{Q}$

$$C = \sum_{i=l}^{m_0} \frac{i!}{l!} \mathcal{Q}_i x^{i-l} z^{m_0-i-l}.$$

Si $p|(m_0 - l + 1)$, alors pour tout $i \in \{m_0 - l + 1, \ldots, m_0\}$,

$$p \mid \frac{i!}{l!}.$$

Dans ce cas, C est un polynôme homogène d'ordre $m = m_0 - 2l$. De plus, $\mathcal{Q}$ étant un covariant, la proposition 6 (p. 78) assure que $m_0 = nd_0 - 2w_0$. L'ordre de C peut donc s'écrire $m = nd_0 - 2(\omega_0 + l)$. Ainsi, par la proposition 6 (p. 78), C est un covariant sous $\mathbb{T}$. La réciproque est également donnée par la proposition 6 (p. 78). La condition $p|(m_0 - l + 1)$ est donc une condition nécessaire et suffisante pour que C soit un covariant sous $\mathbb{T}$.

Action de Γ. On pose $g : (a, X) \to (a', (x + \mu z, z)) = (a', g_1(x, z), g_2(x, z))$. On cherche à montrer que $C \circ g = C$. C'est à dire

$$(\frac{1}{z^l}\frac{\partial^l \mathcal{Q}}{\partial x^l}) \circ g = \frac{1}{z^l}\frac{\partial^l \mathcal{Q}}{\partial x^l}.$$

Ceci est équivalent à

$$\frac{\partial^l \mathcal{Q}}{\partial x^l} \circ g = \frac{\partial^l \mathcal{Q}}{\partial x^l}.$$

Or $\mathcal{Q}$ étant un covariant sous l'action de Γ, on a

$$\frac{\partial \mathcal{Q}}{\partial x} = \frac{\partial \mathcal{Q} \circ g}{\partial x}.$$

De plus,

$$\frac{\partial \mathcal{Q} \circ g}{\partial x} = \frac{\partial \mathcal{Q}}{\partial x} \circ g.$$

Donc, par récurrence immédiate, on obtient le résultat voulu. Ainsi, C est un covariant sous l'action de Γ.

Action de Γ^*. On reprend les notation du lemme 9 (p. 80). On cherche à montrer que $C \circ g = C$. C'est-à-dire

$$(\frac{1}{z^l}\frac{\partial^l \mathcal{Q}}{\partial x^l}) \circ g = \frac{1}{z^l}\frac{\partial^l \mathcal{Q}}{\partial x^l}.$$

Ceci est équivalent à

$$z^l(\frac{\partial^l \mathcal{Q}}{\partial x^l}) \circ g = (\mu x + z)^l \frac{\partial^l \mathcal{Q}}{\partial x^l}.$$

Grâce au lemme 9 (p. 80), cela revient à montrer

$$z^l \sum_{i=0}^{l} \binom{l}{i} \frac{\partial^l \mathcal{Q}}{\partial x^i \partial z^{l-i}} (-\mu)^{l-i} = \sum_{i=0}^{l} \binom{l}{i} \frac{\partial^l \mathcal{Q}}{\partial x^l} \mu^{l-i} x^{l-i} z^i.$$

Ceci est encore équivalent à

$$\sum_{i=0}^{l} \binom{l}{i} \mu^{l-i} \Big[\frac{\partial^l \mathcal{Q}}{\partial x^l} x^{l-i} z^i + (-1)^{l-i+1} \frac{\partial^l \mathcal{Q}}{\partial x^i \partial z^{l-i}} z^l \Big] = 0$$

ou encore que pour tout $i \in \{0, \dots, l\}$

$$\frac{\partial^l \mathcal{Q}}{\partial x^l} x^{l-i} z^i + (-1)^{l-i+1} \frac{\partial^l \mathcal{Q}}{\partial x^i \partial z^{l-i}} z^l = 0.$$

On suppose que $p|(m_0 - l + 1)$. On développe l'expression de gauche et on obtient

$$0 = \sum_{j=l}^{m_0} \mathcal{Q}_j j(j-1)\dots(j-l+1) x^{j-i} z^{m_0+i-j} +$$

$$(-1)^{l-i+1} \sum_{j=i}^{m_0-l+i} \mathcal{Q}_j j(j-1)\dots(j-i+1) x^{j-i} (m_0-j)(m_0-j-1)\dots(m_0-j-l+i+1) z^{m_0-j+i}.$$

Pour tout $j \in \{m_0 - l, \dots, m\}$, $p|j(j-1)\dots(j-l+1)$. De même, pour tout $j \in \{m_0 - l, \dots, m_0 - l + i\}$, $p|j(j-1)\dots(j-i+1)$. Ainsi, les sommes considérées s'arrêtent à $m_0 - l$. Pour tout $j \in \{i, \dots, l-1\}$, $p|(m_0-j)(m_0-j-1)\dots(m_0-j-l+i+1)$. Ainsi les deux sommes commencent à l. Enfin, puisque $p|(m_0 - l + 1)$,

$$(m_0-j)(m_0-j-1)\dots(m_0-j-l+i+1) \equiv (l-1-j)(l-2-j)\dots(-j+i) \equiv (-1)^{l-i}(j-i)\dots(j-l+1) \pmod{p}$$

Ce qui prouve la nullité de l'expression. On a donc montré que si $p|(m_0 - l + 1)$ alors C est invariant sous Γ^*.

Démonstration du théorème 13 (p. 80). D'après le paragraphe "Action de $\mathbb{T}$" (p. 80), C est un covariant sous l'action de $\mathbb{T}$ si et seulement si $p|(m_0 - l + 1)$. D'après le paragraphe "Action de Γ" (p. 81), C est un covariant sous l'action de Γ. D'après le paragraphe "Action de Γ^*" (p. 81), si $p|(m_0 - l + 1)$ alors C est un covariant sous l'action de Γ^*. Puisque $\mathrm{SL}_2(k)$ est engendré par $\mathbb{T}$, Γ et Γ^*, si $p|(m_0 - l + 1)$, C est un covariant sous l'action de $\mathrm{SL}_2(k)$.

Réciproquement, supposons que C soit un covariant sous l'action de $\mathrm{SL}_2(k)$. L'invariance sous l'action de $\mathbb{T}$ montre que $p|(m_0 - l + 1)$. □

Exemple 9. *Grâce à cette proposition, on peut construire de nouveaux covariants qui n'apparaissent pas en caractéristique nulle.*

- *Pour les formes quartiques binaire en caractéristique* 3 *(cf. section 5.2.3), on trouve* $c_{0,1}$ *(*$\mathcal{Q} = f$ *et* $l = 2$*) et* $c_{4,3}$ *(*$\mathcal{Q} = c_{6,3}$ *et* $l = 1$*) ;*
- *Pour les formes sextiques en caractéristique* 3 *(cf. section 5.2.6), on trouve le covariant* q *(*$\mathcal{Q} = f$ *et* $l = 1$*) de degré* 1 *et d'ordre* 4 *;*
- *Pour les formes sextiques en caractéristique* 5 *(cf. 5.2.6 et 6.6.2.3), on trouve le covariant* c *(*$\mathcal{Q} = f$ *et* $l = 2$*) de degré* 1 *et d'ordre* 2 *;*
- *Pour les formes de degré* 8 *en caractéristique* 5*, on retrouve le covariant ,* $C = a_4$ *(*$\mathcal{Q} = f$ *et* $l = 4$*) d'ordre* 0 *et de degré* 1 *identifié par Basson et Lercier.*

Remarque 21. *Il est tentant de s'interroger sur la possibilité d'obtenir en petite caractéristique un système générateur de covariants par l'ajout de cette nouvelle opération. Une première difficulté est la suivante. Soient* $\mathcal{Q}_1, \dots, \mathcal{Q}_r$ *des covariants,* $l_1, \dots, l_r$ *les entiers tels que*

$$C_i = \frac{1}{z^{l_i}} \frac{\partial^{l_i} \mathcal{Q}_i}{\partial x^{l_i}}$$

soient les covariants obtenus par la nouvelle opération à partir des $\mathcal{Q}_i$*. Soit* $\mathcal{Q}$ *un élément de* $k[\mathcal{Q}_1, \dots, \mathcal{Q}_r, C_1, \dots, C_r]$*. L'expression* $\frac{1}{z^l} \frac{\partial^l \mathcal{Q}}{\partial x^l}$ *n'est pas nécessairement dans* $k[\mathcal{Q}_1, \dots, \mathcal{Q}_r, C_1, \dots, C_r]$*. En effet, on se place sur* $k = \mathbb{F}_5$*, pour* $r = 1$ *et on considère seulement la forme sextique* $\mathcal{Q}_1 = f$*. Le covariant de* f

$$\frac{1}{z^3} \frac{\partial^3 f^2}{\partial x^3} = (a_3a_6 + a_4a_5)x^6 + (4a_2a_6 + 4a_3a_5 + 2a_4^2)x^5z + (a_0a_4 + a_1a_3 + 3a_2^2)xz^5 + (4a_0a_3 + 4a_1a_2)z^6$$

n'est pas dans l'algèbre engendrée par f *et* $C_1 = \frac{1}{z^2} \frac{\partial^2 f}{\partial x^2}$*. En effet, s'il était dans cette algèbre, il serait combinaison linéaire de* f^2*,* fC_1 *et* C_1^2 *puisque ce sont les seuls termes de degré* 2 *en les* a_i*. Or les termes qui ne dépendent pas de* x *dans ces trois covariants sont* a_0^2*,* $2a_0a_2$ *et* $4a_2^2$*. On ne peut pas générer le coefficient* $(4a_0a_3 + 4a_1a_2)$*.*

Il est donc difficile de voir quand la nouvelle opération saturera l'algèbre.

Il s'avère de plus qu'on a un contre-exemple à notre espoir initial. En effet, l'invariant $c_{0,6} \in \mathcal{I}_4$ *en caractéristique* 3 *de la section 5.2.3 ne s'obtient pas de cette façon. Pour l'obtenir par notre opération, il faudrait qu'il soit la dérivée* l*-ième d'un certain covariant d'ordre* m *et de degré* 6*. Les entier* m *et* l *doivent vérifier* $l < m/2$*,* $m - 2l = 0$ *et* $m - l + 1$ *est un multiple de* 3*. On obtiendrait donc cet invariant en effectuant la dérivée seconde d'un covariant* $c_{4,6}$ *d'ordre* 4 *et de degré* 6*. Or en effectuant les calculs, on trouve que l'algèbre des covariant de degré inférieur à* 6 *engendré par notre opérateur sur la réduction des covariants de la caractéristique nulle est engendré par* $c_{0,1}$*,* $f = c_{4,1}$*,* $c_{4,3}$ *et* $c_{6,3}$*. Les deux seules possibilités pour* $c_{4,6}$ *sont* $c_{0,1}^5 c_{4,1}$ *et* $c_{0,1}^3 c_{4,3}$*. Ces deux possibilités ne donnent pas* $c_{0,6}$*.*

Remarque 22. *On aurait aussi pu considérer*

$$\frac{1}{x^l} \frac{\partial^l \mathcal{Q}}{\partial z^l}$$

et montrer que cette quantité est encore un covariant exactement de la même façon. Cependant, le nouveau covariant construit est le même (au signe près) que le précédent.

Chapitre 6

Construction d'une courbe de genre 2 à partir de l'espace de modules $\mathcal{M}_2(k)$

6.1 Groupes d'automorphismes selon la caractéristique

6.1.1 Le cas du genre quelconque

Soit $\mathcal{C} : y^2 = f(x)$ une courbe hyperelliptique de genre $\mathtt{g}$ sur un corps k parfait de caractéristique $p \neq 2$. On rappelle que $\mathrm{Aut}(\mathcal{C})$ désigne son groupe d'automorphismes et $\mathrm{Aut}'(\mathcal{C})$ son groupe d'automorphismes réduit (voir la définition 10 (p. 20)). Les notations pour désigner les divers groupes qui apparaissent dans les résultats sont encore les suivantes :

- $\mathbf{C}_n$, le groupe cyclique d'ordre n,
- $\mathbf{D}_{2n}$, le groupe diédral d'ordre $2n$,
- $\mathcal{A}_n$, le groupe alterné d'ordre $n!/2$,
- $\mathcal{S}_n$, le groupe symétrique d'ordre $n!$.

Nous donnons ci-dessous les groupes d'automorphismes réduits pour les courbes de genre 2. Le résultat est connu, voir par exemple [CGLR99, table 1 p.38] mais nous en donnons ci-dessous une démonstration élémentaire afin de clarifier les liens entre les strates.

Comme $\mathrm{Aut}'(\mathcal{C}) \subset \mathrm{PGL}_2(\overline{k})$, [Hug05, lem 2.2.1 p.25] décline l'ensemble des sous-groupes finis possibles à conjugaison près (en reprenant la classification de [Suz82, p.404], Huggins omet toutefois le groupe $\mathrm{PSL}_2(\mathbb{F}_5)$ en caractéristique 3). Grâce aux résultats de Grotendieck [Gro71, XIII 2.12] et celui de Roquette [Roq70], on peut affiner ce résultat de la manière suivante :

Proposition 24. *Si $p = 0$ ou si $p > \mathtt{g}+1$ et $p \neq 2\,\mathtt{g}+1$ alors*

$$\mathrm{Aut}'(\mathcal{C}) \in \{\mathcal{A}_4, \mathcal{S}_4, \mathcal{A}_5\} \cup \bigcup_{n\in\mathbb{N}} \Big\{\mathbf{C}_n, \mathbf{D}_{2n}\Big\}.$$

Si $p = 2\,\mathtt{g}+1$ alors le résultat ci-dessus est valable sauf si $\mathcal{C}$ est isomorphe à la courbe définie par $y^2 = x^p - x$. Dans ce dernier cas, le groupe d'automorphismes réduit de $\mathcal{C}$ est isomorphe à $\mathrm{PGL}_2(\mathbb{F}_p)$.

On note :

$$G_{\beta,A} = \left\{ \begin{pmatrix} \beta^k & a \\ 0 & 1 \end{pmatrix} : a \in A, k \in \mathbb{Z} \right\}$$

où A est un sous-groupe additif de $\overline{k}$ contenant 1 et β une racine de l'unité telle que $\beta A = A$. Si p divise $|\mathrm{Aut}'(\mathcal{C})|$, on a :

Proposition 25. *Si $p \neq 3$ alors*

$$\mathrm{Aut}'(\mathcal{C}) \in \bigcup_{n\in\mathbb{N}} \{\mathrm{PGL}_2(\mathbb{F}_{p^n}), \mathrm{PSL}_2(\mathbb{F}_{p^n})\} \cup \bigcup_{k,A} \{G_{\beta,A}\}.$$

Si $p = 3$, il faut ajouter le groupe $\mathrm{PSL}_2(\mathbb{F}_5)$.

On renvoie également à la thèse de Brandt [Bra88] pour une étude plus détaillée des groupes d'automorphismes possibles et les modèles de courbes correspondants.

6.1.2 Le cas du genre 2

Soit maintenant $\mathcal{C} : y^2 = f(x)$ une courbe hyperelliptique avec $f \in k[x]$ de degré 6 (ou 5 si le point à l'infini ∞ est un point de $\mathcal{C}$). Puisque $\mathrm{Aut}'(\mathcal{C})$ agit sur f par permutation de ses racines, $\mathrm{Aut}'(\mathcal{C}) \hookrightarrow \mathcal{S}_6$. Ainsi, les éléments de $\mathrm{Aut}'(\mathcal{C})$ sont d'ordre au plus égal à 6. On obtient alors plus précisément :

Corollaire 3. 1. *Si $p = 0$ ou $p \geq 5$ (avec $\mathcal{C}$ non isomorphe à $y^2 = x^5 - x$ pour $p = 5$) alors* $\mathrm{Aut}'(\mathcal{C}) \in \{\mathbf{C}_n, \mathbf{D}_{2n}, \mathcal{A}_4, \mathcal{S}_4, \mathcal{A}_5\}$ *pour* $n \in \{1, 2, 3, 4, 5, 6\}$.
Lorsque $p = 5$ et $\mathcal{C}$ est isomorphe à $y^2 = x^5 - x$, $\mathrm{Aut}'(\mathcal{C}) = \mathrm{PGL}_2(\mathbb{F}_5) \cong \mathcal{S}_5$.

2. *Si $p = 3$ alors*

$$\mathrm{Aut}'(\mathcal{C}) \in \{\mathbf{C}_n, \mathbf{D}_{2n}, \mathrm{PSL}_2(\mathbb{F}_3), \mathrm{PGL}_2(\mathbb{F}_3), \mathrm{PSL}_2(\mathbb{F}_5), \mathrm{PSL}_2(\mathbb{F}_9), \mathrm{PGL}_2(\mathbb{F}_9)\} \cup \bigcup_{k,A} \{G_{\beta,A}\}$$

pour $n \in \{1, 2, 4, 5\}$.

Parmi les groupes du corollaire 3 (p. 84), on va identifier lesquels sont réalisés en adoptant la stratégie suivante : on considère γ un élément d'ordre maximal dans $\mathrm{Aut}'(\mathcal{C})$. D'après le corollaire précédent, γ est d'ordre au plus égal à 6. Pour chaque valeur de m, on cherche ensuite les groupes correspondants.

Quitte à faire une transformation linéaire, lorsque m est premier à p, on peut supposer que $\gamma : (x : z) \to (\zeta_m x : z)$ avec ζ_m une racine primitive m-ième de l'unité et que 1 est une racine de f. Lorsque $p = m$, on suppose que $\gamma : (x : z) \to (x + 1 : z)$. Fort de ces remarques, on va pouvoir effectuer une étude de cas. Dans ce but, on va identifier les groupes d'automorphismes réduits en fonction de m. Pour cela, on va s'appuyer sur le corollaire 3 (p. 84) et une fonction implémentée en `Magma` (voir Annexe B.2).

6.1.2.1 m=6 :

On peut tout d'abord exclure le cas de la caractéristique 3 comme le montre le lemme ci-dessous.

Lemme 10. *Il n'y a pas d'élément d'ordre* 6 *dans* $\mathrm{PGL}_2(\overline{\mathbb{F}}_3)$.

Démonstration. Supposons que $M \in \mathrm{PGL}_2(\overline{\mathbb{F}}_3)$ soit un élément d'ordre 6. Il existe $t \in \overline{\mathbb{F}}_3$ tel que $M^6 = t^3 Id$ car $x \to x^3$ est un isomorphisme en caractéristique 3. Ainsi, $(x - \sqrt{t})^3 (x + \sqrt{t})^3$ est un polynôme annulateur de M. La matrice M est donc trigonalisable et de la forme $\sqrt{t} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ ou $\sqrt{t} \begin{pmatrix} -1 & a \\ 0 & 1 \end{pmatrix}$ avec $a \in \overline{\mathbb{F}}_3$. Or, ces deux matrices ne sont pas d'ordre 6. □

Dans ce cas, $p \neq 3$ et les racines de f sont les puissances de ζ_6. La courbe $\mathcal{C}$ est isomorphe à la courbe d'équation $y^2 = x^6 - 1$. Si $p = 5$, la fonction `IdentifyHyperellipticGroup` (cf annexe B.2) permet d'affirmer que le groupe d'automorphismes réduits de $\mathcal{C}$ est isomorphe à $\mathrm{PGL}_2(\mathbb{F}_5) \cong \mathcal{S}_5$. Si $p \geq 7$, le corollaire 3 (p. 84) met en exergue uniquement deux possibilités : $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{C}_6$ ou $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_{12}$. Comme $\mathrm{Aut}'(\mathcal{C})$ contient aussi l'automorphisme $(x : z) \to (z : x)$ qui n'est pas dans l'orbite de γ, $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_{12}$.

6.1.2.2 m=5 :

Lorsque $m = 5$, si $p \neq 5$, $\mathcal{C}$ contient le point à l'infini et les racines de f sont les puissances de ζ_5. Ainsi, $\mathcal{C}$ est isomorphe à la courbe d'équation $y^2 = x^5 - 1$. Puisque $\mathrm{Aut}'(\mathcal{C})$ contient un élément d'ordre 5, le corollaire 3 (p. 84) précise qu'il y a que deux possibilités : soit $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{C}_5$, soit $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_{10}$. à présent, on va montrer que $\mathrm{Aut}'(\mathcal{C})$ n'est pas isomorphe à $\mathbf{D}_{10}$. Si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Aut}'(\mathcal{C})$, alors il existe $\lambda \in \overline{k}\backslash\{0\}$ tel que :

$$(aX + bZ)^5(cX + dZ) - (cX + dZ)^6 = \lambda \cdot (ZX^5 - Z^6). \tag{6.1.1}$$

On comprend aisément que si $c = 0$ alors M est de la forme $\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$ avec $a^5 = d^5$. Cela correspond à cinq matrices différentes de $\mathrm{PGL}_2(\overline{k})$. On va voir qu'en fait il n'y en a pas plus. En supposant que $c \neq 0$, la relation de degré 6 en X de l'équation (6.1.1) précise qu'il existe une racine cinquième de l'unité ζ_5 telle que $c = a\zeta_5$. Les relations de degré 4 et 3 en X de l'équation (6.1.1) montrent que $b = \frac{1}{\zeta_5}d$. Enfin, la relation de degré 0 en X indique que $\lambda = 0$, ce qui est impossible. Ainsi, il y a uniquement 5 automorphismes dans $\mathrm{Aut}'(\mathcal{C})$. Autrement dit, $\mathrm{Aut}'(\mathcal{C})$ est isomorphe à $\mathbf{C}_5$.

Si $p = 5$, $\mathcal{C}$ contient le point à l'infini et les racines de f sont tous les éléments de $\mathbb{F}_5$. Ainsi, $\mathcal{C}$ est isomorphe à la courbe d'équation $y^2 = x^5 - x$. Ainsi, d'aprés le corollaire 3 (p. 84), $\mathrm{Aut}'(\mathcal{C}) \cong \mathcal{S}_5$. Comme $\mathcal{S}_5$ contient un élément d'ordre 6, on se ramène au cas précédent. Ainsi, $\mathcal{C} \cong y^2 = x^6 - 1$.

6.1.2.3 m=4 :

Lorsque $m = 4$, l'action de γ sur la racine 1 montre que quatre des racines de f sont les puissances de ζ_4. Il reste donc deux racines qui ont une orbite d'ordre au plus 2. Il ne peut donc s'agir que des racines 0 et l'infini. Ainsi, $\mathcal{C}$ est isomorphe à la courbe d'équation $y^2 = x(x^4 - 1)$.

Si $p = 5$, alors on a :

$$f(x - z, a^{22}x + a^2z) = -a^9(x^6 - z^6)$$

avec a une racine de $x^2 + 4x + 2$ dans $\mathbb{F}_{25}$. Ainsi, la courbe $y^2 = f(x)$ et la courbe $y^2 = x^6 - 1$ sont isomorphes.

Si $p = 3$, la fonction `IdentifyHyperellipticGroup` permet d'affimer que le groupe d'automorphismes réduit de $\mathcal{C}$ est isomorphe à $\mathrm{PGL}_2(\mathbb{F}_3)$, lui-même isomorphe à $\mathcal{S}_4$.

Si $p \geq 7$, le corollaire 3 (p. 84) permet d'écrire que $\mathrm{Aut}'(\mathcal{C})$ est isomorphe à $\mathcal{S}_4$ ou $\mathbf{C}_4$ ou $\mathbf{D}_8$ car $\mathrm{Aut}'(\mathcal{C})$ contient un élément d'ordre 4. De plus, pour ζ_4 une racine quatrième primitive de l'unité, on a :

$$f(x - z, \zeta_4 x + \zeta_4 z) = -8\zeta_4(x^5 z - z^5 x).$$

Ainsi, $(x : z) \to (x - z : \zeta_4 x + \zeta_4 z)$ est un automorphisme réduit de $\mathcal{C}$. Par ailleurs, il est facile de voir que cet automorphisme est d'ordre 3. Ainsi, $\mathrm{Aut}'(\mathcal{C}) \cong \mathcal{S}_4$.

6.1.2.4 $m = 3$:

On suppose d'abord que la caractéristique de k est différente de 3. $\gamma \in \mathrm{Aut}'(\mathcal{C})$ est d'ordre 3. Ainsi, les racines de f sont $\{1, \zeta_3, \zeta_3^2, a, a\zeta_3, a\zeta_3^2\}$ ou $a \in \overline{k}^*\backslash\{1, \zeta_3, \zeta_3^2\}$. Le polynôme f a pour équation $x^6 - (a^3 + 1)x^3 + a^3$. On remarque que $i_a : (x : z) \to (az : x)$ est un automorphisme de $\mathcal{C}$ d'ordre 2. Ainsi, d'après le corollaire 3 (p. 84), $\mathrm{Aut}'(\mathcal{C}) \cong \mathcal{A}_4$ ou $\mathbf{D}_6$ puisque les autres groupes possibles contiennent des éléments d'ordre plus grand que 3. On va montrer que $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_6$. On remarque que $< i_a, \gamma >$ est un sous-groupe de $\mathrm{Aut}'(\mathcal{C})$. De plus, ce sous-groupe est isomomorphe à $\mathbf{D}_6$. Ainsi, $\mathrm{Aut}'(\mathcal{C})$, ne peut pas être isomorphe à $\mathcal{A}_4$ car $\mathcal{A}_4$ ne contient pas de sous-groupe isomorphe à $\mathbf{D}_6$. De plus, pour $a = -1$, $\mathcal{C}$ est isomorphe à $y^2 = x^6 - 1$. Ainsi ne caractéristique

5, $\mathcal{S}_5$ est un point de cette strate. En caractéristique différente de 3 et 5, $\mathbf{D}_{12}$ est un point de cette strate. Qui plus est, pour a une racine de x^2+4x+1, $c=1/a$ et b tel que $b^4=1/c^2$, on a

$$f(x+bz,cx+bz)=(c-1)^2(c^2+c+1)b(x^5z-z^5x).$$

Ainsi, en caractéristique différente de 3 et 5, $\mathcal{S}_4$ est un point de cette strate.

Si $p=3$ alors on peut supposer que $\gamma:(x:z)\to(x+z:z)$. Les racines de f sont alors $\{0,1,2,a,a+1,a+2\}$ avec $a\in\overline{k}\backslash\mathbb{F}_3$. Le polynôme f a pour équation $(x^3-x)(x-a)(x-a-1)(x-a-2)$. Grâce à la fonction `IdentifyHyperellipticGroup`, les groupes d'automorphismes réduits de $y^2=f(x)$ sont isomorphes à un $G_{\beta,A}$ de cardinal 6 non commutatif. C'est donc $\mathbf{D}_6$. De plus, pour a une racine du polynôme x^2+2x+2, on obtient

$$f(x+z/a,ax+z/a)=x^5z-xz^5$$

Ainsi, $\mathcal{S}_4$ est un point de cette strate.

6.1.2.5 $m=2$:

Les racines de f sont alors $\{1,-1,a,-a,b,-b\}$ avec $a\neq\pm b\in\overline{k}\setminus\{-1,0,1\}$. Les seuls groupes possibles sont $\mathbf{C}_2$ ou $\mathbf{D}_4$ puisque les autres groupes contiennent des éléments d'ordre plus grand que 2. Si $\mathrm{Aut}'(\mathcal{C})$ contient une autre involution, de simples considérations matricielles montrent qu'on peut supposer qu'il s'agit de $(x:z)\to(z:x)$. Les racines de f sont donc $\{1,-1,a,-a,\frac{1}{a},-\frac{1}{a}\}$ avec $a\notin\{-1,0,1\}$. De plus, pour $a=\zeta_6$, $\mathcal{C}$ est isomorphe à $y^2=x^6-1$. Ainsi ne caractéristique 5, $\mathcal{S}_5$ est un point de cette strate. En caractéristique différente de 3 et 5, $\mathbf{D}_{12}$ est un point de cette strate.

6.1.3 Diagramme de stratification en genre 2

En résumé, on obtient la stratification des groupes d'automorphismes réduits suivante avec leur dimension :

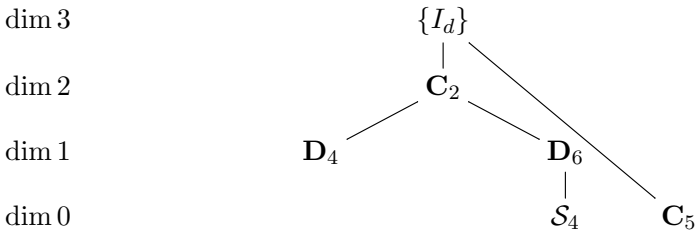


FIGURE 6.1 – Stratification en caractéristique 3

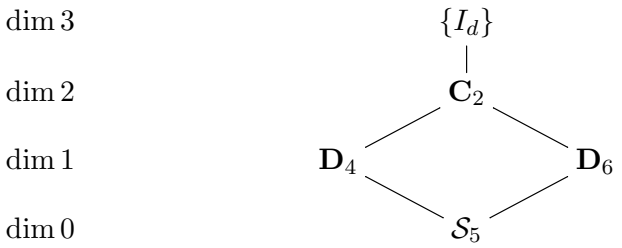


FIGURE 6.2 – Stratification en caractéristique 5

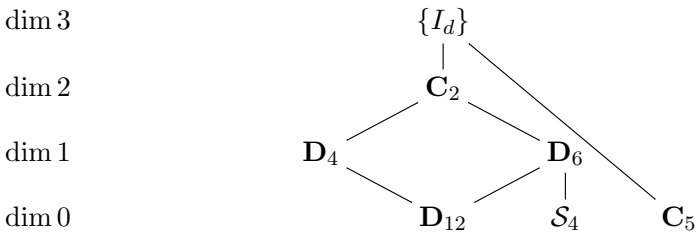


FIGURE 6.3 – Stratification en caractéristique $\neq 3$ et 5

Soit $[\mathcal{C}]$ un point de $\mathcal{M}_2(k)$ et (g_1, g_2, g_3) ses $\mathtt{g}_2$-invariants. On cherche à construire une courbe de genre 2 ayant ces invariants absolus. Les équations des strates sont obtenues par les relations entre les invariants spécialisés aux familles représentatives de la strate.

Nous venons de présenter la stratification de $\mathcal{M}_2(k)$ et la dimension de chaque strate des courbes ayant un groupe d'automorphismes donné. À présent, on va montrer comment reconstruire (par un modèle explicite sauf dans les cas génériques et $\mathbf{C}_2$ où on donne un algorithme) une courbe d'invariants donnés. Lorsque le groupe d'automorphismes réduit de n'est pas trivial, on donnera un modèle hyperelliptiquement définie (définition 9 (p. 20)) sur le corps de modules (définition 16 (p. 35)). Afin de ne donner que des conditions fermées sur les équations des strates, nous procédons par "remontée" : on considère tout d'abord les groupes d'automorphismes les plus gros et on exclut alors de facto les points de l'espace de modules dans les strates supérieures.

6.2 Méthode de construction : les cas de dimension 0

6.2.1 Groupe d'automorphismes réduit $\mathbf{D}_{12}$ avec $p \neq 3, 5$

Proposition 26. *On suppose que $p \neq 3$ et $p \neq 5$. Les assertions suivantes sont équivalentes :*

1. *Les g_2-invariants de $\mathcal{C}$ sont*

$$(g_1, g_2, g_3) = (\frac{6400000}{3}, \frac{440000}{9}, \frac{-32000}{81}).$$

2. *Le groupe d'automorphismes de $\mathcal{C}$ est* $\mathbf{D}_{12}$.
3. *la courbe $\mathcal{C}$ est isomorphe à la courbe* $y^2 = x^6 - 1$.

Démonstration. Dans la section 6.1, on a déjà vu que les points 2 et 3 sont équivalents. Puisque $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_{12}$ correspond à un seul point de l'espace de modules, il suffit de vérifier que $y^2 = x^6 - 1$ posséde ces g_2-invariants. La fonction `g2_invariants(C)` permet de réaliser ce calcul (cf. annexe A.2).

□

Sur le même principe, on obtient les résultats suivants.

6.2.2 Groupe d'automorphismes réduit $\mathcal{S}_4$ ou $\mathcal{S}_5$

Proposition 27. *Les assertions suivantes sont équivalentes :*

1. *Les g_2-invariants de $\mathcal{C}$ sont* $(g_1, g_2, g_3) = (50000, 3750, -125)$.
2. *Si $p \neq 5$ alors le groupe d'automorphismes de $\mathcal{C}$ est $\mathcal{S}_4$. Si $p = 5$ alors le groupe d'automorphismes de $\mathcal{C}$ est $\mathcal{S}_5$.*
3. *La courbe $\mathcal{C}$ est isomorphe à la courbe* $y^2 = x^5 - x$.

6.2.3 Groupe d'automorphismes réduit $\mathbf{C}_5$

Proposition 28. *On suppose que la caractéristique de k est différente de 5. Les assertions suivantes sont équivalentes :*

1. *Les g_2-invariants de $\mathcal{C}$ sont* $(g_1, g_2, g_3) = (0, 0, 0)$.
2. *Le groupe d'automorphismes de $\mathcal{C}$ est* $\mathbf{C}_5$.
3. *La courbe $\mathcal{C}$ est isomorphe à la courbe* $y^2 = x^5 - 1$.

D'après les figures 6.1, 6.2 et 6.3 (p. 87) les strates de dimension 0 sont entièrement traitées.

6.3 Méthode de construction : le cas de la dimension 1

En s'appuyant sur les propositions 2.2 et 2.1 de [CQ07] et sur les théorèmes 8 et 9 de [CQ05], on va distinguer les caractéristiques 3, 5 des autres. En effet, les relations vérifiées par les invariants d'Igusa ne sont pas les mêmes. De plus, dans le cas $\mathbf{D}_6$ en caractéristique 3, la famille n'est pas la même que dans les autres caractéristiques.

Remarque 23. *À plusieurs reprises, on a va supposer que $J_2 \neq 0$. Ceci n'est pas gênant car dans ces cas, la courbe a des automorphismes supplémentaires.*

6.3.1 Groupe d'automorphismes réduit $\mathbf{D}_6$

Caractéristique 3

Proposition 29. *Soient $[\mathcal{C}] \in \mathcal{M}_2(k)$ et J_2, J_4, J_6 et J_{10} ses invariants d'Igusa associés. Les assertions suivantes sont équivalentes.*

1. $J_4 = 0$ *et* $J_{10} + 2J_6J_2^2 = 0$.
2. $J_6 \neq 0$ *et la courbe* $\mathcal{C}_0 : y^2 = x^6 + tx^4 + (t-1)x^3 + tx^2 + 1$, *avec t une racine cubique de* $\dfrac{-J_2^3}{J_6}$, *est un représentant du point $[\mathcal{C}]$ définie sur le corps de modules k.*
3. *Le groupe d'automorphismes réduit de $[\mathcal{C}]$ contient* $\mathbf{D}_6$.

Remarque 24. *On peut très bien se servir directement des g_2-invariants. Les conditions sur les invariants deviennent les suivantes : $g_1 \neq 0$, $g_2 = 0$ et $g_3 = -1/2$. La condition sur t devient : t une racine cubique de $2g_1$.*

Démonstration de la proposition 29 (p. 88). ($1. \Rightarrow 2.$)
Soit $\mathcal{C}_0$ la courbe d'équation $y^2 = x^6 + tx^4 + (t-1)x^3 + tx^2 + 1$ avec t une racine cubique de $\dfrac{-J_2^3}{J_6}$. On pose λ une racine cubique de $\dfrac{J_2^3}{J_6^2}$. Les éléments t et λ sont bien définis car $J_6 \neq 0$. En effet, si $J_6 = 0$ alors $J_{10} = 0$ puisque $J_{10} + 2J_6J_2^2 = 0$. Or, $J_{10} = 0$ est impossible car la courbe $\mathcal{C}_0$ doit être lisse. Soient $i \in \{2, 4, 6, 10\}$ et $J_i(\mathcal{C}_0)$ les invariants d'Igusa de $\mathcal{C}_0$. La fonction `igusa_invariants` de l'annexe A.2 permet d'obtenir les résultats suivants : $J_2(\mathcal{C}_0) = t^2$, $J_4(\mathcal{C}_0) = 0$, $J_6(\mathcal{C}_0) = 2t^3$ et $J_{10}(\mathcal{C}_0) = 2t^7$. On vérifie aisément que $J_2(\mathcal{C}_0) = \lambda^2 J_2$, $J_6(\mathcal{C}_0) = \lambda^6 J_6$ et $J_{10}(\mathcal{C}_0) = \lambda^{10} J_{10}$. La dernière égalité utilise la relation $J_{10} + 2J_6J_2^2 = 0$.
($2. \Rightarrow 1.$)
Soit $\mathcal{C}_0$ définie comme dans 2. Grâce à la fonction `igusa_invariants`, les relations suivantes se vérifient aisément : $J_4 = 0$ et $J_{10} + 2J_6J_2^2 = 0$.
($2. \Rightarrow 3.$) On note $\alpha : (x : z) \to (-x + z : z)$ et $\beta : (x : z) \to (z, x)$. On remarque que $< \alpha, \beta > \subseteq \mathrm{Aut}'(\mathcal{C}_0)$. De plus, $< \alpha, \beta >$ est isomorphe à $\mathbf{D}_6$. Lorsque $t = 1$, on retrouve la strate du dessous.
($3. \Rightarrow 2.$)
Soit $\mathcal{C}$ un représentant de $[\mathcal{C}]$. On sait que $\mathrm{Aut}'(C) \cong \mathbf{D}_6 \cong < \alpha, \beta >$. On peut donc choisir $\mathcal{C}$ tel que $\mathrm{Aut}'(\mathcal{C}) \cong < \alpha, \beta >$. Comme $\mathrm{Aut}'(\mathcal{C})$ contient β, le polynôme hyperelliptique de $\mathcal{C}$ peut s'écrire :

$$f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_4x^2 + a_5x + a_6, \text{ avec } a_6, a_5, a_4 \text{ et } a_3 \in k.$$

Puisque $\mathrm{Aut}'(\mathcal{C})$ contient α, l'équation de f peut se réduire en :

$$f(x) = a_6x^6 + a_4x^4 + (a_4 - a_6)x^3 + a_4x^2 + a_6.$$

Comme a_6 est non nul (sinon la courbe définie ne serait pas de genre 2), on pose $t = \dfrac{a_4}{a_6}$ et on obtient le modèle voulu. Il reste à exprimer t en fonction des invariants d'Igusa de $\mathcal{C}$. Grâce à la fonction `igusa_invariants`, cette manipulation est aisée : on vérifie que le rapport $\dfrac{-J_2^3}{J_6}$ est le cube de t.

□

Caractéristique 5

Proposition 30. *Soient $[\mathcal{C}] \in \mathcal{M}_2(k)$ et J_2, J_4, J_6 et J_{10} ses invariants d'Igusa associés. On suppose que $J_2 \neq 0$. Les assertions suivantes sont équivalentes :*

1. *$J_{10}J_4J_2^2 + J_6^3 + 3J_6J_4^3 + 2J_4^4J_2 = 0$, $J_{10}J_2^3 + 3J_6^2J_4 + 4J_4^4 + 2J_4^3J_2^2 = 0$ et $J_6J_2 + 2J_4^2 = 0$.*
2. *La courbe $\mathcal{C}_0$ d'équation $y^2 = x^6 + x^3 + t$ où $t = -1 - \dfrac{J_4}{J_2^2}$ est un représentant du point $[\mathcal{C}]$ défini sur le corps de modules k.*
3. *Le groupe d'automorphismes réduit de $[\mathcal{C}]$ est isomorphe à $\mathbf{D}_6$.*

Remarque 25. *On peut très bien se servir directement des g_2-invariants. Puisque on suppose que $J_2 \neq 0$, on peut supposer que $g_1 \neq 0$. Les conditions sur les invariants deviennent les suivantes :*

$$\begin{aligned} g_2g_1^3 + g_3^3g_1^2 + 3g_3g_2^3g_1 + 2g_2^4g_1 &= 0 \\ g_1^3 + 3g_3^2g_2g_1 + 4g_2^4 + 2g_2^3g_1 &= 0 \\ g_3g_1 + 2g_2^2 &= 0 \end{aligned}$$

Grâce aux fonctions de `Magma`*, on trouve que variété définie par les* 3 *équations sur* g_1*,* g_2 *et* g_3 *est composé d'une courbe de genre* 0 *(lorsque* $g_1 \neq 0$*) et d'une autre composante (lorsque* $g_1 = 0$*). On peut ainsi paramétrer cette courbe de genre* 0 *avec des fonctions de* `Magma`*. Soit* $(t_1 : t_2) \in \mathbb{P}^1$*, on obtient*

$$g_1 = \frac{3t_2^5}{3t_1^5 + 3t_1^4 t_2 + 2t_1^3 t_2^2}$$
$$g_2 = \frac{t_1 t_2^4}{3t_1^5 + 3t_1^4 t_2 + 2t_1^3 t_2^2}$$
$$g_3 = \frac{t_1^2 t_2^3}{3t_1^5 + 3t_1^4 t_2 + 2t_1^3 t_2^2}$$

La condition sur t *devient* $t = -1 - t_1/3t_2$*.*

Démonstration de la proposition 30 (p. 89). (1. $\Rightarrow$ 2.)
Les polynômes $J_{10}J_4J_2^2 + J_6^3 + 3J_6J_4^3 + 2J_4^4J_2$, $J_{10}J_2^3 + 3J_6^2J_4 + 4J_4^4 + 2J_4^3J_2^2$ et $J_6J_2 + 2J_4^2$ sont homogènes de degré respectif 18, 16 et 8. Comme on suppose que $J_2 \neq 0$, on pose $j_1 = J_4/J_2^2$, $j_2 = J_6/J_2^3$ et $j_3 = J_{10}/J_2^5$. Ainsi, $t = -1 - j_1$ et les relations du 1. se réécrivent de la façon suivante :

$$j_3j_1 + j_2^3 + 3j_2j_1^3 + 2j_1^4 = 0,\ j_3 + 3j_2^2j_1 + 4j_1^4 + 2j_1^3 = 0 \text{ et } j_2 + 2j_1^2 = 0.$$

On pose aussi $J_2(\mathcal{C}_0)$, $J_4(\mathcal{C}_0)$, $J_6(\mathcal{C}_0)$ et $J_{10}(\mathcal{C}_0)$ les invariants d'Igusa de $\mathcal{C}_0$. Grâce à la fonction `igusa_invariants`, on se rend compte que $J_2(\mathcal{C}_0) \neq 0$. On peut donc considérer :

$$j_1(\mathcal{C}_0) = \frac{J_4(\mathcal{C}_0)}{J_2(\mathcal{C}_0)^2},\ j_2(\mathcal{C}_0) = \frac{J_6(\mathcal{C}_0)}{J_2(\mathcal{C}_0)^3} \text{ et } j_3(\mathcal{C}_0) = \frac{J_{10}(\mathcal{C}_0)}{J_2(\mathcal{C}_0)^5}.$$

Pour conclure, il suffit de vérifier que $j_1(\mathcal{C}_0) = j_1$, $j_2(\mathcal{C}_0) = j_2$ et $j_3(\mathcal{C}_0) = j_3$ modulo les relations ci-dessus. Le programme de l'annexe B.3.1 fournit une vérification.
(2. $\Rightarrow$ 1.)
Soit $\mathcal{C}_0$ définie comme dans le 2. La fonction `igusa_invariants` permet de vérifier aisément les relations suivantes :

$$J_{10}J_4J_2^2 + J_6^3 + 3J_6J_4^3 + 2J_4^4J_2 = 0,\ J_{10}J_2^3 + 3J_6^2J_4 + 4J_4^4 + 2J_4^3J_2^2 = 0 \text{ et } J_6J_2 + 2J_4^2 = 0.$$

(2. $\Rightarrow$ 3.)
Soient ζ_3 une racine primitive troisième de l'unité, $a \in \overline{k}$ une racine cubique de t et $\alpha : (x : z) \to (\zeta_3 x : z)$ *et* $\beta : (x : z) \to (az, x)$. On remarque que $< \alpha, \beta > \subseteq \mathrm{Aut}'(\mathcal{C}_0)$. De plus, $< \alpha, \beta >$ est isomorphe à $\mathbf{D}_6$. La figure 6.2 (p. 87) permet de conclure. En effet, les seuls groupes de la classification des automorphismes en genre 2, en caractéristique 5 contenant $\mathbf{D}_6$ sont lui-même et $\mathcal{S}_5$. Or, d'après la proposition 27 (p. 88), le point de $\mathcal{M}_2(k)$ qui admet pour groupe d'automorphismes $\mathcal{S}_5$ a pour $\mathtt{g}_2$-invariants $(0, 0, 0)$ et son invariant d'Igusa J_2 associé est nul. Puisqu'on a supposé $J_2 \neq 0$, on a bien $\mathrm{Aut}'(\mathcal{C}_0) \cong \mathbf{D}_6$.
(3. $\Rightarrow$ 2.)
Soient $\mathcal{C}$ un représentant de $[\mathcal{C}]$, α défini comme précédemment et $\beta : (x : z) \to (z : x)$. Sachant que $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_6$, $\mathbf{D}_6 \cong < \alpha, \beta >$. On peut donc choisir $\mathcal{C}$ tel que $\mathrm{Aut}'(\mathcal{C}) \cong < \alpha, \beta >$. Comme $\mathrm{Aut}'(\mathcal{C})$ contient β, le polynôme hyperelliptique de $\mathcal{C}$ peut s'écrire :

$$f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_4x^2 + a_5x + a_6 \text{ avec } a_6, a_5, a_4 \text{ et } a_3 \in k.$$

Puisque $\mathrm{Aut}'(\mathcal{C})$ contient α, l'équation de f peut réduire en :

$$f(x) = a_6x^6 + a_3x^3 + a_6.$$

Pour que la courbe définie soit de genre 2, a_6 est non nul. L'élément a_3 est aussi non nul. Sinon $\mathrm{Aut}'(\mathcal{C})$ contiendrait aussi l'automorphisme d'ordre 6 $(x : z) \to (\zeta_6 x : z)$, avec ζ_6 une racine primitive sixiéme de l'unité. Cet automorphisme ne peut pas être dans $\mathrm{Aut}'(\mathcal{C})$ puisqu'il est isomorphe à $\mathbf{D}_6$. On pose $t = (\frac{a_6}{a_3})^2$ ainsi, avec le changement de variable $x \to \sqrt[3]{a_6}x$, on construit le modèle voulu. Grâce à la fonction `igusa_invariants`, on vérifie que t s'exprime en fonction des invariants d'Igusa de $\mathcal{C}$.

□

Caractéristique $\neq 3, 5$

Proposition 31. *Soient $[\mathcal{C}] \in \mathcal{M}_2(k)$ et J_2, J_4, J_6 et J_{10} ses invariants d'Igusa associés. Les assertions suivantes sont équivalentes.*

1. $750J_{10} + 90J_6J_4 - 3J_6J_2^2 - J_4^2J_2 = 0$ *et* $2700J_6^2 + 540J_6J_4J_2 - 27J_6J_2^3 + 160J_4^3 - 9J_4^2J_2^2 = 0$.
2. *La courbe $\mathcal{C}_0$ d'équation $y^2 = x^6 + x^3 + t$ où*

$$t = \frac{13/160J_4J_2 + 9/16J_6 - 3/640J_2^3}{J_4J_2 + 45/2J_6 - 3/160J_2^3}$$

   est un représentant du point $[\mathcal{C}]$ sur le corps de modules k.
3. *Le groupe d'automorphismes réduit de $[\mathcal{C}]$ est isomorphe à $\mathbf{D}_6$.*

Remarque 26. *On peut très bien se servir directement des $\mathtt{g}_2$-invariants. Les conditions sur les invariants deviennent les suivantes :*

$$\begin{aligned} g_1 &\neq 0 \\ 750g_1 + 90g_2g_3 - 3g_1g_3 - g_2^2 &= 0 \\ 2700g_3^2g_1 + 540g_1g_2g_3 - 27g_1^2g_3 + 160g_2^3 - 9g_2^2g_1 &= 0 \end{aligned}$$

Grâce aux fonctions de `Magma`*, on trouve que variété définie par les 2 équations sur g_1, g_2 et g_3 est composé d'une courbe de genre 0 (lorsque $g_1 \neq 0$) et d'une autre composante (lorsque $g_1 = 0$). On peut ainsi paramétrer cette courbe de genre 0 avec des fonctions de* `Magma`*. Soit $(t_1 : t_2) \in \mathbb{P}^1$, on obtient*

$$\begin{aligned} g_1 &= \frac{-270t_2^5}{-1/151875t_1^5 + 1/10125t_1^4t_2 - 1/2700t_1^3t_2^2} \\ g_2 &= \frac{t_1^2t_2^3 - 9t_1t_2^4}{-1/151875t_1^5 + 1/10125t_1^4t_2 - 1/2700t_1^3t_2^2} \\ g_3 &= \frac{-2/135t_1^3t_2^2 + 1/10t_1^2t_2^3}{-1/151875t_1^5 + 1/10125t_1^4t_2 - 1/2700t_1^3t_2^2} \end{aligned}$$

La condition sur t devient

$$t = \frac{2^2 13g_2 + 2^3 3^2 5g_3 - 3g_1}{2^7 5g_2 + 2^6 3^2 5g_2 - 2^2 3g_1}.$$

Pour le cas $g_1 = 0$, les équations sur les invariants d'Igusa fournissent les valeurs des $\mathtt{g}_2$-invariants suivante : $g_1 = 0$, $g_2 = 3 \cdot 5^5/2^3$ et $g_3 = -25/3$ ainsi que $t = 1/40$.

Démonstration de la proposition 31 (p. 91). (1. $\Rightarrow$ 2.)
Cas 1 : $J_2 \neq 0$.
Les notations de la caractéristique 5 sont encore valables puisque $J_2 \neq 0$. On a donc les relations suivantes :

$$750j_3 + 90j_2j_1 - 3j_2 - j_1^2 \text{ et } 2700j_2^2 + 540j_2j_1 - 27j_2 + 160j_1^3 - 9j_1^2.$$

Un programme similaire à l'annexe B.3.1 permet de conclure.
Cas 2 : $J_2 = 0$.
Dans ce cas, $t = 1/40$ et les relations se réduisent à :

$$25J_{10} + 3J_6J_4 = 0 \text{ et } 135J_6^2 + 8J_4^3 = 0.$$

On pose $J_2(\mathcal{C}_0)$, $J_4(\mathcal{C}_0)$, $J_6(\mathcal{C}_0)$ et $J_{10}(\mathcal{C}_0)$ les invariants d'Igusa de $\mathcal{C}_0$ et $\lambda = 3/4\sqrt[4]{\frac{3}{10J_4}}$. Avec cette valeur de t, $J_2(\mathcal{C}_0) = 0$, $J_4(\mathcal{C}_0) = \frac{3^5}{5.2^9}$, $J_6(\mathcal{C}_0) = \frac{3^6}{2^{12}.5^2}$ et $J_{10}(\mathcal{C}_0) = \frac{3^{12}}{2^{21}.5^5}$. On vérifie aisément que $J_2(\mathcal{C}_0) = \lambda^2 J_2$, $J_4(\mathcal{C}_0) = \lambda^4 J_4$, $J_6(\mathcal{C}_0) = \lambda^6 J_6$ et $J_{10}(\mathcal{C}_0) = \lambda^{10} J_{10}$. L'avant-dernière égalité utilise la relation $25J_{10} + 3J_6J_4 = 0$. La dernière égalité requiert en plus la relation $135J_6^2 + 8J_4^3 = 0$.
(2. $\Rightarrow$ 1.)
Soit $\mathcal{C}_0$ définie comme dans le 2. Grâce à la fonction `igusa_invariants`, les relations suivantes se vérifient aisément :

$$750J_{10} + 90J_6J_4 - 3J_6J_2^2 - J_4^2J_2 = 0,$$

$$2700J_6^2 + 540J_6J_4J_2 - 27J_6J_2^3 + 160J_4^3 - 9J_4^2J_2^2 = 0.$$

(2. $\Rightarrow$ 3.)
Soient ζ_3 une racine primitive troisième de l'unité, a une racine troisième de t, $\alpha : (x : z) \to (\zeta_3 x : z)$ et $\beta : (x, y) \to (az : x)$. On remarque que $< \alpha, \beta > \subseteq \mathrm{Aut}'(\mathcal{C}_0)$. De plus, $< \alpha, \beta >$ est isomorphe à $\mathbf{D}_6$. La figure 6.3 (p. 87) permet de conclure. En effet, les seuls groupes de la classification des automorphismes en genre 2, en caractéristique $\neq 3, 5$ contenant $\mathbf{D}_6$ sont lui-même, $\mathcal{S}_4$ et $\mathbf{D}_{12}$. Or, d'après les proposition 26 et 27 (p. 88), le point de $\mathcal{M}_2(k)$ qui a pour groupe d'automorphismes réduits $\mathbf{D}_{12}$ (resp. $\mathcal{S}_4$) admet pour $\mathtt{g}_2$-invariants $(640000/3, 440000/9, -32000/81)$ (resp. $(50000, 3750, -125)$). Or, ces $\mathtt{g}_2$-invariants ne vérifient pas les relations de la remarque 26 (p. 91). On a bien $\mathrm{Aut}'(\mathcal{C}_0) \cong \mathbf{D}_6$.
(3. $\Rightarrow$ 2.)
Soit $\mathcal{C}$ un représentant de $[\mathcal{C}]$. On reprend α comme précédemment et on pose $\beta : (x : z) \to (z : x)$. Sachant que $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_6$, $\mathbf{D}_6 \cong < \alpha, \beta >$. On peut donc choisir $\mathcal{C}$ tel que $\mathrm{Aut}'(\mathcal{C}) \cong < \alpha, \beta >$. Comme $\mathrm{Aut}'(\mathcal{C})$ contient β, le polynôme hyperelliptique de $\mathcal{C}$ peut s'écrire :

$$f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_4x^2 + a_5x + a_6 \text{ avec } a_6, a_5, a_4 \text{ et } a_3 \in k.$$

Puisque $\mathrm{Aut}'(\mathcal{C})$ contient α l'équation de f peut se réduire en :

$$f(x) = a_6x^6 + a_3x^3 + a_6.$$

L'élément a_6 est non nul car la courbe définie est de genre 2. Quant à a_3 il est aussi non nul. Sinon, $\mathrm{Aut}'(\mathcal{C})$ contiendrait aussi l'automorphisme d'ordre 6 $(x : z) \to (\zeta_6 x : z)$, avec ζ_6 une racine primitive sixième de l'unité. Cet automorphisme ne peut pas être dans $\mathrm{Aut}'(\mathcal{C})$ puisqu'il est isomorphe à $\mathbf{D}_6$. On pose $t = (\frac{a_6}{a_3})^2$ ainsi, avec le changement de variable $x \to \sqrt[3]{a_6}x$, on construit le modèle voulu. Enfin, on vérifie que t s'exprime en fonction des invariants d'Igusa de $\mathcal{C}$ en utilisant la fonction `igusa_invariants`.

□

6.3.2 Groupe d'automorphismes réduit $\mathbf{D}_4$

Caractéristique $\neq 5$

Proposition 32. *Soit $[\mathcal{C}] \in \mathcal{M}_2(k)$ et J_2, J_4, J_6 et J_{10} ses invariants d'Igusa associés. On suppose que $J_2 \neq 0$. Les assertions suivantes sont équivalentes :*

1.

$$172800J_6^2 - 23040J_6J_4J_2 + 592J_6J_2^3 - 40960J_4^3 + 3584J_4^2J_2^2 - 104J_4J_2^4 + J_2^6 = 0,$$
$$128000J_{10} + 5760J_6J_4 - 192J_6J_2^2 - 1024J_4^2J_2 + 64J_4J_2^3 - J_2^5 = 0.$$

2. La courbe $\mathcal{C}_0$ d'équation $y^2 = x^5 + x^3 + tx$ ou

$$t = \frac{9/20J_4J_2 - 27/8J_6 - 7/640J_2^3}{J_4J_2 + 45/2J_6 - 3/160J_2^3},$$

est un représentant du point $[\mathcal{C}]$ sur le corps de modules k.

3. Le groupe d'automorphismes de $[\mathcal{C}]$ est isomorphe à $\mathbf{D}_4$.

Remarque 27. *On peut très bien se servir directement des g_2-invariants. On suppose que $g_1 \neq 0$ Les conditions sur les invariants deviennent les suivantes :*

$$172800g_1g_3^2 - 23040g_1g_2g_3 + 592g_1^2g_3 - 40960g_2^3 + 3584g_1g_2^2 - 104g_1^2g_2 + g_1^3 = 0,$$
$$128000g_1 + 5760g_2g_3 - 192g_1g_3 - 1024g_2^2 + 64g_1g_3 - g_1^2 = 0.$$

Grâce aux fonctions de `Magma`*, on trouve que la variété définie par les 2 équations sur g_1, g_2 et g_3 est composée d'une courbe de genre 0 (lorsque $g_1 \neq 0$) et d'une autre composante (lorsque $g_1 = 0$). On peut ainsi paramétrer cette courbe de genre 0 avec des fonctions de* `Magma`*. Soit $(t_1 : t_2) \in \mathbb{P}^1$, on obtient*

$$g_1 = \frac{37996698009600000t_2^5}{t_1^5 - 2415t_1^4t_2 + 6942526/3t_1^3t_2^2 - 1082801886t_1^2t_2^3 + 241333744965t_1t_2^4 - 19082904041475t_2^5}$$

$$g_2 = \frac{40888320000t_1^2t_2^3 - 43096289280000t_1t_2^4 + 12226629888000000t_2^5}{t_1^5 - 2415t_1^4t_2 + 6942526/3t_1^3t_2^2 - 1082801886t_1^2t_2^3 + 241333744965t_1t_2^4 - 19082904041475t_2^5}$$

$$g_3 = \frac{-61952000/3t_1^3t_2^2 + 35374592000t_1^2t_2^3 - 20078952960000t_1t_2^4 + 3772519027200000t_2^5}{t_1^5 - 2415t_1^4t_2 + 6942526/3t_1^3t_2^2 - 1082801886t_1^2t_2^3 + 241333744965t_1t_2^4 - 19082904041475t_2^5}$$

La condition sur t devient

$$t = \frac{2^5 3^2 g_2 - 2^4 3^3 5 g_3 - 7g_1}{2^7 5 g_2 + 2^6 3^2 5 g_2 - 2^2 3 g_1}.$$

Démonstration de la proposition 32 (p. 92). ($1. \Rightarrow 2.$)
On peut reprendre les mêmes notations que pour $\mathbf{D}_6$ en caractéristique 5 puisque $J_2 \neq 0$. Il s'ensuit les relations suivantes :

$$172800j_2^2 - 23040j_2j_1 + 592j_2 - 40960j_1^3 + 3584j_1^2 - 104j1 + 1 = 0,$$
$$128000j_3 + 5760j_2j_1 - 192j_2 - 1024j_1^2 + 64j_1 - 1 = 0.$$

Un programme similaire à l'annexe B.3.1 permet de conclure.
($2. \Rightarrow 1.$)
Soit $\mathcal{C}_0$ définie comme dans le 2. Grâce à la fonction `igusa_invariants`, on vérifie aisément les relations :

$$172800J_6^2 - 23040J_6J_4J_2 + 592J_6J_2^3 - 40960J_4^3 + 3584J_4^2J_2^2 - 104J_4J_2^4 + J_2^6 = 0,$$
$$128000J_{10} + 5760J_6J_4 - 192J_6J_2^2 - 1024J_4^2J_2 + 64J_4J_2^3 - J_2^5 = 0.$$

($2. \Rightarrow 3.$)
Soient i une racine carré de -1 et a une racine carrée de t, $\alpha : (x : z) \to (-x : z)$ et $\beta : (x : z) \to$

$(z : ax)$. On remarque que $< \alpha, \beta > \subseteq \mathrm{Aut}'(\mathcal{C}_0)$. De plus, $< \alpha, \beta >$ est isomorphe à $\mathbf{D}_4$. Les figures 6.3 (p. 87) et 6.1 (p. 87) permettent de conclure. En effet, les seuls groupes de la classification des automorphismes en genre 2 contenant $\mathbf{D}_4$ sont lui-même et $\mathbf{D}_{12}$ (en caractéristique $\neq 3$). Or, d'après la proposition 26 (p. 87), le point de $\mathcal{M}_2(k)$ qui a pour groupe d'automorphismes réduits $\mathbf{D}_{12}$ est $P = (6400000/3, 440000/9, -32000/81)$. Or, ces $\mathtt{g}_2$-invariants ne vérifient pas les relations de la remarque 27 (p. 93). On a bien $\mathrm{Aut}'(\mathcal{C}_0) \cong \mathbf{D}_4$.
(3. $\Rightarrow$ 2.)
Soit $\mathcal{C}$ un représentant de $[\mathcal{C}]$. On reprend α comme précédemment et on pose $\beta : (x : z) \to (z : x)$. Sachant que $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_4$, $\mathbf{D}_4 \cong < \alpha, \beta >$. On peut donc choisir $\mathcal{C}$ tel que $\mathrm{Aut}'(\mathcal{C}) \cong < \alpha, \beta >$. Comme $\mathrm{Aut}'(\mathcal{C})$ contient β, le polynôme hyperelliptique de $\mathcal{C}$ peut s'écrire :

$$f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_4x^2 + a_5x + a_6 \text{ avec } a_6, a_5, a_4 \text{ et } a_3 \in k.$$

Puisque $\mathrm{Aut}'(\mathcal{C})$ contient α l'équation de f peut se réduire en :

$$y^2 = a_5x^5 + a_3x^3 + a_5x.$$

L'élément a_5 est non nul car la courbe définie est de genre 2. Quant à a_3, il est aussi non nul. Sinon, $\mathrm{Aut}'(\mathcal{C})$ contiendrait aussi l'automorphisme d'ordre 4 $(x : z) \to (\zeta_4 x : z)$, avec ζ_4 une racine primitive quatrième de l'unité. Ceci est exclu car $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_4$. On pose $t = (\frac{a_5}{a_3})^2$ ainsi, avec le changement de variable $x \to \sqrt{\frac{a_3}{a_5}}x$, on construit le modéle voulu. Enfin, on vérifie que t s'exprime en fonction des invariants d'Igusa de $\mathcal{C}$ en utilisant la fonction `igusa_invariants`. □

Caractéristique 5

Proposition 33. *Soit $[\mathcal{C}] \in \mathcal{M}_2(k)$ et J_2, J_4, J_6 et J_{10} ses invariants d'Igusa associés. On suppose que $J_2 \neq 0$. Les assertions suivantes sont équivalentes.*

1.
$$\begin{aligned}
&J_{10}J_4^5 + 4J_6^5 + 2J_6^3J_4^3 + 2J_4^6J_2^3 + 2J_4^4J_2^7 + 4J_4^3J_2^9 + 2J_2^{15} = 0\\
&J_{10}J_4^3J_2 + 2J_6^4 + 3J_6^2J_4^3 + 3J_4^6 + J_4^5J_2^2 + 3J_4^4J_2^4 + 2J_4^3J_2^6 + J_4^2J_2^8 + 2J_4J_2^{10} + 3J_2^{12} = 0\\
&J_{10}J_4J_2^2 + J_6^3 + 3J_4^4J_2 + 2J_4^2J_2^5 + 4J_4J_2^7 + 2J_2^9 = 0\\
&J_{10}J_2^3 + 3J_6^2J_4 + 3J_4^4 + J_4^2J_2^4 + 3J_2^8 = 0\\
&J_6J_2 + 2J_4^2 + 3J_4J_2^2 + 3J_2^4 = 0.
\end{aligned}$$

2. *La courbe $\mathcal{C}_0$ d'équation $y^2 = x^5 + x^3 + tx$, avec $t = 1 + \dfrac{J_4}{J_2^2}$, est un représentant du point $[\mathcal{C}]$ sur son corps de modules.*
3. *Le groupe d'automorphismes de $[\mathcal{C}]$ est isomorphe à $\mathbf{D}_4$.*

Remarque 28. *On peut très bien se servir directement des $\mathtt{g}_2$-invariants. On suppose que $g_1 \neq 0$ Les conditions sur les invariants deviennent les suivantes :*

$$\begin{aligned}
&g_2^5 + 4g_1g_3^5 + 2g_2^3g_3^3 + 2g_2^6 + 2g_1^2g_2^4 + 4g_1^3g_2^3 + 2g_1^6 = 0\\
&g_1^2g_2^3 + 2g_1^2g_3^4 + 3g_1g_3^2g_2^3 + 3g_2^6 + g_1g_2^5 + 3g_1^2g_2^4 + 2g_1^3g_2^3 + g_1^4g_2^2 + 2g_1^5g_2 + 3g_1^6 = 0\\
&g_1^2g_2 + g_1g_3^3 + 3g_2^4 + 2g_1^2g_2^2 + 4g_1^3g_2 + 2g_1^4 = 0\\
&g_1^3 + 3g_1g_2g_3^2 + 3g_2^4 + g_1^2g_2^2 + 3g_1^4 = 0\\
&g_1g_3 + 2g_2^2 + 3g_1g_2 + 3g_1^2 = 0.
\end{aligned}$$

Grâce aux fonctions de `Magma`*, on trouve que variété définie par les 5 équations sur g_1, g_2 et g_3 est composé d'une courbe de genre 0 (lorsque $g_1 \neq 0$) et d'une autre composante (lorsque $g_1 = 0$).*

On peut ainsi paramétrer cette courbe de genre 0 *avec des fonctions de* Magma. *Soit* $(t_1 : t_2) \in \mathbb{P}^1$, *on obtient*

$$g_1 = \frac{t_2^5}{3t_1^5 + t_1^4t_2 + 2t_1^3t_2^2 + 3t_1t_2^4 + 2t_2^5}$$
$$g_2 = \frac{t_1t_2^4}{3t_1^5 + t_1^4t_2 + 2t_1^3t_2^2 + 3t_1t_2^4 + 2t_2^5}$$
$$g_3 = \frac{3t_1^2t_2^3 + 2t_1t_2^4 + 2t_2^5}{3t_1^5 + t_1^4t_2 + 2t_1^3t_2^2 + 3t_1t_2^4 + 2t_2^5}$$

La condition sur t *devient* $t = 1 + t_1/t_2$.

Démonstration de la proposition 33 (p. 94). (1. $\Rightarrow$ 2.)
On peut reprendre les mêmes notations que pour $\mathbf{D}_6$ en caractéristique 5 puisque $J_2 \neq 0$. On a donc les relations suivantes :

$$j_3j_1^5 + 4j_2^5 + 2j_2^3j_1^3 + 2j_1^6 + 2j_1^4 + 4j_1^3 + 2,$$
$$j_3j_1^3 + 2j_2^4 + 3j_2^2j_1^3 + 3j_1^6 + j_1^5 + 3j_1^4 + 2j_1^3 + j_1^2 + 2j_1 + 3,$$
$$j_3j_1 + j_2^3 + 3j_1^4 + 2j_1^2 + 4j_1 + 2,$$
$$j_3 + 3j_2^2j_1 + 3j_1^4 + j_1^2 + 3 \text{ et}$$
$$j_2 + 2j_1^2 + 3j_1 + 3$$

Un programme similaire à l'annexe B.3.1 permet de conclure.
(2. $\Rightarrow$ 1.)
Soit $\mathcal{C}_0$ définie comme dans le 2. On peut aisément vérifier les relations, sur les invariants d'Igusa de la proposition 33 (p. 94), en utilisant la fonction `igusa_invariants`.
(2. $\Rightarrow$ 3.)
Soient i une racine carrée de -1, a une racine carrée de t, $\alpha : (x : z) \to (-x : z)$ et $\beta : (x : z) \to (x : az)$. On remarque que $< \alpha, \beta > \subseteq \mathrm{Aut}'(\mathcal{C}_0)$. De plus, $< \alpha, \beta >$ est isomorphe à $\mathbf{D}_4$. La figure 6.2 (p. 87) permet de conclure. En effet, les seuls groupes de la classification des automorphismes en genre 2 contenant $\mathbf{D}_4$ sont lui-même et $\mathcal{S}_5$. D'après la proposition 27 (p. 88), le point de $\mathcal{M}_2(k)$ qui a pour groupe d'automorphismes $\mathcal{S}_5$ est $P = (0, 0, 0)$. Or, son invariant d'Igusa J_2 est nul. Puisqu'on a supposé que $J_2 \neq 0$, on a bien $\mathrm{Aut}'(\mathcal{C}_0) \cong \mathbf{D}_4$.
(3. $\Rightarrow$ 2.)
Soit $\mathcal{C}$ un représentant de $[\mathcal{C}]$. On reprend α comme précédemment et on pose $\beta : (x : z) \to (z : x)$. Sachant que $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_4$, $\mathbf{D}_4 \cong < \alpha, \beta >$. On peut donc choisir $\mathcal{C}$ tel que $\mathrm{Aut}'(\mathcal{C}) \cong < \alpha, \beta >$. Comme $\mathrm{Aut}'(\mathcal{C})$ contient β, le polynôme hyperelliptique de $\mathcal{C}$ peut s'écrire

$$f(x) = a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_4x^2 + a_5x + a_6 \text{ avec } a_6, a_5, a_4 \text{ et } a_3 \in k.$$

Puisque $\mathrm{Aut}'(\mathcal{C})$ contient α l'équation de f peut se réduire en :

$$y^2 = a_5x^5 + a_3x^3 + a_5x.$$

L'élément a_5 est non nul car la courbe définie est de genre 2. Quant à l'élément a_3, il est non nul. Sinon, $\mathrm{Aut}'(\mathcal{C})$ contiendrait aussi l'automorphisme d'ordre 4 $(x : z) \to (\zeta_4x : z)$, avec ζ_4 une racine primitive quatrième de l'unité. Ceci est exclu car $\mathrm{Aut}'(\mathcal{C}) \cong \mathbf{D}_4$. On pose $t = (\frac{a_5}{a_3})^2$ ainsi, avec le changement de variable $x \to \sqrt{\frac{a_3}{a_5}}x$, on construit le modèle voulu. La fonction `igusa_invariants` permet de vérifier que t s'exprime en fonction des invariants d'Igusa de $\mathcal{C}$. □

6.4 L'invariant $\mathcal{R}$

Après avoir traité le cas des strates de dimension inférieure à 1, on va expliquer comment séparer la strate de dimension 2 du cas générique. Pour cela, on va démontrer deux lemmes. Le premier fait le lien entre le degré en les coefficients et le degré en les crochets introduits dans la section 5.2.1. Le second est un lemme très utile qui lie un invariant $\mathcal{R}$ de degré 15 à l'existence d'une involution dans $\mathrm{Aut}'(\mathcal{C})$. Par rapport à l'invariant de degré 15 de la figure 5.1 (p. 55) et qui est en caractéristique 0 proportionnel à $\mathcal{R}$, l'invariant $\mathcal{R}$ a l'avantage de continuer à indiquer l'existence d'une involution en toute caractéristique. Finalement on se servira d'un résultat de Bolza en caractéristique 0 qu'on généralise en caractéristique impaire quelconque.

Lemme 11. *Si I est un invariant de f de degré m en les coefficients de f et de degré d en les crochets de f alors $2d = nm$.*

Démonstration. Soit $f(x,z) = \sum_{i=0}^{n} a_i x^i z^{6-i} = \prod_{i=0}^{n}(\alpha_i x - \beta_i z)$. On écrit $I_d(\alpha_i, \beta_i)$ l'invariant I exprimé en fonction des crochets de f et $I_m(a_i)$ l'invariant I exprimé en fonction des coefficients de f. Soit $\lambda \in \overline{k}$, on a :

$$f(\lambda x, \lambda z) = \prod_{i=0}^{n}(\lambda\alpha_i x - \lambda\beta_i z) = \lambda^n \sum_{i=0}^{n} a_i x^i z^{n-i}.$$

Puisque $I_d(\alpha_i, \beta_i)$ est de degré d en les $[ij]$, on obtient :

$$I_d(\lambda\alpha_i, \lambda\beta_i) = \lambda^{2d} I_d(\alpha_i, \beta_i).$$

De plus, $I_m(a_i)$ est de degré m en les a_i, d'où :

$$I_m(\lambda^n a_i) = \lambda^{nm} I_m(a_i).$$

Puisque ces deux quantités sont égales, $2d = nm$. □

Lemme 12. *Soit f le polynôme hyperelliptique de $\mathcal{C}$. Quitte à faire un changment de variable, on peut supposer que $f = \prod_{i=1}^{6}(x - x_i)$ où x_i sont deux à deux différents. On note aussi :*

$$D(x_1,x_2,x_3,x_4,x_5,x_6) = \det \begin{pmatrix} x_1+x_2 & 1 & -x_1x_2 \\ x_3+x_4 & 1 & -x_3x_4 \\ x_6+x_6 & 1 & -x_5x_6 \end{pmatrix}.$$

Alors

$$\begin{aligned}\mathcal{R} =& D(x_1,x_2,x_3,x_4,x_5,x_6)D(x_1,x_2,x_3,x_5,x_4,x_6)D(x_1,x_2,x_3,x_6,x_5,x_4)\\ & D(x_1,x_3,x_2,x_4,x_5,x_6)D(x_1,x_3,x_2,x_5,x_4,x_6)D(x_1,x_3,x_2,x_6,x_5,x_4)\\ & D(x_1,x_4,x_2,x_3,x_5,x_6)D(x_1,x_4,x_2,x_5,x_3,x_6)D(x_1,x_4,x_2,x_6,x_5,x_3)\\ & D(x_1,x_5,x_2,x_3,x_4,x_6)D(x_1,x_5,x_2,x_4,x_3,x_6)D(x_1,x_5,x_2,x_6,x_4,x_3)\\ & D(x_1,x_6,x_2,x_3,x_4,x_5)D(x_1,x_6,x_2,x_4,x_3,x_5)D(x_1,x_6,x_2,x_5,x_4,x_3)\end{aligned}$$

est un invariant de degré 15 de $\mathcal{C}$.

Avant de démontrer ce lemme, on va préciser l'origine de $D(x_1,x_2,x_3,x_4,x_5,x_6)$. On considère x_1, x_2, x_3, x_4, x_5 et x_6, six éléments de $\overline{k}$ et ι une homographie involutive qui envoie x_1 sur x_2, x_3 sur x_4 et x_5 sur x_6. Puisque ι est une involution, sa matrice est de la forme $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, avec a, b et $c \in \overline{k}$ non tous nuls. De plus, par définition de ι, on a $\frac{ax_i+b}{cx_i-a} = x_{i+1}$ pour $i \in \{1,3,5\}$. On obtient ainsi :

$$a(x_i + x_{i+1}) + b - x_i x_{i+1} c = 0 \text{ pour } i \in \{1,3,5\}.$$

Ou encore $D(x_1,x_2,x_3,x_4,x_5,x_6) = 0$. Réciproquement, si $D(x_1,x_2,x_3,x_4,x_5,x_6) = 0$ alors il existe une matrice A comme ci-dessus telle que $A.x_i = x_{i+1}$ pour $i \in \{1,3,5\}$.

Démonstration du lemme 12 (p. 96). .

On va montrer que $D(x_1, x_2, x_3, x_4, x_5, x_6)$ est un invariant de 6 points de degré 3 en les crochets. On reprend les notations de la partie 5.2.4 :

$$\begin{aligned}
t_0 &= (x_2 - x_1)(x_4 - x_3)(x_6 - x_5),\\
t_1 &= (x_4 - x_1)(x_3 - x_2)(x_6 - x_5),\\
t_2 &= (x_6 - x_1)(x_3 - x_2)(x_5 - x_4),\\
t_3 &= (x_6 - x_1)(x_5 - x_2)(x_4 - x_3) \text{ et}\\
t_4 &= (x_2 - x_1)(x_6 - x_3)(x_5 - x_4).
\end{aligned}$$

Les polynômes t_0, t_1, t_2, t_3, et t_4 forment une base des invariants de 6 points et sont de degré 3 en les crochets. De plus, on remarque que $D(x_1, x_2, x_3, x_4, x_5, x_6) = t_0 + t_1 + 2t_2 + t_3 + t_4$. Ainsi, D est un invariant de 6 points de degré 3 en les crochets. Ainsi $\mathcal{R}$ est un polynôme de degré 45 en les crochets. Grâce à la fonction `IsSymmetric` de Magma, on montre que $\mathcal{R}$ est symétrique. En d'autres termes, $\mathcal{R} \in \mathcal{B}_{reg,sym}$ (cf. la page 60). D'après le théorème 10 (p. 60), $\mathcal{R}$ est donc un invariant de f. De plus, d'après le lemme 11 (p. 96), $\mathcal{R}$ est de degré 15. □

Fort de ce lemme, on va montrer le résultat de Bolza étendu en toute caractéristique différente de 2, à savoir :

Proposition 34. *$\mathcal{R} = 0$ si et seulement si $\mathrm{Aut}'(\mathcal{C})$ contient (au moins) une involution.*

Démonstration. On analyse d'abord le cas $\mathcal{R} = 0$. D'après le lemme 12 (p. 96), il existe une matrice A telle que $A.x_i = x_{i+1}$ pour $i \in \{1, 3, 5\}$. L'application $\varphi : (x : z) \to A.(x : z)$ est un automorphisme réduit de $\mathcal{C}$. En effet, φ envoie l'ensemble des points des Weirstraß sur lui-même.

À présent on s'intéresse au cas où $\mathrm{Aut}'(\mathcal{C})$ contient une involution ι. Quitte à faire un changement de coordonnées, on peut supposer que cette involution est $i : (x : z) \to (-x : z)$. Ainsi, une équation de $\mathcal{C}$ est $y^2 = f(x) = f(-x)$. Ceci s'écrit aussi de façon équivalente $M_0.f = f$ pour

$$M_0 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Puisque $\mathcal{R}$ est un invariant de f de poids 45, $\mathcal{R}(M.f) = \det(M)^{45} M.\mathcal{R}(f)$ pour tout $M \in \mathrm{GL}_2(\overline{k})$. Il s'ensuit que $\mathcal{R}(f) = \mathcal{R}(M_0.f) = \det(M_0)^{45} M_0.\mathcal{R}(f) = -\mathcal{R}(f) = 0$. □

Pour exploiter ce résultat, on a besoin de connaître $\mathcal{R}$. Or, a priori, celui-ci est inconnu puisqu'on part des invariants absolus (g_1, g_2, g_3) pour construire une courbe de genre 2. Afin de contourner ce problème, on va exprimer $\mathcal{R}^2$ en fonction des invariants d'Igusa de la façon suivante :

Proposition 35.

$$\begin{aligned}
\mathcal{R}^2 = 2^{22}(\ & J_2^6 J_6^3 - 2J_2^5 J_4^2 J_6^2 - 72 J_2^5 J_4 J_6 J_{10} - 432 J_2^5 J_{10}^2 + J_2^4 J_4^4 J_6\\
& + 8 J_2^4 J_4^3 J_{10} - 72 J_2^4 J_4 J_6^3 - 48 J_2^4 J_6^2 J_{10} + 136 J_2^3 J_4^3 J_6^2\\
& + 4816 J_2^3 J_4^2 J_6 J_{10} + 28800 J_2^3 J_4 J_{10}^2 + 216 J_2^3 J_6^4 -\\
& 64 J_2^2 J_4^5 J_6 - 512 J_2^2 J_4^4 J_{10} + 1080 J_2^2 J_4^2 J_6^3 -\\
& 12960 J_2^2 J_4 J_6^2 J_{10} - 96000 J_2^2 J_6 J_{10}^2 - 2304 J_2 J_4^4 J_6^2 -\\
& 84480 J_2 J_4^3 J_6 J_{10} - 512000 J_2 J_4^2 J_{10}^2 - 7776 J_2 J_4 J_6^4 -\\
& 129600 J_2 J_6^3 J_{10} + 1024 J_4^6 J_6 + 8192 J_4^5 J_{10} + 6912 J_4^3 J_6^3 +\\
& 691200 J_4^2 J_6^2 J_{10} + 11520000 J_4 J_6 J_{10}^2 + 11664 J_6^5 + 51200000 J_{10}^3).
\end{aligned}$$

Démonstration. On utilise la méthode de l'annexe B.3.4. □

Puisque les invariants d'Igusa sont valables en toute caractéristique, on peut considérer l'annulation de $\mathcal{R}^2$ en toute caractéristique différente de 2.

6.5 Groupe d'automorphismes réduit $\mathbf{C}_2$

On présente une alternative à la méthode de [CQ05] avec l'avantage d'être valable en toute caractéristique (différente de 2 bien évidemment). Il n'y a donc pas d'obstruction à la reconstruction sur le corps de modules dans ce cas-là. En effet, on reconstruit notre courbe sur le corps $I_{\mathcal{C}}$.

Proposition 36. *Soient $[\mathcal{C}] \in \mathcal{M}_2(k)$, (g_1, g_2, g_3) ses $\mathfrak{g}_2$-invariants associés et $\mathcal{R}$ défini par le lemme 12 (p. 96). Les assertions suivantes sont équivalentes :*

1. $\mathcal{R} = 0$.
2. *La courbe $\mathcal{C}$ d'équation $y^2 = a_0x^6 + a_1x^5 + a_2x^4 + a_3x^3 + ta_2x^2 + t^2a_1x + t^3a_0$ est un représentant de $[\mathcal{C}]$. Les coefficients a_i sont définis par :*

$$\begin{aligned}
A_u =& J_2^5J_4^2 - 64J_2^3J_4^3 + 1024J_2J_4^4 + 3J_2^6J_6 - 202J_2^4J_4J_6 + 4014J_2^2J_4^2J_6 - 20160J_4^3J_6 + \\
& 666J_2^3J_6^2 - 20520J_2J_4J_6^2 + 48600J_6^3 - 30J_2^4J_{10} + 2800J_2^2J_4J_{10} - 192000J_4^2J_{10} - 360000J_2J_6J_{10},\\
B_u =& 2J_2^4J_4J_6 - 114J_2^2J_4^2J_6 + 1344J_4^3J_6 + 6J_2^3J_6^2 + 216J_2J_4J_6^2 - 3240J_6^3 + 18J_2^4J_{10} - \\
& 1040J_2^2J_4J_{10} + 12800J_4^2J_{10} + 4800J_2J_6J_{10},\\
A_v =& J_2^6J_4^2 - 96J_2^4J_4^3 + 3072J_2^2J_4^4 - 32768J_4^5 + 3J_2^7J_6 - 164J_2^5J_4J_6 + 1250J_2^3J_4^2J_6 + \\
& 29760J_2J_4^3J_6 + 858J_2^4J_6^2 - 22680J_2^2J_4J_6^2 - 172800J_4^2J_6^2 + 81000J_2J_6^3 + 1176J_2^5J_{10} - \\
& 79600J_2^3J_4J_{10} + 1344000J_2J_4^2J_{10} - 72000J_2^2J_6J_{10} - 12960000J_4J_6J_{10} - 134400000J_{10}^2,\\
B_v =& 3J_2^3J_4^2J_6 - 160J_2J_4^3J_6 + J_2^4J_6^2 - 36J_2^2J_4J_6^2 + 3456J_4^2J_6^2 - 1188J_2J_6^3 + 24J_2^3J_4J_{10} - \\
& 1280J_2J_4^2J_{10} + 160J_2^2J_6J_{10} + 105600J_4J_6J_{10} + 640000J_{10}^2,\\
u =& \frac{A_u}{B_u} \text{ et}\\
v =& \frac{A_v}{B_v}.
\end{aligned}$$

Si $u \neq 0$, on a :

$$\begin{aligned}
t &= v^2 - 4u^3\\
a_0 &= v^2 + u^2v - 2u^3\\
a_1 &= 2(u^2 + 3v)(v^2 - 4u^3)\\
a_2 &= (15v^2 - u^2v - 30u^3)(v^2 - 4u^3)\\
a_3 &= 4(5v - u^2)(v^2 - 4u^3)^2
\end{aligned}$$

Sinon :

$$\begin{aligned}
t &= 1\\
a_0 &= 1 + 2v\\
a_1 &= 2(3 - 4v)\\
a_2 &= 15 + 14v\\
a_3 &= 4(5 - 4v)
\end{aligned}$$

3. *Le groupe d'automorphismes réduit de $\mathcal{C}$ contient $\mathbf{C}_2$.*

Remarque 29. *On peut aussi avoir une expression de A_u, B_u, A_v et B_v en fonction des $\mathtt{g}_2$-invariants. On va distinguer 3 cas.*

1. *Si $g_1 \neq 0$ alors*

$$\begin{aligned}
A_u =& g_1^2g_2^2 - 64g_1g_2^3 + 1024g_2^4 + 3g_1^3g_3 - 202g_1^2g_2g_3 + 4014g_1g_2^2g_3 - 20160g_2^3g_3 + \\
& 666g_1^2g_3^2 - 20520g_1g_2g_3^2 + 48600g_1g_3^3 - 30g_1^3 + 2800g_1^2g_2 - 192000g_1g_2^2 - 360000g_1^2g_3,\\
B_u =& 2g_1^2g_2g_3 - 114g_1g_2^2g_3 + 1344g_2^3g_3 + 6g_1^2g_3^2 + 216g_1g_2g_3^2 - 3240g_1g_3^3 + 18g_3 - \\
& 1040g_1^2g_2 + 12800g_1g_2^2 + 4800g_1^2g_3,\\
A_v =& g_1^3g_2^2 - 96g_1^2g_2^3 + 3072g_1g_2^4 - 32768g_2^5 + 3g_1^4g_3 - 164g_1^3g_2g_3 + 1250g_1^2g_2^2g_3 + \\
& 29760g_1g_2^3g_3 + 858g_1^3g_3^2 - 22680g_1^2g_2g_3^2 - 172800g_1g_2^2g_3^2 + 81000g_1^2g_3^3 + 1176g_1^4 - \\
& 79600g_1^3g_2 + 1344000g_1^2g_2^2 - 72000g_1^3g_3 - 12960000g_1^2g_2g_3 - 134400000g_1^3,\\
B_v =& 3g_1^2g_2^2g_3 - 160g_1g_2^3g_3 + g_1^3g_3^2 - 36g_1^2g_2g_3^2 + 3456g_1g_2^2g_3^2 - 1188g_1^2g_3^3 + 24g_1^3g_2 - \\
& 1280g_1^2g_2^2 + 160g_1^3g_3 + 105600g_1^2g_2g_3 + 640000g_1^3.
\end{aligned}$$

2. *Si $g_1 = 0$ et $g_2 \neq 0$ alors*

$$\begin{aligned}
A_u =& -15,\\
B_u =& 1,\\
A_v =& -256g_2 - 1350g_3^2 - 101250g_3 - 1050000,\\
B_v =& 27g_3^2 + 825g_3 + 5000.
\end{aligned}$$

3. *Si $g_1 = g_2 = 0$ alors on pose $A_u = -15$, $B_u = 1$, $A_v = -210$, $B_v = 1$.*

Démonstration de la proposition 36 (p. 98). (1. $\Rightarrow$ 2.)
On suppose que $\mathcal{R} = 0$. D'après la proposition 34 (p. 97), $\mathrm{Aut}'(\mathcal{C})$ contient une involution. On note A une matrice de cette involution. Comme $A^2 = tI_d$ avec $t \in \overline{k}$, $P_o = X^2 - t$ est le polynôme caractéristique de A. La matrice A est donc équivalente à la matrice compagnon de P_o, à savoir

$$\begin{pmatrix} 0 & t \\ 1 & 0 \end{pmatrix}.$$

Quitte à faire un changement de coordonnées, on peut donc supposer que A est la matrice compagnon de P_0. De fait, $\mathcal{C}$ a un modèle de la forme $y^2 = a_0x^6 + a_1x^5 + a_2x^4 + a_3x^3 + ta_2x^2 + t^2a_1x + t^3a_0$. Pour la suite, il faut vérifier dans les deux cas que les invariants de la courbe $\mathcal{C}$ correspondent bien au point P. On effectue le même raisonnement que pour les strates de dimension 1. L'annexe B.3.2 fournit une vérification.
(2. $\Rightarrow$ 3.)
Si $\mathcal{C}$ la courbe d'équation $y^2 = a_0x^6 + a_1x^5 + a_2x^4 + a_3x^3 + ta_2x^2 + t^2a_1x + t^3a_0$ alors $\mathrm{Aut}'(\mathcal{C})$ contient l'involution $i : (x : z) \to (tz : x)$. Ainsi, $\mathrm{Aut}'(\mathcal{C}) \supset < i > \cong \mathbf{C}_2$.
(3. $\Rightarrow$ 1.)
Si $\mathrm{Aut}'(\mathcal{C})$ contient une involution alors $\mathcal{R} = 0$ (cf. proposition 34 (p. 97)). □

6.6 Groupe d'automorphisme réduit trivial

L'ensemble des points restants de $\mathcal{M}_2(k)$ ont un groupe d'automorphismes réduit trivial. On va alors appliquer une méthode algorithmique, dite méthode de Mestre. Dans celle-ci, on construit une conique et une cubique dont les six points d'intersection correspondent aux racines d'un polynôme f de degré 6 tel que $y^2 = f(x)$ est une équation de la courbe d'invariants souhaités.
La construction de la cubique et de la conique repose sur la donnée d'un triplet de covariants de f d'ordre 2 linéairement indépendants. Le choix classique fait dans Mestre doit être adaptée

en caractéristique 5 pour plusieurs raisons. Tout d'abord, les trois covariants qu'il choisit sont tous liés, et sont même proportionnels au covariant $c = a_4x^2 + 3a_3x + a_2$. Il faut donc construire à la main des "bons" covariants pour éviter ceci. Quand bien même, quel que soit le choix des covariants, la conique est contenu dans la cubique. Enfin, les covariants d'ordre 2 de petit degré ont une fâcheuse tendance à être des multiples de J_2. Cela pose problème lorsque $J_2 = 0$ car il est alors difficile de déterminer un triplet de covariants d'ordre 2 non liés. C'est pourquoi, le cas de la caractéristique 5 est traité à part : uniquement pour ce cas, on analyse la situation $J_2 = 0$ et $J_2 \neq 0$ à part.

6.6.1 Méthode de Mestre

Les égalités établies par Clebsch et utlisées dans la méthode de Mestre sont valides en caractéristique quelconque lorsqu'on supprime les divisions par des facteurs $n!$. Nous les donnons ci-dessous dans cette optique.

6.6.1.1 Les identités de Clebsh

Aprés avoir rappeler les résultats de l'exemple 3 de [Mes91], on expliquera comment adapter les résultats obtenus en caractéristique quelconque. Soient q_1, q_2, q_3 et f, quatre formes quadratiques définies sur $k[x, z]$. On note :

$$q_1^* = (q_2, q_3)_1,\ q_2^* = (q_3, q_1)_1 \text{ et } q_3^* = (q_1, q_2)_1,$$

$$A_{i,j} = (q_i, q_j)_2 \text{ pour i,j } \in [1, 2, 3],$$

$$R(q_1, q_2, q_3) \text{ le déterminant de } q_1,\ q_2,\ q_3 \text{ dans la base } x^2, xz, z^2.$$

Soient g et h deux formes binaires et $k \in \mathbb{N}$. On rappelle que $(g, h)_k$ est le transvectant d'indice k. On a les relations suivantes :

$$q_1q_1^* + q_2q_2^* + q_3q_3^* = 0, \tag{6.6.1}$$

$$2\det\big((A_{i,j})_{i,j=1,2,3}\big) = R^2(q_1, q_2, q_3), \tag{6.6.2}$$

$$R(q_1, q_2, q_3).f = 2\big((f, q_1)_2.q_1^* + (f, q_2)_2.q_2^* + (f, q_3)_2.q_3^*\big), \tag{6.6.3}$$

$$\sum_{i,j} A_{i,j}.q_i^*.q_j^* = 0. \tag{6.6.4}$$

Cette dernière égalité permet de construire la conique L. On note que les constantes différent de celles de Mestre. Toutes ces formules peuvent être vérifiées grâce à un logiciel de calcul. Le résultat suivant permet de construire la cubique M.

Proposition 37 ([LR12, p.11])**.** *Soit f une forme binaire de degré n.*

$$n! \cdot R(q_1, q_2, q_3)^{n/2}.f(x, z) = \Big(\sum_{i=1}^{3} q_i^*(x, z)\delta_i\Big)^{n/2} f(x_1, z_1), \tag{6.6.5}$$

où δ_i est l'opérateur différentiel $\varphi(x_1, z_1) \to \Omega_{12}^2(\varphi(x_1, z_1).q_i(x_2, z_2))$ (on rappelle que $\Omega_{12} = \frac{\partial}{\partial x_1}\frac{\partial}{\partial z_2} - \frac{\partial}{\partial x_2}\frac{\partial}{\partial z_1}$).

6.6.1.2 Un algorithme de construction générique en caractéristique $\neq 2, 3$ ou 5

On part d'un point de l'espace de modules $\mathcal{M}_2(k)$, représenté par ses g_2-invariants (g_1, g_2, g_3). On note J_2, J_4, J_6 et J_{10} les invariants d'Igusa associés (cf lemme 5 (p. 58)) ainsi que $\mathcal{R}$ l'invariant de degré 15 (voir le lemme 12 (p. 96)).

Remarque 30. *À l'exception d'un cas précis, on se sert uniquement de l'annulation ou non de $\mathcal{R}$. Ainsi, la donnée de $\mathcal{R}^2$ est suffisante. Lorsqu'on a besoin de sa valeur, on utilise la preuve du lemme 5 (p. 58) pour avoir une expression de $\mathcal{R}$ sur le corps de modules.*

Le but est de construire une courbe $C : y^2 = f(x)$ telle que le triplet de ses $\mathfrak{g}_2$-invariants $(g_1(\mathcal{C}), g_2(\mathcal{C}), g_3(\mathcal{C}))$ soit égal à (g_1, g_2, g_3). On note j_2, j_4, j_6 et j_{10} les invariants d'Igusa associés et $\mathcal{R}$ l'invariant de degré 15 .

1. Déterminer un triplet de covariants (q_1, q_2, q_3) d'ordre 2 et la quantité associée $R(q_1, q_2, q_3)$, que l'on note simplement R introduite dans la section 6.6.1.1. Cette dernière est un invariant. L'évaluation de R en les j_i est non nulle si et seulement si le triplet de covariants évalués en les j_i est linéairement indépendant. On suppose que c'est le cas ici.
2. Calculer la conique $L : \sum A_{i,j} x_i x_j = 0$ définie par (6.6.4). L est non singulière car son discriminant est $\frac{1}{2}R^2$. Elle est donc en particulier irréductible. Les $A_{i,j}$ sont des invariants évalués en les j_i.
3. Calculer la cubique $M : \sum a_{i,j,k} x_i x_j x_k$ définie par l'expression des coefficients $a_{i,jk}$ du membre de droite de (6.6.5) (vu comme un polynôme en les q_i^*). Les $a_{i,jk}$ sont des invariants évalués en les j_i.
4. Exploiter la proposition suivante pour déterminer f.

Proposition 38. *Soient q_1, q_2 et q_3 trois covariants d'ordre 2 d'une forme binaire de degré 6 définie sur k. Si $R \neq 0$ alors il existe un $\overline{k}$-isomorphisme $L \to \mathbb{P}^1$ qui envoie les points d'intersection de $L \cap M$ sur les racines de $f(X, Z)$. De plus, cet isomorphisme est défini sur :*

- *une extension au plus quadratique de k,*
- *k dès que L a un point rationnel.*

Démonstration. On considère le morphisme $\varphi : \mathbb{P}^1 \to L$ tel que $\varphi(x : z) = (q_1^*(x, z) : q_2^*(x, z) : q_3^*(x, z))$. Ce morphisme est bien défini car, d'après (6.6.4), $\Big(q_1^*(x, z) : q_2^*(x, z) : q_3^*(x, z)\Big)$ est un point de L. À présent, on montre que φ est un isomorphisme.
Soit $(X : Y : Z) \in L$, on cherche x, z tels que $\Big(q_1^*(x, z) : q_2^*(x, z) : q_3^*(x, z)\Big) = (X : Y : Z)$. On note A la matrice des q_i^* dans la base x^2, xz, z^2. On cherche donc à résoudre le système projectif :

$$A. \begin{pmatrix} x^2 \\ xz \\ z^2 \end{pmatrix} = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

Le déterminant de A est $-1/4R^2$. Puisque $R \neq 0$, la matrice A est inversible. φ est donc un isomorphisme. De plus, si $\varphi(x : z)$ est un point de $L \cap M$ alors, d'après (6.6.5), $6! \cdot R^3 \cdot f(x, z) = 0$. Il s'ensuit $f(x, z) = 0$ car $R \neq 0$ et on a supposé $p \neq 2, 3, 5$. En conséquence, $(x : z)$ est une racine de f. Réciproquement, si $(x : z)$ est une racine de f alors, d'après (6.6.5) et (6.6.4), $\varphi(x : z)$ est un point de $L \cap M$.

□

Cette proposition donne un paramétrisation rationnelle de L qui envoie les points d'intersection de $L \cap M$ sur les abscisses des points de Weirstraß de la courbe $\mathcal{C} : y^2 = f(x, z)$. Cependant, on ne connait ni f, ni ses covariants pour la reconstruction. La paramétrisation (q_1^*, q_2^*, q_3^*) reste donc inconnue. Par suite, ce résultat n'est pas directement exploitable pour la reconstruction. Néanmoins, toutes les paramétrisations rationnelles de L sont $\mathrm{GL}_2(\overline{k})$ équivalentes. Il suffit donc de choisir une paramétrisation rationnelle de L et d'envoyer les points de $L \cap M$ dans $\mathbb{P}^1$. Pour cela, on choisit un point affine de L qu'on appelle $(\xi : \eta : 1)$. On note K le corps de définition de $(\xi : \eta : 1)$. Puisque L est une conique sur k, $K = k$ ou K est une extension quadratique de

k. À partir de ce point, on paramétrise la conique de la façon suivante. On considère la droite passant par $(\xi : \eta : 1)$ d'équation

$$\begin{cases} x_1 = \xi + \alpha t \\ x_2 = \eta + \beta t \\ x_3 = 1 \end{cases} \quad \text{avec } t \in K.$$

On suppose que $\beta \neq 0$ et on pose $y = \beta t$, $x = \frac{\alpha}{\beta}$. On a donc

$$L(\xi + xy : \eta + y : 1) = ay^2 + by$$

avec a et b des polynômes en x tels que $(a, b) \neq (0, 0)$. On cherche les points d'intersection de la conique L avec la cubique M. Le point $(\xi + xy : \eta + y : 1)$ appartient à L si et seulement si $y = 0$ ou $ay = -b$. Si $(\xi + xy : \eta + y : 1) \in L \cap M$ alors $M(a\xi - bx : a\eta - b : a) = 0$. Réciproquement, si on pose $f(x) = M(a\xi - bx : a\eta - b : a)$ alors $f(x) = 0$ et par suite, $(a\xi - bx : a\eta - b : a)$ est un point de M. On pose $y = -b/a$; le point $(a\xi - bx : a\eta - b : a) = (\xi + xy : \eta + y : 1)$ est un point de L. Donc, $(a\xi - bx : a\eta - b : a)$ est un point de $M \cap L$. Ainsi, en posant $f(x) = M(a\xi - bx : a\eta - b : a)$, $f(x) = 0$ si et seulement si $(a\xi - bx : a\eta - b : a) \in L \cap M$.

6.6.2 Construction de la conique L et de la cubique M.

Dans ce paragraphe, on note

$$f = a_6x^6 + a_5x^5z + a_4x^4z^2 + a_3x^3z^3 + a_2x^2z^4 + a_1xz^5 + a_0z^6$$

une sextique binaire générique sur un corps k de caractéristique différente de 2. On va construire une conique L et une cubique M qui permettent la reconstruction par la méthode de Mestre. Les expressions de leur coefficients en fonction des J_i et de $\mathcal{R}$ peuvent être obtenues grâce à l'annexe B.3.4.

6.6.2.1 Caractéristique 0 ou ≥ 7

Covariants	ordre	degré
$i = (f, f)_4$	4	2
$\Delta = (i, i)_2$	4	4
$c_1 = (f, i)_4$	2	3
$c_2 = (i, y_1)_2$	2	5
$c_3 = (i, y_2)_2$	2	7
$c_4 = (y_1, y_2)_1$	2	8

Dans ce cas, il suffit de poser $q_1 = c_1$, $q_2 = c_2$ et $q_3 = c_3$. On a $R(q_1, q_2, q_3) = \frac{1}{2 \cdot 3^9 \cdot 5^{10}} \cdot \mathcal{R}(f)$. Puisque $\mathcal{R} \neq 0$, les trois covariants considérés sont linéairement indépendants.

A partir des covariants du tableau précédent, on va définir des covariants bien définis en petite caractéristique. Dans ce but, on multiplie c_i par de bonnes constantes :

$$y_1 = (2 \cdot 3^2 \cdot 5^3) \cdot c_1,\ y_2 = (2 \cdot 3^3 \cdot 5^5) \cdot c_2,\ y_3 = (2 \cdot 3^4 \cdot 5^7) \cdot c_3 \text{ et } y_4 = (2^2 \cdot 3^5 \cdot 5^6) \cdot c_4.$$

Dans la suite, on note $\overline{y_i}$ (resp. $\overline{J_i}(f)$ et $\overline{\mathcal{R}}(f)$) la réduction de y_i (resp. $J_i(f)$ et $\mathcal{R}(f)$) en caractéristique p.

6.6.2.2 Caractéristique 3

On exploite encore la méthode en caractéristique 3 avec quelques modifications. On pose $q_1 = \overline{y}_1$, $q_2 = \overline{y}_2$ et $q_3 = \overline{y}_3$. Un calcul montre que $\det(q_1, q_2, q_3) = 2 \cdot \mathcal{R}(f)$. Ainsi puisque $\mathcal{R} \neq 0$, les trois covariants considérés sont linéairement indépendants. Pour calculer les coefficients de L, on utilise uniquement des opérations de transvection d'indice inférieur ou égal à 2. Ces opérations sont donc bien définies. On construit ainsi $L = \sum A_{ij} x_i x_j$, où $A_{ij} = (q_i, q_j)_2$ pour tout $i, j \in \{1, 2, 3\}$.

Le calcul de M est un peu plus délicat. En effet, en effectuant les calculs de la partie droite de la formule (6.6.5), on obtient une expression nulle, ce qui est en accord avec le fait que la partie gauche l'est trivialement en caractéristique 3. Afin de palier à cela, on effectue tout d'abord les calculs en caractéristique 0 en utilisant les y_i. On s'aperçoit alors qu'on obtient une expression dont tous les coefficients sont divisibles par 9. On peut alors diviser les deux membres de l'égalité de (6.6.5) par 9 pour obtenir une relation valide en caractéristique 3 et pour laquelle on peut appliquer l'algorithme de Mestre. Les équations explicites sont données ci-dessous.

$$
\begin{aligned}
M = {} & (-3200000J_{10} + (-288000J_4 + 600J_2^2)J_6 - 100J4J_2^3 + 3200J_4^2J_2 + J_2^5)x_1^3 + \\
& (4000000J_{10}J_2 + 2160000J_6^2 + (-1600J_2^3 + 432000J_4J_2)J_6 - 128000J_4^3 - 320J_4J_2^4 + \\
& 3.J_2^6 + 10400J_4^2J_2^2)x_1^2x_2 + \\
& ((32000000J_4 - 2400000J_2^2)J_{10} - 160000J_4^3J_2 + 13000J_4^2J_2^3 - 2700000J_6^2J_2 - \\
& 180000J_6J_4J_2^2 - 340J_4J_2^5 + 3J_2^7)x_1^2x_3 + \\
& ((32000000J_4 - 2400000J_2^2)J_{10} - 160000J_4^3J_2 + 13000J_4^2J_2^3 - 2700000J_6^2J_2 - \\
& 180000J_6J_4J_2^2 - 340J_4J_2^5 + 3J_2^7)x_1x_2^2 + \\
& ((16000000J_4J_2 + 1200000J_2^3 + 960000000J_6)J_{10} + (43200000J_4 + 3060000J_2^2)J_6^2 + \\
& (-1800J_2^5 + 260000J_4J_2^3 - 960000J_4^2J_2)J_6 + 2560000J_4^4 - 496000J_4^3J_2^2 + \\
& 29800J_4^2J_2^4 + 6J_2^8 - 720J_4J_2^6)x_1x_2x_3 + \\
& ((-800000J_2^4 - 200000000J_6J_2 - 320000000J_4^2 + 28000000J_4J_2^2)J_{10} - 108000000J_6^3 + \\
& (-5400000J_4.J_2 - 1405000J_2^3)J_6^2 + (-880000J_4^2J_2^2 - 3000J_4J_2^4 - 550.J_2^6 + \\
& 6400000J_4^3)J_6 + 17350J_4^2J_2^5 - 380J_4J_2^7 + 3.J_2^9 + 2240000J_4^4J_2 - 334000J_4^3J_2^3)x_1x_3^2 + \\
& ((-8000000J_4J_2 + 400000J_2^3 - 80000000J_6)J_{10} + (-7200000J_4 + 1140000J_2^2)J_6^2 + \\
& (2200J_2^5 - 100000J_4J_2^3 + 1760000J_4^2J_2)J_6 + 1280000J_4^4 - 136000J_4^3J_2^2 + 5800J_4^2J_2^4 + J_2^8 - 120J_4J_2^6)x_2^3 + \\
& ((-1400000J_2^4 - 800000000J_6J_2 - 960000000J_4^2 + 64000000J_4J_2^2)J_{10} + 54000000J_6^3 + \\
& (-37800000J_4J_2 - 760000J_2^3)J_6^2 + (7700000J_4^2J_2^2 - 318000J_4J_2^4 + 3200J_2^6 - 60800000J_4^3)J_6 + \\
& 18600J_4^2J_2^5 - 380J_4J_2^7 + 3J_2^9 + 3520000J_4^4J_2 - 414000J_4^3J_2^3)x_3x_2^2 + \\
& (160000000000J_{10}^2 + ((20000000000.J_4 + 100000000J_2^2)J_6 + 70000000J_4J_2^3 - 1200000000J_4^2J_2 - \\
& 900000J_2^5)J_{10} + (648000000J_4^2 - 7200000J_4J_2^2 + 895000J_2^4)J_6^2 + (6480000J_4^2J_2^3 - \\
& 129000J_4J_2^5 + 1050J_2^7 - 94400000J_4^3J_2)J_6 - 12800000J_4^5 + 4880000J_4^4J_2^2 - 480000J_4^3J_2^4 + \\
& 20350J_4^2J_2^6 - 400J_4J_2^8 + 3J_2^{10})x_3^2x_2 + \\
& ((3200000000J_4^3 - 20000000000J_6^2 + 24000000J_4J_2^4 - 350000J_2^6 - 100000000J_6J_2^3 - \\
& 520000000J_4^2J_2^2)J_{10} + (19500000J_2^2 - 1260000000J_4)J_6^3 + (-80000J_2^5 - 10250000J_4J_2^3 + \\
& 122000000J_4^2J_2)J_6^2 + (-29000000J_4^3J_2^2 + 1325000J_4^2J_2^4 + 50J_2^8 + 224000000J_4^4 - \\
& 23500J_4J_2^6)J_6 + J_2^{11} + 2300000J_4^4J_2^3 - 193500J_4^3J_2^5 + 7550J_4^2J_2^7 - 9600000J_4^5J_2 - 140J_4J_2^9)x_3^3
\end{aligned}
$$

et

$$\begin{aligned}L = &(-3600J_6 - 160J_4J_2 + 3J_2^3)x_1^2+\\ &(6000J_6J_2 + 6400J_4^2 - 360J_4J_2^2 + 6J_2^4)x_1x_2+\\ &(-1600000J_{10} + (-96000J_4 - 800J_2^2)J_6 - 400J_4J_2^3 + 6400J_4^2J_2 + 6.J_2^5)x_1x_3+\\ &(-800000J_{10} + (-48000J_4 - 400J_2^2)J_6 - 200J_4J_2^3 + 3200J_4^2J_2 + 3J_2^5)x_2^2+\\ &(360000J_6^2 + (-8000J_4J_2 + 2400J_2^3)J_6 + 10000J_4^2J_2^2 - 440J_4J_4^2 + 6J_2^6 - 64000J_4^3)x_2x_3+\\ &((-600000J_2^2 + 8000000J_4)J_{10} - 150000J_6^2J_2 + (300J_2^4 - 38000J_4J_2^2 + 320000J_4^2)J_6+\\ &3J_2^7 - 240J_4J_2^5 + 6100J_4^2J_2^3 - 48000J_4^3J_2)x_3^2.\end{aligned}$$

6.6.2.3 Caractéristique 5

Ce cas est plus difficile. En effet nous ne pouvons plus du tout réduire simplement le choix de covariants fait par Mestre puisque $\det(\overline{y}_1, \overline{y}_2, \overline{y}_3) = 0$. Plus précisément, on a

$$\overline{y}_1 = 4\overline{J}_2(f)c,\ \ \overline{y}_2 = 3\overline{J}_2(f)^2c \text{ et } \overline{y}_3 = \overline{J}_2(f)^3c \text{ avec } c = a_4x^2 + 3a_3xz + a_2z^2.$$

On va construire par des manipulations élémentaires sur les y_i trois autres covariants en caractéristique nulle de telle sorte qu'ils ne soient pas liés en caractéristique 5. Puisque $\overline{y}_2 = 2\overline{J}_2(f)\overline{y}_1$, $y_2 - 2J_2(f)y_1$ est un multiple de 5. En remplaçant y_2 par $y_2' = (y_2 - 2J_2(f)y_1)/5$, on obtient

$$\overline{y'}_2 = (\overline{J}_4(f) + 2\overline{J}_2(f)^2)c = \frac{\overline{J}_4(f) + 2\overline{J}_2(f)^2}{4\overline{J}_2(f)}\overline{y}_1.$$

On remplace encore y_2' par

$$y_2'' = (4J_2(f)y_2' - (J_4(f) + 2J_2(f)^2)y_1)/5 = 5^{-2}\cdot 2\cdot J_2(f)(y_2 - 4J_2(f)y_1) - 5^{-1}\cdot 4y_1(4J_4(f) + 3J_2(f)^2).$$

De façon analogue, on construit un troisième covariant y_3' tel que $\overline{y'}_3$ soit génériquement linéairement indépendant (i.e. avec les coefficients génériques a_i) de $\overline{y}_1$ et $\overline{y''}_2$. Cela se fait de la manière suivante

$$\begin{aligned}y_3' = &5^{-3}\cdot 3\cdot J_2(f)(3y_3 + 2J_2(f)y_2 + 4J_2(f)^2y_1) + 5^{-2}\cdot J_2(f)(2J_4(f) + J_2(f)^2)y_1 -\\ &5^{-1}\cdot 2\cdot (J_6(f) + J_4(f)J_2(f) + 3J_2(f)^3)y_1.\end{aligned}$$

Dans la base x^2, xz, z^2, le déterminant de $\overline{y}_1$, $\overline{y''}_2$ et $\overline{y'}_3$ vaut $\overline{J}_2(f)^2\overline{\mathcal{R}}(f)$. Les trois covariants sont donc indépendants si et seulement si $J_2(f) \neq 0$. On traitera donc le cas $J_2(f) = 0$ à part.

Cas où $J_2 \neq 0$. On considère les covariants $q_1 = y_1$, $q_2 = y_2''$ et $q_3 = y_3'$ et $\overline{q}_i$ la réduction de q_i en caractéristique 5. Puisque $J_2 \neq 0$ et $\mathcal{R} \neq 0$, $\overline{q}_1$, $\overline{q}_2$ et $\overline{q}_3$ sont linéairement indépendants.

On construit :

— la conique $L = \sum_{i,j} A_{i,j}x_ix_j$ avec $A_{i,j} = (q_i, q_j)_2$ pour $i, j \in \{1, 2, 3\}$,

— la cubique $M = \sum_{i,j,k} x_ix_jx_k$ grâce à (6.6.5).

On appelle $\overline{L}$ et $\overline{M}$ les réductions de L et M en caractéristique 5. La cubique a l'expression suivante.

$$\begin{aligned}\overline{M} = &\Big(2\overline{J}_2(f)^2x_1 + (3\overline{J}_2(f)^4 + 4\overline{J}_2(f)^2\overline{J}_4(f) + \overline{J}_4(f)^2 + 2.\overline{J}_2(f)\overline{J}_6(f))x_2 + (\overline{J}_2(f)^5 +\\ &3\overline{J}_2(f)^3\overline{J}_4(f) + 3\overline{J}_2(f)\overline{J}_4(f)^2 + \overline{J}_2(f)^2\overline{J}_6(f) + 4\overline{J}_4(f)\overline{J}_6(f))x_3\Big)\overline{L}.\end{aligned}$$

Pour conclure avec la méthode de Mestre, il faut que le côté gauche de l'égalité (6.6.5) ne soit pas identiquement nul. Or c'est le cas puisque $5|6!$. Nous allons donc transformer la cubique M afin de faire ressortir un multiple de 5 qui n'apparaît pas pour le moment. Ceci se fait en soustrayant

à M un facteur linéaire fois l'équation de L (ce qui ne modifie pas la valeur en les q_i^* de la partie droite de (6.6.5) et donc l'égalité avec f).

$$M' = \Big(M - \{2.J_2(f)^2x_1 + (3.J_2(f)^4 + 4.J_2(f)^2J_4(f) + J_4(f)^2 + 2.J_2(f)J_6(f))x_2 + (J_2(f)^5 + 3.J_2(f)^3J_4(f) + 3.J_2(f)J_4(f)^2 + J_2(f)^2J_6(f) + 4.J_4(f)J_6(f))x_3\}L\Big)/5.$$

Puisque les coefficients de $\overline{M'}$ et $\overline{L}$ sont des invariants de degré pair, on peut les exprimer en fonction de $\overline{J}_2(f)$, $\overline{J}_4(f)$, $\overline{J}_6(f)$ et $\overline{J}_{10}(f)$. Après avoir évaluation en les J_i, on obtient

$$\begin{aligned}\overline{L} = {} & J_2^3x_1^2 + \\ & 2(4J_2^5 + 2J_2^3J_4 + 3J_2J_4^2 + J_2^2J_6)x_1x_2 + \\ & 2(3J_2^6 + 4J_2^4J_4 + 4J_2^2J_4^2 + 3J_2^3J_6 + 2J_2J_4J_6)x_1x_3 + \\ & (J_2^7 + J_2^5J_4 + 2J_2^3J_4^2 + J_2J_4^3 + J_2^2J_4J_6 + 2J_4^2J_6)x_2^2 + \\ & 2(2J_2^8 + 2J_2^6J_4 + 2J_2^2J_4^3 + J_2^5J_6 + J_2^3J_4J_6 + J_2J_4^2J_6 + J_2^2J_6^2 + 3J_4J_6^2 + 3J_2^3J_{10})x_2x_3 + \\ & (4J_2^9 + 4J_2^7J_4 + J_2^5J_4^2 + 3J_2^3J_4^3 + J_2^6J_6 + J_2^4J_4J_6 + 3J_2^2J_4^2J_6 + 2J_2^3J_6^2 + 2J_2J_4J_6^2 + \\ & 2J_6^3 + 3J_2^4J_{10} + 4J_2^2J_4J_{10})x_3^2\end{aligned}$$

et

$$\begin{aligned}\overline{M'} = {} & (3J_2^3J_4)x_1^3 + \\ & (4J_2^7 + 3J_2^5J_4 + J_2J_4^3 + J_2^2J_4J_6)x_1^2x_2 + \\ & (3J_2^8 + 2J_2^6J_4 + 3J_2^4J_4^2 + 3J_2^2J_4^3 + 2J_2^3J_4J_6 + 4J_2J_4^2J_6 + J_2^2J_6^2)x_1^2x_3 + \\ & (2J_2^9 + J_2^7J_4 + 3J_2^5J_4^2 + J_2^6J_6 + 4J_2^4J_4J_6 + 4J_2^2J_4^2J_6 + 2J_4^3J_6 + 3J_2^3J_6^2 + J_2^4J_{10})x_1x_2^2 + \\ & (3J_2^{10} + 2J_2^8J_4 + J_2^6J_4^2 + 2J_2^2J_4^4 + 3J_2^7J_6 + 3J_2^5J_4J_6 + 3J_2^3J_4^2J_6 + 2J_2J_4^3J_6 + 3J_2^4J_6^2 + \\ & J_2^2J_4J_6^2 + J_4^2J_6^2 + J_2^3J_4J_{10})x_1x_2x_3 + \\ & (3J_2^{11} + J_2^7J_4^2 + 2J_2^5J_4^3 + J_2^3J_4^4 + 3J_2^4J_4^2J_6 + 4J_2^2J_4^3J_6 + 3J_2^5J_6^2 + 3J_2^3J_4J_6^2 + 3J_2J_4^2J_6^2 + \\ & 4J_2^2J_6^3 + 2J_4J_6^3 + J_2^6J_{10} + 4J_2^4J_4J_{10} + 4J_2^2J_4^2J_{10} + 3J_2^3J_6J_{10})x_1x_3^2 + \\ & (4J_2^{11} + 3J_2^9J_4 + 4J_2^7J_4^2 + 4J_2J_4^5 + 2J_2^8J_6 + 3J_2^6J_4J_6 + J_2^4J_4^2J_6 + J_4^4J_6 + J_2^5J_6^2 + J_2^3J_4J_6^2 + \\ & 4J_2J_4^2J_6^2 + 2J_2^6J_{10} + 2J_2^3J_6J_{10})x_2^3 + \\ & (4J_2^{12} + 4J_2^{10}J_4 + 4J_2^8J_4^2 + 4J_2^6J_4^3 + J_2^4J_4^4 + 2.J_2^2J_4^5 + 4J_2^9J_6 + 3J_2^7J_4J_6 + J_2^5J_4^2J_6 + \\ & J_2^3J_4^3J_6 + 3J_2J_4^4J_6 + 2J_2^6J_6^2 + 2J_2^4J_4J_6^2 + 4J_2^2J_4^2J_6^2 + 3J_4^3J_6^2 + J_2^3J_6^3 + 2J_2J_4J_6^3 + 4J_2^7J_{10} + \\ & 3J_2^5J_4J_{10} + 2J_2^3J_4^2J_{10} + J_2J_4^3J_{10} + 2J_2^4J_6J_{10} + 2J_2^2J_4J_6J_{10})x_2^2x_3 + \\ & (3J_2^{13} + 3J_2^9J_4^2 + 2J_2^5J_4^4 + J_2^3J_4^5 + 2J_2^{10}J_6 + J_2^8J_4J_6 + 4J_2^6J_4^2J_6 + 2J_2^4J_4^3J_6 + 2J_2^7J_6^2 + \\ & 2J_2^5J_4J_6^2 + 3J_2^3J_4^2J_6^2 + 4J_2J_4^3J_6^2 + 3J_2^4J_6^3 + J_2^2J_4J_6^3 + J_4^2J_6^3 + 4J_2J_6^4 + 3J_2^2J_4^3J_{10} + \\ & 2J_2^5J_6J_{10} + 3J_2^3J_4J_6J_{10} + 3J_2J_4^2J_6J_{10} + 3J_2^2J_6^2J_{10})x_2x_3^2 + \\ & (2J_2^{14} + 3J_2^{12}J_4 + 2J_2^{10}J_4^2 + 2J_2^8J_4^3 + 2J_2^6J_4^4 + 3J_2^4J_4^5 + 4J_2^{11}J_6 + J_2^7J_4^2J_6 + J_2^8J_6^2 + \\ & J_2^4J_4^2J_6^2 + 4J_2^2J_4^3J_6^2 + 3J_2^5J_6^3 + 3J_2^3J_4J_6^3 + 4J_2J_4^2J_6^3 + 4J_2^2J_6^4 + 3J_2^9J_{10} + 3J_2^7J_4J_{10} + \\ & J_2^3J_4^3J_{10} + 4J_2^2J_4^2J_6J_{10} + 2J_2^3J_6^2J_{10} + J_2J_4J_6^2J_{10} + 2J_2^4J_{10}^2)x_3^3.\end{aligned}$$

Cas où $J_2 = 0$. Les covariants considérés précédemment ne sont plus linéairement indépendants, il faut en choisir d'autres. On pose :

$$q_1 = \frac{1}{25}J_2(f)(2y_2 + J_2(f)y_1) - \frac{1}{5}y_1(3J_4(f) + J_2(f)^2),$$

$$q_2 = y_4,$$

$$q_3 = \frac{3}{5}J_2(f)y_3 + \frac{3}{5}J_2(f)^2y_2 + \frac{2}{5}J_4(f)y_2 + \frac{2}{5}J_2(f)^3y_1 + \frac{1}{5}J_2(f)J_4(f)y_1.$$

Les coefficients de ces 3 covariants sont bien réductibles en caractéristique 5. Lorsque $\overline{J}_2(f) = 0$, le déterminant de $\overline{q}_1$, $\overline{q}_2$ et $\overline{q}_3$, dans la base $\{x^2, xz, z^2\}$, est $2J_4(f)^6$.

Supposons tout d'abord que $J_4 \neq 0$. De même que précédemment, la réduction de l'équation de la cubique est un multiple de celle de la conique :

$$\overline{M} = \Big((3J_2^4 + 4J_2^2J_4 + J_4^2 + 2J_2J_6)x_1 + (2J_2^3J_4 + 3J_2J_4^2)x_3\Big)\overline{L}.$$

De manière similaire au paragraphe précédent, on pose

$$M' := (M - (3J_2^4 + 4J_2^2J_4 + J_4^2 + 2J_2J_6)x_1 + (2J_2^3J_4 + 3J_2J_4^2)x_3)L)/5$$

et on peut alors conclure à la validité de la méthode de Mestre dans ce cas également.

Après avoir évalué en les J_i, on obtient les formules suivantes.

$$\overline{M'} = J_4^2J_6x_1^3 + 4\,\mathcal{R}\,x_1^2x_2 + (J_4^4 + 4J_4J_6^2)x_1^2x_3 + (J_4^4 + 4J_4J_6^2)x_1x_2^2 + 2J_4^3J_6x_1x_3^2 + 3J_4^5x_3^3$$

et

$$\overline{L} = 2J_6x_1^2 + 2J_4^2x_1x_3 + 2J_4^2x_2^2.$$

Remarque 31. *La présence de $\mathcal{R}$ n'est pas gênante pour la reconstruction sur le corps de modules. On effectue le changement de la preuve du lemme 5 (p. 58) et on obtient ainsi une expression de $\mathcal{R}$ (et de nouvelles valeurs des J_i) définie sur le corps de modules.*

On suppose maintenant que $J_4 = 0$ (on a toujours $J_2 = 0$). On peut directement construire une famille de courbe ayant les invariants voulus.

Proposition 39. *Soient $(g_1, g_2, g_3) \in \mathcal{M}_2$ et j_2, j_4, j_6 et j_{10} les invariants d'Igusa associés. Si $j_2 = j_4 = 0$ alors une courbe ayant ces invariants est définie par $y^2 = x^5 + j_6x^2 + 2j_{10}$.*

Démonstration. Soient $\mathcal{C}$ la courbe d'équation $y^2 = x^5 + j_6x^2 + 2j_{10}$ et $J_2(\mathcal{C})$, $J_4(\mathcal{C})$, $J_6(\mathcal{C})$ et $J_{10}(\mathcal{C})$ ses invariants d'Igusa. Grâce à la fonction `IgusaInvariants(C)` de `magma`, on trouve :

$$J_2(\mathcal{C}) = J_4(\mathcal{C}) = 0,\ \ J_6(\mathcal{C}) = J_6^4 \text{ et } J_{10}(\mathcal{C}) = J_6^5J_{10}.$$

On pose $\lambda = \sqrt{j_6}$. On obtient alors $J_6(\mathcal{C}) = \lambda^6 j_6$ et $J_{10}(\mathcal{C}) = \lambda^{10}j_{10}$. □

Appendice A

Implémentation sage

A.1 Fonctions auxiliaires

Soit $K \subset \mathbb{F}$ un sous-corps de $\mathbb{F}$ et $\mathbb{F} \subset L$ une extension de $\mathbb{F}$. Soit $a \in K$, cette fonction plonge a dans $\mathbb{F}$. Soit $a \in L$ tel que $a^{|\mathbb{F}|} = a$ cette fonction trouve un représentant dans $\mathbb{F}$ de a.

```
def change_field(a,FF):
# coerce an ellement a of a subfield of FF in FF or
# an element a of an extenttion of FF such that a^(#FF) = a in FF
    n = len(FF)
    if a^n <> a:
        print "The element is not in the field"
        assert a^n == a

    FFa = a.parent();na=len(FFa);
    if ZZ(na).is_prime() or ZZ(n).is_prime():
    # When FF is prime or FFa is prime, the coertion already exists in sage, just use it :-)
        return FF(a)

    genFFa = FFa.gen()
    genFF  = FF.gen()
    if n >= na:
    #the case a is in a non prime subfield of FF
        Pm= genFFa.minimal_polynomial()
        B = genFF^n
        n = n//na
        while Pm(B) <> 0:
            B*=genFF

        V = vector(a)
        A = 0
        for i in range(len(V)):
            A+= V[i]*B^i

    else:
    #the case a is in an extention of FF and FF is non prime
        Pm= genFF.minimal_polynomial()
        B = genFFa^n
        n = na//n
        while Pm(B) <> 0:
```

```
            B*=genFFa

        i = log(a,B)
        A = genFF^i
    return A
```

Étant donné un polynôme f et un corps $\mathbb{F}$, cette fonction projette f dans un anneau de polynômes construit sur $\mathbb{F}$ si la coercion est possible.

```
def change_field_polynom(f,FF):
    PFF.<X> = PolynomialRing(FF)
    F = 0*X
    for i in range(f.degree()+1):
        F+=change_field(f[i],FF)*X^i
    return F
```

Étant donné une suite d'entiers v de taille n et un corps fini $\mathbb{F} = \mathbb{F}_{p^n}$, cette fonction renvoie l'élément du corps $\sum_{i=0}^{n-1} v[i]a^i$ avec a un générateur du corps $\mathbb{F}$.

```
def elt_seq(v,FF):
    a = FF.gen()
    n = len(v)
    e = 0
    for i in range(n):
e+=v[i]*a^i
    return e

def pre_image_element(V,w):
    W = w.parent()
    for v in V:
if W.coerce_map_from(V)(v) == w:
return v

def pre_images(W,V):
    im = []
    pim =[]
    for v in V:
        w = W.coerce_map_from(V)(v)
        if not w in pim:
            im +=[w]
            pim +=[v]
    return pim

def matrix_action(f,M):
    N = M^(-1)
    P = f.parent();x=P.gen()
    return P(f((N[0,0]*x+N[0,1])/(N[1,0]*x+N[1,1]))*(N[1,0]*x+N[1,1])^6)

def random_model(f):
# compute f(M.x) where M is a invertible matrix
    FF = f.base_ring()
    GL2 = MatrixSpace(FF,2,2)
    P = f.parent();x = P.gen()
    P.<X,Z> = PolynomialRing(FF,2)
```

```
    M = GL2.random_element()
    while M.is_invertible()==false:
        M = GL2.random_element()
    g = P(f(Z/X)*X^6)
    return g(M[0,0]*X+M[0,1]*Z,M[1,0]*X+M[1,1]*Z)(x,1),M.det()

def transvectant(F,G,r):
    Q,Qdeg,n = F
    R,Rdeg,m = G
    n = ZZ(n)
    m = ZZ(m)
    K = Q.parent().base_ring()
    h = 0
    for k in range(r+1):
        h +=(-1)^k*binomial(m-k,r-k)*Q.derivative(r-k)*binomial(n-r+k,k)*R.derivative(k)
    h *=factorial(r)*factorial(m-r)*factorial(n-r)/(factorial(m)*factorial(n))
    return [h,Qdeg+Rdeg,m+n-2*r]
```

A.2 Calcul d'invariants

A.2.1 Les invariants d'Igusa

```
def formal_igusa_invariants():
    Cst.<a0,a1,a2,a3,a4,a5,a6> = PolynomialRing(QQ,7)
    P.<x> = PolynomialRing(Cst)
    f = a6*x^6 + a5*x^5 + a4*x^4 + a3*x^3 + a2*x^2 +a1*x + a0
    i = transvectant([f,1,6],[f,1,6],4)
    delta = transvectant(i,i,2)
    y1 = transvectant([f,1,6],i,4)
    y2 = transvectant(i,y1,2)
    y3 = transvectant(i,y2,2)
    A = transvectant([f,1,6],[f,1,6],6)
    B = transvectant(i,i,4)
    C = transvectant(i,delta,4)
    D = transvectant(y3,y1,2)
    Ap = -120*A[0]
    Bp = -720*A[0]^2+6750*B[0]
    Cp = 8640*A[0]^3 - 108000*A[0]*B[0] + 202500*C[0]
    Dp = -62208*A[0]^5 + 972000*A[0]^3*B[0] + 1620000*A[0]^2*C[0]
     - 3037500*A[0]*B[0]^2 - 6075000*B[0]*C[0] - 4556250*D[0]
    J2 = 2^(-3)*Ap
    J4 = 2^(-5)*3^(-1)*(4*J2^2-Bp)
    J6 = 2^(-6)*3^(-2)*(8*J2^3-160*J2*J4 - Cp)
    J8 = 2^(-2)*(J2*J6-J4^2)
    J10= 2^(-12)*Dp
    return Cst(J2),Cst(J4),Cst(J6),Cst(J8),Cst(J10)

def igusa_invariant(C):
    f,h = C.hyperelliptic_polynomials()
    d = f.degree()
    if d == 5:
        a0,a1,a2,a3,a4,a5 = f.coeffs()
        a6 = a0*0
```

```
    else:
        a0,a1,a2,a3,a4,a5,a6 = f.coeffs()
    FF = a0.parent()
    p = FF.characteristic()
    J2,J4,J6,J8,J10 = formal_igusa_invariants()
    if p == 0:
        return J2(a0,a1,a2,a3,a4,a5,a6),
        J4(a0,a1,a2,a3,a4,a5,a6),
        J6(a0,a1,a2,a3,a4,a5,a6),
        J8(a0,a1,a2,a3,a4,a5,a6),
        J10(a0,a1,a2,a3,a4,a5,a6)

    else:
        q = ZZ(len(FF))
        if q.is_prime():
            a0 = QQ(a0);a1 = QQ(a1);a2 = QQ(a2);
            a3 = QQ(a3);a4 = QQ(a4);a5 = QQ(a5);a6 = QQ(a6);
            return
            FF(J2(a0,a1,a2,a3,a4,a5,a6)),
            FF(J4(a0,a1,a2,a3,a4,a5,a6)),
            FF(J6(a0,a1,a2,a3,a4,a5,a6)),
            FF(J8(a0,a1,a2,a3,a4,a5,a6)),
            FF(J10(a0,a1,a2,a3,a4,a5,a6))

        else:
            FFP.<x> = PolynomialRing(FF)
            a = FF.multiplicative_generator()
            pol = a.minimal_polynomial()
            QQP.<X> = PolynomialRing(QQ)
            pQQ = QQP(pol)
            A0 = QQP(list(vector(a0)))
            A1 = QQP(list(vector(a1)))
            A2 = QQP(list(vector(a2)))
            A3 = QQP(list(vector(a3)))
            A4 = QQP(list(vector(a4)))
            A5 = QQP(list(vector(a5)))
            A6 = QQP(list(vector(a6)))
            J2,J4,J6,J8,J10 = formal_igusa_invariants()
            return
            FFP((J2)(A0,A1,A2,A3,A4,A5,A6)%pQQ)(a),
            FFP((J4)(A0,A1,A2,A3,A4,A5,A6)%pQQ)(a),
            FFP((J6)(A0,A1,A2,A3,A4,A5,A6)%pQQ)(a),
            FFP((J8)(A0,A1,A2,A3,A4,A5,A6)%pQQ)(a),
            FFP((J10)(A0,A1,A2,A3,A4,A5,A6)%pQQ)(a)
```

A.2.2 Les fonctions de passage des invariants d'Igusa à d'autre types d'invariants

Cette fonction convertit les invariants d'Igusa en les invariants absolus de Cardona-Quer-Nart-Pujolas

```
def Igusa_to_g2_invariants(JI):
    taille = len(JI)
```

```
    if taille <>5:
        print"Argument must be a sequence of five Igusa J invariants."
    assert taille == 5

    J2 = JI[0]
    FF = parent(J2)
    if is_Integer(J2):
        FF = RationalField()
        GI = [FF(J2),FF(JI[1]),FF(JI[2]),FF(JI[3]),FF(JI[4])]

    bool = is_Field(FF)
    if not bool:
        print "Argument must be defined over a field."
    assert is_Field(FF)
    J2, J4, J6, J8, J10 = tuple(JI)

    # Characteristic 2 fields
    if FF.characteristic()==2:
        if J2<>0:
            return [Sqrt(J10/J2^5), Sqrt((J8/J2^4)-(J4/J2^2)^4-(J4/J2^2)^3), Sqrt(J4/J2^2)]

        if J6<>0:
            return [FF(0), Sqrt(J10^3/J6^5), Sqrt(Sqrt(Sqrt(J8*J10^4/J6^8)))]

        return [FF(0), FF(0), Sqrt(Sqrt(Sqrt(J8^5/J10^4)))]


    # Other fields
    if J2 <> 0:
        return [J2^5/J10, J2^3*J4/J10, J2^2*J6/J10]

    if J4 <> 0:
        return [FF(0), J4^5/J10^2, J4*J6/J10]

    return [FF(0), FF(0), J6^5/J10^3]
```

Cette fonction convertit les invariants absolus de Cardona-Quer-Nart-Pujolas en les invariants d'Igusa.

```
def g2_to_Igusa_invariants(GI):
    taille = len(GI)
    if taille <>3:
        print"Argument must be a sequence of three absolute invariants."
    assert taille == 3
    g1 = GI[0]
    FF = parent(g1)
    if is_Integer(g1):
        FF = RationalField()
        GI = [FF(g1),FF(GI[1]),FF(GI[2])]
    bool = is_Field(FF)
    if not bool:
        print "Argument must be defined over a field."
    assert is_Field(FF)
```

```
    g1 = GI[0];g2 = GI[1];g3 = GI[2]

    # Characteristic 2 fields
    if FF.characteristic()==2:
        if g1<>0:
            return [1, g3^2, g3^4, g2^2+g3^8+g3^6, g1^2]

        if g2<>0:
            return [FF(0), FF(0), g2^2, g3^8, g2^4]

        if g3<>0:
            return [ FF(0), FF(0), FF(0), g3^4, g3^3]

        return [ FF(0), FF(0), FF(0), FF(0), FF(1)];


    # Other fields
    if g1<>0:
        return [g1, g1*g2, g1^2*g3, (g1^3*g3-g1^2*g2^2)/4, g1^4]

    if g2<>0:
        return [FF(0), g2, g2*g3, -g2^2/4, g2^2]

    if g3<>0:
        return [FF(0), FF(0), g3^2, FF(0), g3^3];

    return [FF(0), FF(0), FF(0), FF(0), FF(1)]
```

Cette fonction transforme les invariants d'Igusa en les invariants de Clebsch. Cette fonction est valable en caractéristique $\neq 2, 3, 5$.

```
def igusa_to_clebsch(Ji):
J2,J4,J6,_,J10 = tuple(Ji)
FF = J2.parent()
Ap = FF(8)*J2
Bp = FF(4)*J2^2-FF(96)*J4
Cp = FF(8)*J2^3-FF(160)*J2*J4-FF(576)*J6
Dp = FF(4096)*J10
A = FF((-120)^(-1))*Ap
B = (FF(720*A^2)+Bp)*FF(6750^(-1))
C = (FF(-8640)*A^3+FF(108000)*A*B+Cp)*FF(202500^(-1))
D = (FF(62208)*A^5-FF(972000)*A^3*B-FF(1620000)*A^2*C+
FF(3037500)*A*B^2+FF(6075000)*B*C+Dp)*FF((-4556250)^(-1))
return [A,B,C,D]
```

Étant donnée une courbe hyperellitpique, cette fonction renvoie ses invariants absolus de Cardona-Quer-Nart-Pujolas.

```
def g2_invariants(C):
return Igusa_to_g2_invariants(igusa_invariant(C))
```

A.3 Reconstruction des courbes hyperelliptiques en genre g = 2

Étant donnée une forme quadratique Cr, cette fonction renvoie son modèle de Legendre $LAx^2 + By^2 + Cz^2$ ainsi qu'une liste représentant le morphisme de passage de Cr vers L.

```
def legendre_model(Cr):
# We use this function when Cr have no rational point.
    Up.<x,y,z> = PolynomialRing(Cr.base_ring(),3)
    L = Cr.coefficients()
    a = L[0];b = L[1];c = L[2];d = L[3];e = L[4];f = L[5]
    # Trivial case
    if b == 0 and c == 0 and e == 0:
        return a*x^2+d*y^2+f*z^2,[[1,0,0],[0,1,0],[0,0,1]]
    if a<>0:
        A = a
        B = d - b^2/(4*a)
        if B<>0:
            C = f - c^2/(4*a) - (e-b*c/(2*a))^2/(4*B)
            return A*x^2+B*y^2+C*z^2,[[1,b/(2*a),c/(2*a)],[0,1,(e-b*c/(2*a))/(2*B)],[0,0,1]]
        C = f - c^2/(4*a)
        if C<>0:
            B = d - b^2/(4*a) - (e-b*c/(2*a))^2/(4*C)
            return A*x^2+B*y^2+C*z^2,[[1,b/(2*a),c/(2*a)],[0,1,0],[0,(e-b*c/(2*a))/(2*C),1]]

    if d<>0:
        B = d
        C = f - e^2/(4*d)
        if C<>0:
            A = a - b^2/(4*d) - (c-b*e/(2*d))^2/(4*C)
            return A*x^2+B*y^2+C*z^2,[[1,0,0],[b/(2*d),1,e/(2*d)],[(c-b*e/(2*d))/(2*C),0,1]]
        A = a - b^2/(4*d)
        if A<>0:
            C = f - e^2/(4*d) - (c-b*e/(2*d))^2/(4*A)
            return A*x^2+B*y^2+C*z^2,[[1,0,(c-b*e/(2*d))/(2*A)],[b/(2*d),1,e/(2*d)],[0,0,1]]

    if f<>0:
        C = f
        A = a - c^2/(4*f)
        if A<>0:
            B = d - e^2/(4*f) - (b-c*e/(2*f))^2/(4*A)
            return A*x^2+B*y^2+C*z^2,[[1,(b-c*e/(2*f))/(2*A),0],[0,1,0],[c/(2*f),e/(2*f),1]]
        B = d - e^2/(4*f)
        if B<>0:
            A = d - c^2/(4*f) - (b-c*e/(2*f))^2/(4*B)
            return A*x^2+B*y^2+C*z^2,[[1,0,0],[(b-c*e/(2*f))/(2*B),1,0],[c/(2*f),e/(2*f),1]]
    # Otherwithe Cr is a conic with equation of the form
    # axy+bxz+cyz = 0 or (ax+by+cz)^2 = 0 or ax^2+byz = 0 up to permutation of the variable.
    # In this cases, Cr have a rational point
```

Cette fonction renvoie la partie sans facteur carré de i ainsi que la racine carrée de sa partie carrée.

```
def cheap_integer_square_free_part(i):
    sf = squarefree_part(i)
    a = ZZ(sqrt(i//sf))
    return sf, a

def cheap_rational_square_free_part(r):
```

```
an, bn = cheap_integer_square_free_part(numerator(r))
ad, bd = cheap_integer_square_free_part(Denominator(r))
return an*ad, bn/(ad*bd)

def mestre_find_point_on_conic(L,K):
# Find an affine point (x,y,1) on the projective conic L.
    UP.<u> = PolynomialRing(K)
    P.<x,y,z> = PolynomialRing(K,3)
    if K.is_field() and K.is_finite(): # When K is a finite field
        x1 = K.random_element()
        x3 = K(1)
        LL = L(x1,u,x3)
        r = LL.roots()
        while r == []:
            x1 = K.random_element()
            x3 = K(1)
            LL = L(x1,u,x3)
            r = LL.roots()
x2 = r[0][0]
        return x1,x2

    else:
     if K == QQ:
            C = Conic(L)
            #P = C.rational_point()
            if not C.has_rational_point():
                LL,m = legendre_model(C)
                i1 = LL.coefficient({x:2})
                i2 = LL.coefficient({y:2})
                i3 = LL.coefficient({z:2})
                b1, a1 = cheap_rational_square_free_part(-i3/i1)
                b2, a2 = cheap_rational_square_free_part(-i3/i2)
                if abs(b1) < abs(b2):
                    S.<b> = QuadraticField(b1)
                    Lsol  = [a1*b, 0, 1]
             else:
                    S.<b> = QuadraticField(b2)
                    Lsol  = [0, a2*b, 1]
             sol = [ m[0][0]*Lsol[0]+m[0][1]*Lsol[1]+m[0][2]*Lsol[2] ,
             m[1][0]*Lsol[0]+m[1][1]*Lsol[1]+m[1][2]*Lsol[2] ,
             m[2][0]*Lsol[0]+m[2][1]*Lsol[1]+m[2][2]*Lsol[2] ]
             return sol[0]/sol[2],sol[1]/sol[2]

     else:
         found = false
         while not found:
             S = C.random_rational_point()
                if S[2] <> 0:
                    found = true
                else:
                    pol = L(S[0],S[1],u) # pol = c*u*(u-t)
                    c = diff(diff(pol))
                    if c <> 0:
```

```
                        s3 = -diff(pol)/c
                        found = true

            assert L(list(S)) == 0
            if S[2] == 0:
                if s3 <> 0:
                    return S[0]/s3, S[1]/s3
## There is only one tangent line...
if S[0] == 0:
    pol = L(S[0]+u,S[1],u) # pol = c*u*(u-t)
else:
    pol = L(S[0],S[1]+u,u) # pol = c*u*(u-t)
    c = diff(diff(pol))
                    s3 = -diff(pol)/c
                    if s3 == 0:
                        print "Error in MestreFindPointOnConic"
                assert L(S[0],S[1],s3) == 0
                return S[0]/s3, S[1]/s3
            else:
                return S[0]/S[2], S[1]/S[2]
    print "Algorithm not available for this type of field.\n"

def clebsch_mestre_conic_and_cubic(GI):
# Compute a hyperelliptic Curve whith absolute invariants GI
    J = g2_to_Igusa_invariants(GI)
    J2 = J[0];J4 = J[1];J6 = J[2];J10= J[4]
    FF = J2.parent()
    p = FF.characteristic()
    P3.<x1,x2,x3> = PolynomialRing(FF, 3)

    # Clebsch-Mestres conics & cubics, as a function of Igusa Invariants
    if p == 5:

        if J2 == 0:

            # J4 <> 0
            R2 = J6^5+3*J10*J4^5+3*J6^3*J4^3+J6*J4^6
            if not R2.is_square():
                J4 *= R2^2; J6 *= R2^3; J10 *= R2^5; R2 *= R2^15

            R = sqrt(R2)
            L = J6*x1^2+4*J4^2*x2*x1+4*x3^2*J4^2
            M = (3*J4^4+4*J6^2*J4)*x1^2*x2 +
            (4*J4^4+3*J6^2*J4)*x1*x3^2 +
            2*J4^5*x2^3+J6*J4^2*x1^3+4*x1*J6*J4^3*x2^2+4*x3*x1^2*R
        else:

            L = J2*x1^2 +
            ((J4*J2^2+2*J4^2+J2^4+4*J2*J6)*x2 +
            (2*J2*J4^2+J6*J4+4*J2^5)*x3)*x1 +
            (J4^2*J2^3+4*J2^7+3*J6*J4^2+3*J4*J2^5+2*J4^3*J2)*x2^2 +
            (3*J2^3*J10+(3*J4+3*J2^2)*J6^2+(J2*J4^2+4*J2^5+J2^3*J4)*J6+2*J2^8+2*J2^6*J4+
            3*J2^2*J4^3+2*J2^4*J4^2)*x3*x2 +
```

```
        ((4*J4*J2^2+3*J2^4)*J10+2*J6^3+3*J6^2*J2^3+(2*J4*J2^4+3*J2^6+3*J4^2*J2^2)*J6+
        4*J2^9+J4^3*J2^3)*x3^2

        M1 = (3*J4*J2+3*J2^3)*x1^3
        M2 = (((2*J2^3+2*J4*J2)*J6+3*J4*J2^4+J2^6+2*J4^3+2*J4^2*J2^2)*x2+
        (4*J6^2*J2+(J4^2+3*J4*J2^2+J2^4)*J6+ 2*J4^3*J2+J4^2*J2^3+4*J4*J2^5+J2^7)*x3)*x1^2
        M3 = ((4*J10*J2^4+2*J6^2*J2^3+(4*J2^6+3*J4^3+J4^2*J2^2+2*J4*J2^4)*J6+2*J4^2*J2^5+
        J4^4*J2+3*J4^3*J2^3+J4*J2^7)*x2^2 + ((4*J2^5+3*J2^3*J4)*J10+
        (J4*J2^2+2*J2^4+3*J4^2)*J6^2+(3*J4*J2^5+3*J2^7+2*J4^2*J2^3+J4^3*J2)*J6+2*J2^10+
        2*J4^4*J2^2+J4*J2^8+3*J4^2*J2^6)*x3*x2 + ((4*J4^2*J2^2+J4*J2^4+3*J6*J2^3)*J10+
        (2*J4+4*J2^2)*J6^3+(4*J2*J4^2+2*J2^5)*J6^2+(J2^2*J4^3+2*J2^4*J4^2+J2^6*J4)*J6+
        3*J2^11+2*J4^3*J2^5+J4^4*J2^3+2*J4^2*J2^7)*x3^2)*x1
        M4 = ((J4*J2^5+J2^7+J6*J2^4)*J10+(3*J2^6+2*J4^2*J2^2+J4*J2^4)*J6^2+
        (3*J4^3*J2^3+J2^9+2*J4^2*J2^5)*J6+2*J4*J2^10+2*J2^12+3*J4^3*J2^6+
        4*J4^5*J2^2+3*J4^2*J2^8)*x2^3
        M5 = (((4*J2^5+2*J2^3*J4)*J6+J2^6*J4+4*J2^8+J2^2*J4^3+4*J2^4*J4^2)*J10+
        (2*J2^4+2*J4*J2^2)*J6^3+(J4*J2^5+4*J2^7+J4^2*J2^3+4*J4^3*J2)*J6^2+(4*J2^4*J4^3+
        2*J2^10+2*J4^2*J2^6+4*J4^4*J2^2+3*J4*J2^8)*J6+J4^5*J2^3+3*J4^2*J2^9+
        3*J4^3*J2^7+2*J2^13)*x3*x2^2
        M6 = ((J6^2*J2^3+(J4^2*J2^2+2*J2^6+2*J4*J2^4)*J6+2*J4^3*J2^3+J2^9+4*J4*J2^7)*J10+
        3*J6^4*J2^2+(2*J2^3*J4+J2^5+4*J2*J4^2)*J6^3+(3*J2^8+4*J2^4*J4^2+3*J2^2*J4^3)*J6^2+
        (J2^11+J4*J2^9+3*J4^4*J2^3)*J6+2*J4^5*J2^4+3*J4^4*J2^6+2*J4^2*J2^10)*x3^2*x2
        M7 = (3*J10^2*J2^5+((4*J4*J2^2+2*J2^4)*J6^2+(3*J4*J2^5+3*J4^2*J2^3+J2^7)*J6+
        J4^2*J2^6+3*J2^4*J4^3+2*J4*J2^8+3*J2^10)*J10+(J2^3+J4*J2)*J6^4+
        (J4^2*J2^2+3*J2^6+3*J4*J2^4)*J6^3+(2*J4^2*J2^5+2*J4^3*J2^3+4*J4*J2^7+J2^9)*J6^2+
        (3*J4^2*J2^8+4*J4^3*J2^6+4*J4^4*J2^4)*J6+J2^15+3*J4*J2^13+3*J4^2*J2^11+J4^4*J2^7+
        2*J4^3*J2^9)*x3^3

        M = M1  +  M2  +  M3  +  M4  +  M5  +  M6  +  M7

else:

    L = (-3600*J6-160*J4*J2+3*J2^3)*x1^2 + (6000*J6*J2+6400*J4^2-360*J4*J2^2+6*J2^4)*x1*x2 +
    (-1600000*J10+(-96000*J4-800*J2^2)*J6-400*J4*J2^3+6400*J4^2*J2+6*J2^5)*x1*x3 +
    (-800000*J10+(-48000*J4-400*J2^2)*J6-200*J4*J2^3+3200*J4^2*J2+3*J2^5)*x2^2 +
    (360000*J6^2+(-8000*J4*J2+2400*J2^3)*J6+10000*J4^2*J2^2-440*J4*J2^4+
    6*J2^6-64000*J4^3)*x2*x3 + ((-600000*J2^2+8000000*J4)*J10-150000*J6^2*J2+
    (300*J2^4-38000*J4*J2^2+320000*J4^2)*J6+3*J2^7-240*J4*J2^5+
    6100*J4^2*J2^3-48000*J4^3*J2)*x3^2

    M = (-3200000*J10+(-288000*J4+600*J2^2)*J6-100*J4*J2^3+3200*J4^2*J2+J2^5)*x1^3 +
    (4000000*J10*J2+2160000*J6^2+(-1600*J2^3+432000*J4*J2)*J6-128000*J4^3-320*J4*J2^4+
    3*J2^6+10400*J4^2*J2^2)*x1^2*x2 +
    ((32000000*J4-2400000*J2^2)*J10-160000*J4^3*J2+13000*J4^2*J2^3-2700000*J6^2*J2-
    180000*J6*J4*J2^2-340*J4*J2^5+3*J2^7)*x1^2*x3 +
    ((32000000*J4-2400000*J2^2)*J10-160000*J4^3*J2+13000*J4^2*J2^3-
    2700000*J6^2*J2-180000*J6*J4*J2^2-340*J4*J2^5+3*J2^7)*x1*x2^2 +
    ((16000000*J4*J2+1200000*J2^3+960000000*J6)*J10+(43200000*J4+3060000*J2^2)*J6^2+
    (-1800*J2^5+260000*J4*J2^3-960000*J4^2*J2)*J6+2560000*J4^4-496000*J4^3*J2^2+
    29800*J4^2*J2^4+6*J2^8-720*J4*J2^6)*x1*x2*x3 +
    ((-800000*J2^4-200000000*J6*J2-320000000*J4^2+28000000*J4*J2^2)*J10-108000000*J6^3+
    (-5400000*J4*J2-1405000*J2^3)*J6^2+(-880000*J4^2*J2^2-3000*J4*J2^4-550*J2^6+
```

```
        6400000*J4^3)*J6+17350*J4^2*J2^5-380*J4*J2^7+3*J2^9+2240000*J4^4*J2-
        334000*J4^3*J2^3)*x1*x3^2 +
        ((-8000000*J4*J2+400000*J2^3-80000000*J6)*J10+(-7200000*J4+1140000*J2^2)*J6^2+
        (2200*J2^5-100000*J4*J2^3+1760000*J4^2*J2)*J6+
        1280000*J4^4-136000*J4^3*J2^2+5800*J4^2*J2^4+J2^8-120*J4*J2^6)*x2^3 +
        ((-1400000*J2^4-800000000*J6*J2-960000000*J4^2+64000000*J4*J2^2)*J10+54000000*J6^3+
        (-37800000*J4*J2-760000*J2^3)*J6^2+(7700000*J4^2*J2^2-318000*J4*J2^4+3200*J2^6-
        60800000*J4^3)*J6+18600*J4^2*J2^5-380*J4*J2^7+3*J2^9+3520000*J4^4*J2-
        414000*J4^3*J2^3)*x3*x2^2 +
        (160000000000*J10^2+((20000000000*J4+100000000*J2^2)*J6+70000000*J4*J2^3-
        1200000000*J4^2*J2-900000*J2^5)*J10+(648000000*J4^2-7200000*J4*J2^2+
        895000*J2^4)*J6^2+(6480000*J4^2*J2^3-129000*J4*J2^5+1050*J2^7-94400000*J4^3*J2)*J6-
        12800000*J4^5+4880000*J4^4*J2^2-480000*J4^3*J2^4+20350*J4^2*J2^6-
        400*J4*J2^8+3*J2^10)*x3^2*x2 +
        ((3200000000*J4^3-20000000000*J6^2+24000000*J4*J2^4-350000*J2^6-
        100000000*J6*J2^3-520000000*J4^2*J2^2)*J10+(19500000*J2^2-1260000000*J4)*J6^3+
        (-80000*J2^5-10250000*J4*J2^3+122000000*J4^2*J2)*J6^2+(-29000000*J4^3*J2^2+
        1325000*J4^2*J2^4+50*J2^8+224000000*J4^4-23500*J4*J2^6)*J6+J2^11+
        2300000*J4^4*J2^3-193500*J4^3*J2^5+7550*J4^2*J2^7-9600000*J4^5*J2-140*J4*J2^9)*x3^3


    xi, eta = mestre_find_point_on_conic(L,FF)
    P3.<x1,x2,x3> = PolynomialRing(parent(xi), 3)
    pol = L(xi + x2*x1, eta + x1,1)
    a = pol.coefficient({x1:2})
    b = pol.coefficient({x1:1})
    P.<x> = PolynomialRing(parent(xi))
    f = M(xi*a-x2*b,a*eta-b,a)
    return HyperellipticCurve(f(0,x,0))

#
#   y^2 = x^6 - 1 in char <> 3, 5,
#   see [CaNa2007].
#
def g2_models_in_FF_2D12(GI):
FF = base_ring(GI[0])
P.<x> = PolynomialRing(FF)
return HyperellipticCurve(x^6 - 1)

#
#   y^2 = x^5 - x in char 5,
#   see [CaNa2007].
#

def g2_models_in_char_5_FF_G240(GI):
    FF = base_ring(GI[0])
    P.<x> = PolynomialRing(FF)
    return HyperellipticCurve(x^5 - x)

#
#   y^2 = x^5 - x in char <> 5,
#   see [CaNa2007].
#
```

```
def g2_models_in_FF_G48(GI):

    FF = base_ring(GI[0])
    P.<x> = PolynomialRing(FF)
    f = x^5-x
    return HyperellipticCurve(f)

#
#  y^2 = x^5 - 1,
#  see [CaNa2007].
#
def g2_models_in_FF_C10(GI):

    FF = base_ring(GI[0])
    P.<x> = PolynomialRing(FF)

    return HyperellipticCurve(x^5 - 1)

# y^2 = 1/t*x^6+x^4+x^2+1 in char 3, and its twists
def g2_models_in_char3_FF_D12(GI):

FF = base_ring(GI[0])
P.<x> = PolynomialRing(FF)
J2, J4, J6, _, J10 = tuple(g2_to_Igusa_invariants(GI))
t = (-J2^3/J6-x^3).roots()[0][0]
f = x^6+t*x^4+(t-1)*x^3+t*x^2+1
return HyperellipticCurve(f)

#
#   y^2 = x^6 + x^3 + t in char <> 3,
#   see [CaNa2007].
#
def g2_models_in_FF_D12(GI):

    FF = base_ring(GI[0])
    P.<x> = PolynomialRing(FF)
    p = FF.characteristic()

    Ji = g2_to_Igusa_invariants(GI)
    if p == 5:
        a = -1-Ji[1]/Ji[0]^2
    else:
        C2, C4, C6, C10 = tuple(igusa_to_clebsch(Ji))
        a = (3*C4*C6-C10)/50/C10


    return HyperellipticCurve(x^6+x^3+a)

#
#   y^2 = x^5 + x^3 + t*x,
#   see [CaNa2007].
#
def g2_models_in_FF_D8(GI):
```

```
    FF = base_ring(GI[0])
    P.<x> = PolynomialRing(FF)
    p = FF.characteristic()

    Ji = g2_to_Igusa_invariants(GI)

    if p == 3:
        t = -Ji[0]^2/Ji[1]
    else:
        if p==5:
            t= 1+Ji[2]/Ji[0]^2
        else:
            C2, C4, C6, C10 = tuple(igusa_to_clebsch(Ji))
            t = (8*C6*(6*C4-C2^2)+9*C10)/900/C10
    return HyperellipticCurve(x^5+x^3+t*x)

# V4 case,
#   see [ShVo2004], [CaQu2005]
def g2_models_in_FF_V4(GI):

    FF = base_ring(GI[0])
    P.<x> = PolynomialRing(FF)
    J2, J4, J6, _, J10 = tuple(g2_to_Igusa_invariants(GI))

    Au = J2^5*J4^2-64*J2^3*J4^3+1024*J2*J4^4+3*J2^6*J6-202*J2^4*J4*J6+4014*J2^2*J4^2*J6-
    20160*J4^3*J6+666*J2^3*J6^2-20520*J2*J4*J6^2+48600*J6^3-30*J2^4*J10+
    2800*J2^2*J4*J10-192000*J4^2*J10-360000*J2*J6*J10

    Bu = 2*J2^4*J4*J6-114*J2^2*J4^2*J6+1344*J4^3*J6+6*J2^3*J6^2+216*J2*J4*J6^2-3240*J6^3+
    18*J2^4*J10-1040*J2^2*J4*J10+12800*J4^2*J10+4800*J2*J6*J10

    Av = J2^6*J4^2-96*J2^4*J4^3+3072*J2^2*J4^4-32768*J4^5+3*J2^7*J6-164*J2^5*J4*J6+
    1250*J2^3*J4^2*J6+29760*J2*J4^3*J6+858*J2^4*J6^2-22680*J2^2*J4*J6^2-172800*J4^2*J6^2+
    81000*J2*J6^3+1176*J2^5*J10-79600*J2^3*J4*J10+1344000*J2*J4^2*J10-72000*J2^2*J6*J10-
    12960000*J4*J6*J10-134400000*J10^2

    Bv = 3*J2^3*J4^2*J6-160*J2*J4^3*J6+J2^4*J6^2-36*J2^2*J4*J6^2+3456*J4^2*J6^2-1188*J2*J6^3+
    24*J2^3*J4*J10-1280*J2*J4^2*J10+160*J2^2*J6*J10+105600*J4*J6*J10+640000*J10^2

    u = Au/Bu;v = Av/Bv
    if u <> 0:
t = v^2-4*u^3
a0= v^2+u^2*v-2*u^3
a1= 2*(u^2+3*v)*(v^2-4*u^3)
a2= (15*v^2-u^2*v-30*u^3)*(v^2-4*u^3)
a3= 4*(5*v-u^2)*(v^2-4*u^3)^2
    else:
t = FF(1)
a0= 1+2*v
a1= 2*(3-4*v)
a2= 15+14*v
a3= 4*(5-4*v)
```

```
    f = a0*x^6+a1*x^5+a2*x^4+a3*x^3+t*a2*x^2+t^2*a1*x+t^3*a0
    return HyperellipticCurve(f)

#
#   Generic case.
#
#   Everything here is based on [Mestre91], especially the conic and
#   cubic used in finite fields of characteristic 3 or > 5.
#
#   In characteristic 5, we had to face difficulties, mostly because
#   the covariants used to define the cubics and conics given
#   in [Mestre91] are no more a basis, and we had to consider other covariants.
#   This yields new conics and cubics that we use here.
#
################################

def g2_models_in_FF_C2(GI):

    FF = base_ring(GI[0])
    P.<x> = PolynomialRing(FF)
    p = FF.characteristic()
    J2, J4, J6, _, J10 = tuple(g2_to_Igusa_invariants(GI))
    _, _, g3 = tuple(GI);

    if p == 5 and J2 == 0 and J4 == 0:
c = FF.random_element()
roo = (x^3-3*c^2/g3).roots()
ret = len(roo)>0
while c == 0 and not ret:
c = FF.random_element()
roo = (x^3-3*c^2/g3).roots()
ret = len(roo)>0
a = roo[0][0]
H = HyperellipticCurve(x^5+c*x^2+a*c)
    else:
H = clebsch_mestre_conic_and_cubic(GI)

    return H

#
# Switching routine
#
###################


def g2_models(GI, models = true):

    FF = base_ring(GI[0])
    g1, g2, g3 = tuple(GI)
    p = FF.characteristic()
    twists = []
    # y^2 = x^6-1
```

```
    if p <> 3 and p <> 5 and GI == [ FF(6400000/3), FF(440000/9), FF(-32000/81) ]:
if models:
    twists = g2_models_in_FF_2D12(GI)

return twists,SymmetricGroup(12).subgroup([(1,3,2,4,6,5,10,12,11,7,9,8),
(9,8,7,12,11,10,6,5,4,3,2,1)])

    # y^2 = x^5-x */
    if GI == [ FF(50000), FF(3750), FF(-125)]:
       if p == 5:
   if models:
       twists = g2_models_in_char_5_FF_G240(GI)

#    return twists, SmallGroup(240,90);
   return twists, "2 cover of S5"

       if models:
   twists = g2_models_in_FF_G48(GI)

       return twists, SymmetricGroup(8).subgroup([(2,1,3,4,7,8,5,6),(3,4,5,6,1,2,7,8)])

    # y^2 = x^5-1, p <> 5
    if GI == [ FF(0), FF(0), FF(0) ]:
        if models:
    twists = g2_models_in_FF_C10(GI)

        return twists, CyclicPermutationGroup(10)


    J2, J4, J6, _, J10 = tuple(g2_to_Igusa_invariants(GI))

    if p == 3:
       # y^2 = 1/t*x^6+x^4+x^2+1
       if J4 == 0 and J10 + 2*J6*J2^2 == 0:
   if models:
       twists = g2_models_in_char3_FF_D12(GI)

   return twists, DihedralGroup(6)

    else:
if p == 5:
        # y^2 = x^6+x^3+t
        if J10*J4*J2^2 + J6^3 + 3*J6*J4^3 + 2*J4^4*J2 == 0 and
 J10*J2^3 + 3*J6^2*J4 + 4*J4^4 + 2*J4^3*J2^2 == 0 and J6*J2 + 2*J4^2 == 0:
    if models:
        twists = g2_models_in_FF_D12(GI)

                return twists, DihedralGroup(6)

    else:
        # y^2 = x^6+x^3+t
        if 750*J10+90*J6*J4-3*J6*J2^2-J4^2*J2 == 0 and
```

```
 2700*J6^2+540*J6*J4*J2-27*J6*J2^3+160*J4^3-9*J4^2*J2^2 == 0:
    if models:
        twists = g2_models_in_FF_D12(GI)

            return twists, DihedralGroup(6)

    # y^2 = x^5+x^3+t*x
    if p <> 5:
       if 172800*J6^2-23040*J6*J4*J2+592*J6*J2^3-40960*J4^3+3584*J4^2*J2^2-104*J4*J2^4+
       J2^6 == 0 and 128000*J10+5760*J6*J4-192*J6*J2^2-1024*J4^2*J2+64*J4*J2^3-J2^5 == 0:
   if models:
       twists = g2_models_in_FF_D8(GI)

   return twists, DihedralGroup(4)

    else:
       if [ J10*J4^5 + 4*J6^5 + 2*J6^3*J4^3 + 2*J4^6*J2^3 + 2*J4^4*J2^7 + 4*J4^3*J2^9 + 2*J2^15 ,
       J10*J4^3*J2 + 2*J6^4 + 3*J6^2*J4^3 + 3*J4^6 + J4^5*J2^2 + 3*J4^4*J2^4 + 2*J4^3*J2^6 +
       J4^2*J2^8 + 2*J4*J2^10 + 3*J2^12 ,
       J10*J4*J2^2 + J6^3 + 3*J4^4*J2 + 2*J4^2*J2^5 + 4*J4*J2^7 + 2*J2^9 , J10*J2^3 + 3*J6^2*J4 +
       3*J4^4 + J4^2*J2^4 + 3*J2^8 ,
       J6*J2 + 2*J4^2 + 3*J4*J2^2 + 3*J2^4 ] == [FF(0),FF(0),FF(0),FF(0),FF(0)]:
   if models:
       twists = g2_models_in_FF_D8(GI)

   return twists, DihedralGroup(4)

    R = J2^6*J6^3 - 2*J2^5*J4^2*J6^2 - 72*J2^5*J4*J6*J10 - 432*J2^5*J10^2 + J2^4*J4^4*J6 +
    8*J2^4*J4^3*J10 - 72*J2^4*J4*J6^3 - 48*J2^4*J6^2*J10 + 136*J2^3*J4^3*J6^2 +
    4816*J2^3*J4^2*J6*J10 + 28800*J2^3*J4*J10^2 + 216*J2^3*J6^4 - 64*J2^2*J4^5*J6 -
    512*J2^2*J4^4*J10 + 1080*J2^2*J4^2*J6^3 - 12960*J2^2*J4*J6^2*J10 - 96000*J2^2*J6*J10^2 -
    2304*J2*J4^4*J6^2 - 84480*J2*J4^3*J6*J10 - 512000*J2*J4^2*J10^2 - 7776*J2*J4*J6^4 -
    129600*J2*J6^3*J10 + 1024*J4^6*J6 + 8192*J4^5*J10 + 6912*J4^3*J6^3 +
    691200*J4^2*J6^2*J10 + 11520000*J4*J6*J10^2 + 11664*J6^5 + 51200000*J10^3

    if R == 0:
if models:
    twists = g2_models_in_FF_V4(GI)

return twists,
direct_product_permgroups([CyclicPermutationGroup(2),CyclicPermutationGroup(2)])

    if models:
twists = g2_models_in_FF_C2(GI)

    return twists, CyclicPermutationGroup(2)
```

Appendice B

Implémentation magma

B.1 Tordues

B.1.1 Cas non hyperelliptique

Cette fonction renvoie un élément non nul de la matrice `M` si elle est non nulle et un message d'erreur sinon.

```
NonZeroElement := function(M)
  N := Nrows(M);
  for j in [1 .. N] do
    for i in [1 .. N] do
      if M[i,j] ne 0 then
        return M[i,j];
      end if;
    end for;
  end for;
  printf("Error, your matrix is zero");
  return 0;
end function;
```

Étant donné un groupe `G` et un corps fini `F`, cette fonction renvoie les classes de cohomologie de `G` (voir la définition 5 (p. 8)).

```
CohomologyClass := function(G,F)
  n := #G;
  L := G;
  e := Degree(F); // cardinal of F is p^e
  CohoClass := [**];
  while not IsEmpty(L) do
    Append(~CohoClass,L[1]);
    if not IsEmpty(L) then
        for i in [1 .. n] do
        EqClassCoho := FrobeniusImage(G[i],e)*CohoClass[#CohoClass]*G[i]^(-1);
Exclude(~L,1/NonZeroElement(EqClassCoho)*EqClassCoho);
        end for;
   end if;
  end while;
  return CohoClass;
end function;
```

Étant donnée une matrice `M` définie sur une extension du corps fini `F`, cette fonction renvoie une liste (m,λ) telle que $\mathtt{M}^{\varsigma^{m-1}} \dots \mathtt{M}^{\varsigma}\mathtt{M} = \lambda Id$ (voir la proposition 4 (p. 12)).

```
OrderAutomorphism := function(M,F)
  e := Degree(F);
  H := M;
  P := M;
  m := 1;
  while not IsScalar(P) do
    P := FrobeniusImage(P,e)*H;
    m := m+1;
  end while;
 return [*m, P[1, 1]*];
end function;
```

Cette fonction renvoie la matrice `M` sur son corps minimal de définition.

```
MCorpsMinimal := function(M)
  Fs := BaseRing(M);
  F := PrimeField(Fs);
  p := Characteristic(F);
  r := Degree(Fs);
  D := Divisors(r);
  Exclude(~D,r);
  for i in D do
    if FrobeniusImage(M,i) eq M then
      K := ext<F | i>;
      Embed(K,Fs);
      return Matrix(K, M);
    end if;
  end for;
  return M;
end function;
```

Étant donnés une matrice `M` définie sur une extension du corps fini `F`, cette fonction calcule la matrice de descente `A` de la proposition 5 (p. 13).

```
ComputationInvertibleMatrix := function(M,F)
  M := MCorpsMinimal(M);
  Z := Integers();
  Fs := BaseRing(M);                 // in fact Fs is an F extension.
  N := Nrows(M);
  r := Degree(Fs);
  e := Degree(F);
  L := OrderAutomorphism (M,F);
  m := L[1] ;
  K1 := ext<F | m>;
  Embed(Fs,K1); // it can be done because r divide m
  _,X := NormEquation(K1,F!L[2]); //L[2] is necesary in F
  Mb := ChangeRing(M,K1)*1/X;
  repeat
    Ab := RandomMatrix(K1,N,N);
    A := Ab;
    for i in [1 ..m-1] do
      Ab := FrobeniusImage(Ab,e)*Mb;
      A :=  A + Ab;
    end for;
```

```
  until IsUnit(A);
// in this step we have computed A such that FrobeniusImage(A,e)^(-1)*A=Mb
  return A;
end function;
```

Étant donnée une matrice de descente `A` et `f`, cette fonction renvoie l'équation de la tordue de `f` associée à `A`.

```
ComputationOfTwist := function(A,f)
  K := BaseRing(A);
  N := Nrows(A);
  AF := Parent(f);
  AK := PolynomialRing(K,N);
  P := [];
  for i in [1..N] do
    c := 0*AK.1;
    for j in [1..N] do
    c := c + A[i,j]*AK.j;
    end for;
    Append(~P,c);
  end for;
  g := Evaluate(AK!f,P);
  g:=g/LeadingCoefficient(g);
  return AF!g;
end function;
```

Cette fonction renvoie `true` si la matrice `A` est défini sue l'anneau `R` et `false` sinon

```
IsInRing := function(A,R)
  N := Nrows(A);
  for j in [1 .. N] do
    for i in [1 .. N] do
      if not A[i,j] in R then
        return false;
      end if;
    end for;
  end for;
  return true;
end function;
```

Étant donnés une liste de matrices `L`, les deux fonctions suivantes calculent le groupe d'automorphisme qu'elle génère.

```
ComputationOfGroupGeneratadByList := function(L)
  n := #L;
  m := 0;
  G := L;
  // Normalisation of the genrators
  for i in [1..n] do
    M :=G[i];
    G[i] := 1/NonZeroElement(M)*M;
  end for;
  while n ne m do
    m := n;
    for B in G do
```

```
      for C in G do
        P := 1/NonZeroElement(C*B)*C*B;
        if not (P in G) then
          Append(~G,P);
          n := n + 1;
        end if;
      end for;
    end for;
  end while;
return G;
end function;

ProjectiveMatrixGroup:=function(L)
n:=Nrows(L[1]);
FF:=BaseRing(L[1]);
prim:=PrimitiveElement(FF);
MM:=MatrixAlgebra(FF,n);
H := MatrixGroup< n, FF | L cat [prim*Identity(MM)]>;
C:= MatrixGroup< n, FF | [prim*Identity(MM)]>;
phi,I,K:=CosetAction(H,C);
psi:=Inverse(phi);
return [MM!psi(h) : h in I], I;
end function;
```

Étant donné une courbe projective `CC` et son groupe d'automorphismes `G` représenté par une liste de matrices, cette fonction calcules les équations des tordues de `CC`.

```
Tordues := function(G,CC)

  // Normalisation of the elements of G;
  n := #G;
  for i in [1 .. n] do
    G[i] := 1/NonZeroElement(G[i])*G[i];
  end for;
  T := []; //future list of the twists of C with #Aut(C') : a list of [Phi',#Aut(C')]
  C := CC;
  f := Polynomial(C);
  F := BaseRing(C);
  AF := Parent(f); x := AF.1; y := AF.2; z := AF.3;
  Coh := CohomologyClass(G,F);//printf("Des tordues il y en a ");#Coh;
  for M in Coh do
    A := ComputationInvertibleMatrix(M,F);
    ff := ComputationOfTwist(A^(-1),f);
    Append(~T,ff);
  end for;
  return T;
end function;
```

B.1.2 Cas Hyperelliptique

Ce programme se sert du package `isgl2equiv.m` qui est une implémentation de [LR12] (la méthode est reprise dans le paragraphe 2.1.5). Ce package permet de calculer le groupe d'automorphismes réduits de la courbe $\mathcal{C}$. On se sert aussi des fonction du programme précédent.

Étant donné le polynôme hyperelliptique d'une courbe C, cette fonction renvoie le genre de $\mathcal{C}$.

```
Genre:= function(f)
  Z := Integers();
  d := Degree(f);
  if d mod 2 eq 0 then
    return Z!(d/2-1);
  end if;
  return Z!((d-1)/2);
end function;
```

Étant donné un polynôme d'un seule variable `f`, cette fonction renvoie le groupe d'automorphismes (géométrique) de la courbe hyperelliptique $y^2 = \mathtt{f}(x)$ en utilisant le package `isgl2equiv.m`.

```
CreationAutomorphismGroup:= function(f)
  g := Genre(f); //Genus of C
  _,L := IsGL2GeometricEquivalent(f,f,2*g+2); //function of "isgl2equiv.m"
  G := [];
  n := #L;
  F := PrimeField(Parent(L[1][1]));
  p := #F;
  N := 1;
  for i in [1 .. n] do
    FF := Parent(L[i][1]);
    N := Lcm(N,Integers()!Log(p,#FF));
  end for;
  FFk<a> := GF(p^N); // Minimal extension how contain all the coeficients of elements of L
  for i in [1 .. n] do
    M := L[i];
    Embed(Parent(M[1]),FFk);
    M := Matrix(FFk, 2, 2,M);
    Append(~G,1/NonZeroElement(M)*M);
    // Definition of the elements of G as matrix 2X2 normalised by the function NonZeroElement
  end for;
  return G;
end function;
```

Étant donnés une matrice de descente `A` et `f`, cette fonction renvoie le polynôme hyperelliptique de la tordue associée à `A`.

```
ComputationOfTwist := function(A,f)
  g := Genre(f); // Genus of C
  K<a> := BaseRing(A);
  N := Nrows(A);
  AF := Parent(f);
  AF2<x,z> := PolynomialRing(BaseRing(AF),2);
  KAF2 := FunctionField(AF2);
  f := AF2!(Evaluate(KAF2!f,x/z)*z^(2*g+2));
  AK<X,Z> := PolynomialRing(K,N);
  P := [];
  for i in [1..N] do
    c := 0*AK.1;
```

```
    for j in [1..N] do
    c := c + A[i,j]*AK.j;
    end for;
    Append(~P,c);
  end for;
  g := Evaluate(AK!f,P);
  g := AF2!(g/LeadingCoefficient(g));
  g := Evaluate(g,[AF.1,1]);
  return AF!g;
end function;
```

Étant donné le groupe des automorphismes réduits `G` de de la courbe $y^2 = \texttt{f}(x)$, `f` ainsi que la matrice de descente `A`, cette fonction calcule le groupe des automorphismes réduits de la tordue associée à `A`. Cette fonction se sert des résultats du paragraphe 2.1.4.

```
ReducedAutomorphisimGroupOfTwistDefinedOverF := function(G,f,A)
  F := BaseRing(f);
  g := Genre(f); // Genus of C
  K<a> := BaseRing(A);
  Embed(F,K);
  r := Nrows(A);
  AF := Parent(f);
  AF2<x,z> := PolynomialRing(BaseRing(AF),2);
  KAF2 := FunctionField(AF2);
  f := AF2!(Evaluate(KAF2!f,x/z)*z^(2*g+2));
  AK<X,Z> := PolynomialRing(K,r);
  L := []; // List of the reduced Automorphism
  eN := []; // List of the associate constant to find the Automorphisms
  for M in G do
    N := MCorpsMinimal(M);
    P := A^-1*N*A;
    l := NonZeroElement(P);
    P := 1/l*P;
    if IsInRing(P,F) then
      if not P in L then
        Append(~L,P);
        Append(~eN,AK!(l^(-2*g-2))*Evaluate(f,[AK!N[1,1]*X + AK!N[1,2]*Z, AK!N[2,1]*X + AK!N[2,2]*
        // I have to multiply by l^(-2*g-2) because e(1/l*P) = e(1/l*N) =1/l^(2g+2)e(N) = 1/l^(2g+
      end if;
    end if;
  end for;
  return [*L,eN*];
end function;
```

Étant donné `[*L,eN*]` donné par la fonction précédente, cette fonction renvoie `true` si la courbe $y^2 = f(x)$ est autoduale et `false` sinon. Cette fonction se sert des résultats du paragraphe 2.1.4.

```
IsSelfDual := function(RAGT,f)
  F := BaseRing(f);
  size := #RAGT[2];
  Numb := 0;
  for i in [1..size] do
    e := RAGT[2][i];
    if e in F and IsSquare(F!e) then
```

```
      Numb := Numb+2;
    end if;
  end for;
  return Numb eq size;
end function;
```

Étant donnée une courbe Hyperelliptique `C`, cette fonction calcule ses tordues.

```
Tordues := function(C)

  f := HyperellipticPolynomials(C);
  G := CreationAutomorphismGroup(f); // creation of the automorphism group of the curve C
  T := [];
  F := BaseRing(f);
  RF<x> := Parent(f);
  Q := FieldOfFractions(RF);
  Coh := CohomologyClass(G,F);
  t := PrimitiveElement(F);
  for M in Coh do
    if IsScalar(M) then
      A := M;
      ff := f;
      Append(~T,C);
    else
      A := ComputationInvertibleMatrix(M,F);
      ff := ComputationOfTwist(A^(-1),f);
      Append(~T,HyperellipticCurve(ff));
    end if;
    RAGT := ReducedAutomorphisimGroupOfTwistDefinedOverF(G,f,A^(-1));
    if not IsSelfDual(RAGT,f) then
      Append(~T,HyperellipticCurve(t*ff));
    end if;
  end for;
  return T;
end function;
```

B.2 Identification du groupe d'automorphisme d'une courbe hyperelliptique

Après avoir expliqué comment on a procédé, on donnera le programme qui :
— reconnaît le groupe d'automorphismes G d'une courbe hyperelliptique $\mathcal{C}$ définie sur un corps k,
— donne un système de générateurs pour G.

On s'est servi des résultats de la thèse d'Huggins, [Hug05], en particulier, le lemme 2.2.1 de la page 25. Lors du test de notre programme, on c'est rendu compte qu'un cas particulier manquait. On a ainsi complété notre programme en utilisant [Suz82, th.6.17 p.404].

B.2.1 Reconnaissance

B.2.1.1 Les cas où p ne divise pas G ou $p = 0$

Le lemme [Hug05, 2.2.1 p.25] décline 5 types possibles pour les sous-groupes de $\mathrm{PGL}_2(\overline{k})$:

1. les groupes cycliques $\mathbf{C}_n$ pour tout entier n strictement positif,

2. les groupes diédraux $\mathbf{D}_{2n}$ pour tout entier n strictement positif,
3. le groupe alterné sur 4 éléments $\mathcal{A}_4$,
4. le groupe symétrique sur 4 élément $\mathcal{S}_4$,
5. le groupe alterné sur 5 éléments $\mathcal{A}_5$.

On peut reconnaître nos groupes en s'intéressant aux éléments d'ordre 2. En effet, les groupes cycliques sont les seuls de cette liste à avoir au plus un élément d'ordre 2. De plus, les groupes diédraux sont les seuls à avoir exactement $|G|/2 + (|G|/2 + 1 \mod 2)$ éléments d'ordre 2. Les trois autres groupes ont $|G|/2$ éléments d'ordre 2. Cela ne pose pas de problème car $|G|/2$ est pair dans ces trois cas. Par ailleurs, les cardinaux de $\mathcal{A}_4$, $\mathcal{S}_4$ et $\mathcal{A}_5$ sont tout trois différents. On procède donc de la façon suivante :

— On calcule les éléments d'ordre 2 de G. La fonction `ListOfElementsOfOrderN` fournit tous les éléments d'ordre au plus égal à 2.
— S'il y en a qu'un, on est dans le cas $\mathbf{C}_n$.
— S'il y en a $|G|/2 + (|G|/2 + 1 \mod 2)$, on est dans le cas $\mathbf{D}_{2n}$.
— On sépare les trois autres groupes en calculant le cardinal de G.

B.2.1.2 Le cas où p divise G

Dans ce cas, [Hug05] précise qu'il existe 3 types de sous-groupes finis de $\mathrm{PGL}_2(\overline{k})$:

1. les groupes projectifs linéaires $\mathrm{PGL}_2(\mathbb{F}_q)$ sur $\mathbb{F}_q$ avec q une certaine puissance de p,
2. les groupes projectifs spéciaux linéaires $\mathrm{PSL}_2(\mathbb{F}_q)$ sur $\mathbb{F}_q$ avec q une certaine puissance de p et
3. des groupes
$$G_{\beta,A} = \left\{ \begin{pmatrix} \beta^k & a \\ 0 & 1 \end{pmatrix} : a \in A, k \in \mathbb{Z} \right\}$$
où A est un sous-groupe additif de $\overline{k}$ contenant 1 et β une racine de l'unité telle que $\beta A = A$.

Remarque 32. *On testant notre programme, on c'est rendu compte qu'il manquait un cas particulier. En effet, lorsque $p = 3$, un autre groupe apparait, il s'agit de $\mathrm{SL}_2(\mathbb{F}_5)$. La preuve de ceci ce trouve dans [Suz82, th.6.17 p.404]. On doit donc rajouter ce cas. pour $p = 3$.*

Les groupes $\mathrm{PGL}_2(\mathbb{F}_q)$ et $\mathrm{PSL}_2(\mathbb{F}'_q)$ sont faciles à distinguer car ils n'ont jamais le même cardinal quelles que soient q et q' deux puissances de p. De plus, on verra que $G_{\beta,A}$ ne peut pas avoir un cardinal égal à un cardinal de $\mathrm{PGL}_2(\mathbb{F}_q)$ ou $\mathrm{PSL}_2(\mathbb{F}_q)$. Cela nous permettra de reconnaître ces 3 groupes en calculant le cardinal de G. On note n l'ordre de β. On considère le morphisme de groupes :

$$G_{\beta,A} \to < \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} > \subset G_{\beta,A}$$

$$\begin{pmatrix} \beta^k & a \\ 0 & 1 \end{pmatrix} \to \begin{pmatrix} \beta^k & 0 \\ 0 & 1 \end{pmatrix}.$$

Le noyau de ce morphisme est le groupe $\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in A \right\}$ isomorphe à A. Ainsi, le cardinal de $G_{\beta,A}$ est :

$$|G_{\beta,A}| = n|A|.$$

En outre, $|A|$ est une puissance de p et β une racine primitive de l'unité. Afin que $G_{\beta,A}$ soit de même cardinal qu'un groupe projectif linéaire (resp. spécial linéaire), il faudrait donc que $n = |A|^2 - 1$ (resp. $n = (|A|^2 - 1)/2$). Or $\beta^k \in A$ pour tout k. C'est pourquoi, il faudrait que $|A|^2 - 1 \leq |A|$ (resp $(|A|^2 - 1)/2 \leq |A|$). Ceci est impossible puisqu'on est en caractéristique $\neq 2$.

En caractéristique 3, on a aussi le groupe $\mathrm{SL}_2(\mathbb{F}_5)$. Ce dernier est isomorphe à $\mathcal{A}_5$. Il a donc 60 éléments. Il est facilement distinguable $\mathrm{PGL}_2(\mathbb{F}_q)$ et de $\mathrm{PSL}_2(\mathbb{F}_q)$ car ces dernier ne peuvent pas être de cardinal 60 en caractéristique 3. Enfin, on peut aussi le distinguer de $G_{\beta,A}$ par les ordres des éléments. En effet, si $G_{\beta,A}$ est de cardinal 60 alors $|A|$ ne peut être que de cardinal 3 et $G_{\beta,A}$ contient donc un élément d'ordre 20. $\mathrm{SL}_2(\mathbb{F}_5)$ n'en contient pas.

Néanmoins, on peut séparer nos cas selon le cardinal du groupe G en procédant de la façon suivante :

— Si $|G|$ est de la forme $(q-1)q(q+1)$ alors c'est un $\mathrm{PGL}_2(\mathbb{F}_q)$. La fonction `IsCardinalOfA_PGL2` permet de détecter ce cas dans le programme suivant.
— S'il est de la forme $(q-1)q(q+1)/2$ alors c'est un $\mathrm{PSL}_2(\mathbb{F}_q)$. La fonction `IsCardinalOfA_PSL2` permet de décider cela dans le programme suivant.
— Si $p = 3$ et $|G| = 60$ et G n'a pas d'éléments d'ordre 20 alors c'est $\mathrm{SL}_2(\mathbb{F}_5)$.
— Sinon, G est un groupe du type $G_{\beta,A}$.

B.2.1.3 L'algorithme séparant les cas

Pour la reconnaissance du groupe, on procède de la façon suivante :

1. On calcule la caractéristique p du corps k et le cardinal $|G|$ de G.
2. Si p divise $|G|$ alors on applique la partie B.2.1.2.
3. Sinon, on applique la partie B.2.1.1.

B.2.2 Générateurs

De nouveau, on sépare notre propos selon que p divise l'ordre du groupe ou pas. Dans ce cas là, on procède de la façon suivante :

1. Dans le cas $\mathbf{C}_n$, il suffit de trouver un élément d'ordre n en utilisant la fonction `ElementOfOrderN`.
2. Dans le cas $\mathbf{D}_{2n}$, il suffit de trouver un élément E d'ordre n et un élément d'ordre 2 qui n'est pas dans l'orbite de E. Pour cela, on se sert de la fonction `ElementOutOfOrbitOfE`
3. Dans le cas $\mathcal{A}_4$, il suffit de trouver un élément d'ordre 2 et un d'ordre 3.
4. Dans le cas $\mathcal{S}_4$, il suffit de trouver un élément d'ordre 2 et un d'ordre 4 tel que le produit des deux soit d'ordre 3.
5. Dans le cas $\mathcal{A}_5$, il suffit de trouver un élément d'ordre 3 et un d'ordre 5.

Dans le cas où p divise l'ordre de G, on procède de la façon suivante :

1. On sait que $\mathrm{SL}_2(\mathbb{F}_q)$ et, par suite, $\mathrm{PSL}_2(\mathbb{F}_q)$ sont engendrés par les matrices de transvection qui sont d'ordre p. Après avoir calculé toutes les matrices d'ordre p de G, on aura un système de générateurs. Pour un peu le réduire, on choisit qu'un élément par orbite de matrice d'ordre p, grâce la fonction `ElementOfOrder_p`.
2. On sait que $\mathrm{GL}_2(\mathbb{F}_q)$ et, par suite, $\mathrm{PGL}_2(\mathbb{F}_q)$ sont engendrés par les matrices de transvection et de dilatation. On reprend le même raisonnement que précédemment pour les matrices d'ordre p. Puisqu'on est dans $\mathrm{PGL}_2(\mathbb{F}_q)$, on suppose que les matrices de dilatation ont leur coefficient de dilatation à la première ligne et la première colonne. En conséquence, toutes les matrices de dilatation de $\mathrm{PGL}_2(\mathbb{F}_q)$ sont engendrées par une seule matrice de dilatation d'ordre $q-1$. Il suffit donc de rajouter à notre système une matrice d'ordre $q-1$. Dans ce but, on utilise la fonction `GeneratorOfPGL`.
3. Le groupe $\mathrm{SL}_2(\mathbb{F}_5)$ est isomorphe à $\mathcal{A}_5$, il suffit de trouver un élément d'ordre 3 et un d'ordre 5.
4. Dans le cas $G_{\beta,A}$, le groupe est engendré par : $M_\beta = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix}$ et par $M_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ où $a \in A$. On va montré qu'on n'est pas obligé de prendre tous les éléments de la forme M_a pour $a \in A$. Si n est l'ordre de β, on sait que :

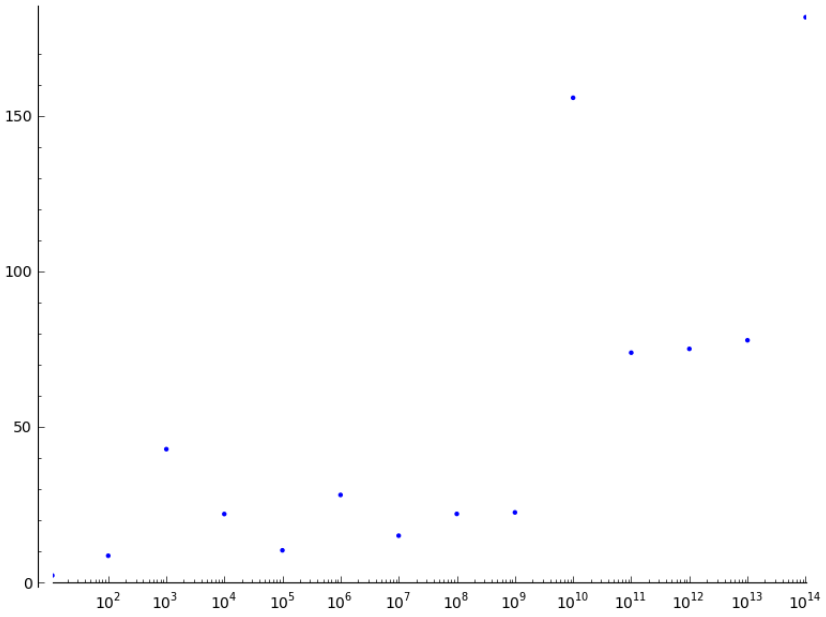
— M_β est d'ordre n,
— $|G_{\beta,A}| = n|A|$,
— n'importe quel élément de $G_{\beta,A}$ est de la forme $M_a M_{\beta^k}$ avec $a \in A$ et $k \in \mathbb{Z}$,
— un tel élément est d'ordre l'ordre de β^k lorsque $k \neq 0 \mod n$,
— p ne divise pas n.

Il s'ensuit que seuls les éléments d'ordre p de $G_{\beta,A}$ sont les éléments de la forme M_a avec $a \in A\backslash\{0\}$. Ainsi, on prend un élément de chaque orbite d'éléments d'ordre p et on complète avec un élément d'ordre n. Pour cela, on utilise la fonction `GeneratorOfGbetaA`.

Voici quelques tests statistiques donnant un aperçu des limites de notre programme.

Lorsque l'on fixe une courbe et que l'on fait varier le corps de définition On considère la courbe $\mathcal{C}$ d'équation $y^2 = x^{47} - 1$ sur le corps $\mathbb{F}_p$. La figure B.1 représente les temps de calcul (en secondes) de l'algorithme sur $\mathcal{C}$ lorsque l'on fait varier son corps de définition.

FIGURE B.1 – Temps de calcul de l'algorithme de reconnaissance du groupe d'automorphismes réduits de la courbe hyperelliptique $y^2 = x^{47} - 1$ sur le corps $\mathbb{F}_p$. Le cardinal de $\mathbb{F}_p$ est représenté en abscisse avec une échelle logarithmique. En ordonné, le temps de calcul est représenté en secondes.

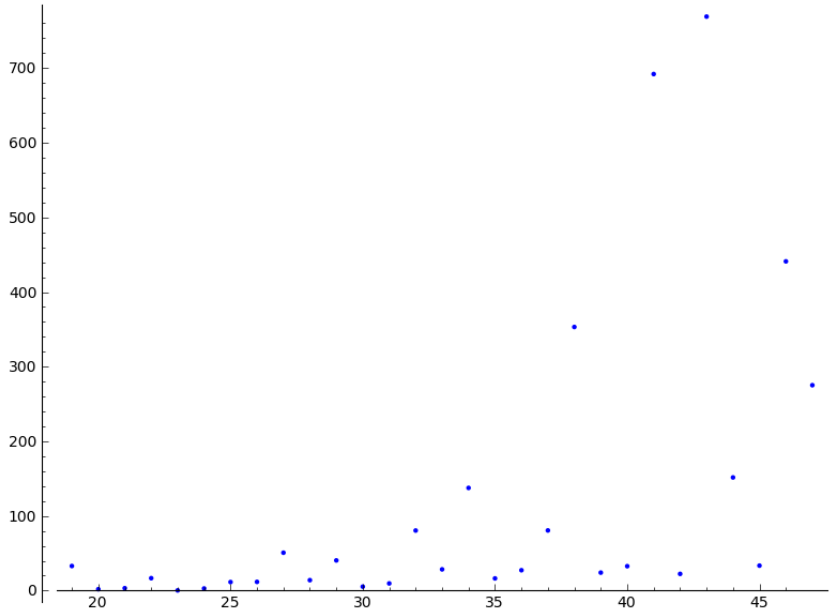


Lorsque l'on fixe un corps de définition et que l'on fait varier la courbe On considère la courbe $\mathcal{C}$ d'équation $y^2 = x^n - 1$ sur le corps $\mathbb{F}_p$ avec

$$p = 10000000000000000000000000000000000000000000000000000000000000159.$$

La figure B.2 représente les temps de calcul (en secondes) de l'algorithme sur $\mathcal{C}$ lorsque l'on fait varier n entre 19 et 47.

FIGURE B.2 – Temps de calcul de l'algorithme de reconnaissance du groupe d'automorphismes réduits de la courbe hyperelliptique $y^2 = x^n - 1$ sur le corps $\mathbb{F}_p$. L'entier n est représenté en abscisse. En ordonné, le temps de calcul est représenté en secondes.



A présent, on va donner une implémentation `Magma` de notre algorithme.

B.2.3 Le programme

```
Attach("isgl2equiv.m");

NonZeroElement := function(M)
  N := Nrows(M);
  for j in [1 .. N] do
    for i in [1 .. N] do
      if M[i,j] ne 0 then
        return M[i,j];
      end if;
    end for;
  end for;
  printf("Error, your matrix is zero");
  return 0;
end function;
```

Étant donné le polynôme d'une courbe hyperelliptique $\mathcal{C}$, cette fonction renvoie le genre de $\mathcal{C}$.

```
Genre:= function(f);
  Z := Integers();
  d := Degree(f);
  if d mod 2 eq 0 then
    return Z!(d/2-1);
  end if;
  return Z!((d-1)/2);
end function;
```

Étant donné un polynôme univarié f, cette fonction calcule le groupe d'automorphismes réduits de la courbe $y^2 = f(x)$ en utilisant le pakage `Magma` "isgl2equiv.m". Ce dernier utilise les résultats de la partie 2.1.5.

```
CreationAutomorphismGroup:= function(f)
  g := Genre(f); //Genus of C
  _,L := IsGL2GeometricEquivalent(f,f,2*g+2); //function of "isgl2equiv.m"
  G := [];
  n := #L;
  N := 1;
  for i in [1 .. n] do
    FF := Parent(L[i][1]);
    N := Lcm(N,Degree(FF));
  end for;
  p := Characteristic(FF);
  FFk<a> := GF(p^N); // Minimal extension how contain all the coefficients of éléments of L
  for i in [1 .. n] do
    M := L[i];
    Embed(Parent(M[1]),FFk);
    M := Matrix(FFk, 2, 2,M);
    Append(~G,1/NonZeroElement(M)*M); // Definition of the elements of G as matrix 2X2 normalised
  end for;
  return FFk,G;
end function;
```

Étant donnée une liste G de matrices et un entier N, cette fonction renvoie la liste des éléments de G qui sont d'ordre au plus égal à N (en pratique, $N = 2$ ou $N = 3$).

```
ListOfElementsOfOrderN:= function(G,N)
  L := [];
  for M in G do
    if IsScalar(M^N) eq true then
      Append(~L,M);
    end if;
  end for;
  return L;
end function;
```

Cette fonction renvoie l'ordre de la matrice `M` vue comme un élément de PGL.

```
OrderMatrix := function(M)
  i := 1;
  Mi := M;
  while true do
    if IsScalar(Mi) then
      return i;
    end if;
    Mi := M*Mi;
    i := i+1;
  end while;
end function;
```

Étant donnés une liste G de matrice et un entier N, cette fonction renvoie un élément de G qui est d'ordre N.

```
ElementOfOrderN := function(G,N)
for M in G do
if OrderMatrix(M) eq N then
return M;
end if;
end for;
printf(" Not found");
return 0*G[1];
```

Étant donnée une liste de matrices G et un élément E de G, cette fonction renvoie un élément en dehors de l'orbite de E sous l'action de la multiplication des matrices.

```
ElementOutOfOrbitOfE := function(G,E)
  n := #G;
  Ei := E;
  for i in [1..n] do
    Exclude(~G,Ei/(NonZeroElement(Ei)));
    if IsScalar(Ei) then
      break i;
    end if;
    Ei := E*Ei;
  end for;
  return G[1];
end function;
```

Étant donné une liste de matrices G, cette fonction renvoie la matrice de translation par 1 si cette dernière est dans G et la matrice nulle sinon.

```
ChercheT := function(G)
for M in G do
  if M[2,1] eq 0 and M[1,1] eq M[1,2] and M[1,2] eq M[2,2] then
    return M;
  end if;
end for;
return 0*G[1];
end function;
```

Étant donné une liste de matrices G, cette fonction renvoie une inversion autour du cercle de rayon 1 dans le demi-plan supérieur des matrices si cette dernière est dans G et la matrice nulle sinon.

```
ChercheS := function(G)
for M in G do
  if M[1,1] eq 0 and M[2,2] eq 0 and M[1,2] eq -1*M[2,1] then
    return M;
  end if;
end for;
return 0*G[1];
end function;
```

Cette fonction renvoie un système d'éléments de tous les ordres possibles dans G. Chaque élément retourné a un ordre différent. Elle renvoie aussi la liste triée de tous les ordres.

```
AllOrderElement_of_G := function(G)
  L := [];
```

```
  Gen :=[];
  for M in G do
    o := OrderMatrix(M);
    if not (o in L) then
      Append(~L,o);
      Append(~Gen,M);
    end if;
  end for;
  return Gen,Sort(L);
end function;
```

Cette fonction renvoie l'ordre maximal d'un élément de `G`

```
MaximalOrder := function(G)
_,L := AllOrderElement_of_G(G);
return L[#L];
end function;
```

Soit n le cardinal d'un groupe et q la puissance d'un nombre premier. Les deux fonctions suivantes renvoient `true` s'il existe un entier i tel que $n = (q^i - 1)q^i(q^i + 1)$
(resp. $n = (q^i - 1)q^i(q^i + 1)/2$), c'est à dire si n est la cardinal de $\mathrm{PGL}_2(F_{q^i})$ (resp. $\mathrm{PSL}_2(F_{q^i})$).

```
IsCardinalOfA_PGL2 := function(n,q)
  qi := 1;
  while true do
    qi:= q*qi;
    m := (qi-1)*qi*(qi+1);
    if m eq n then
      return true,qi;
    end if;
    if n le m then
      return false,1;
    end if;
  end while;
end function;
IsCardinalOfA_PSL2 := function(n,q)
  qi := 1;
  while true do
    qi:= q*qi;
    m := (qi-1)*qi*(qi+1)/2;
    if m eq n then
      return true,qi;
    end if;
    if n le m then
      return false,1;
    end if;
  end while;
end function;
```

Etant donné un groupe G, cette fonction renvoie un ensemble de générateurs des éléments d'ordre p de G.

```
ElementsOfOrder_p := function(G,p)
Gen := [];// Liste d'elements d'ordre p qui engendre tous les element d'ordre p
for M in G do
```

```
if (not IsScalar(M) and IsScalar(M^p)) then
/*L'element M est d'ordre p*/
boo := false;
/*represente le fait que l'orbite de M est dans Gen*/
for i in [1..p-1] do
/*On ne prend qu'un element par orbite*/
Mi := M^i;
e := NonZeroElement(Mi)^(-1);
Mi := Mi*e;
if Mi in Gen then
boo := true;
break;
end if;
end for;
if boo eq false then
Append(~Gen,M);
end if;
end if;
end for;
return Gen;
end function;
```

Cette fonction renvoie un ensemble de générateurs de $\mathrm{PSL}_2(\mathbb{F}_{q_i})$.

```
GeneratorOfPSL := function(G,p,qi)
  Gen := ElementOfOrder_p(G,p);
  return Gen;
end function;
```

Cette fonction renvoie un ensemble de générateurs de $\mathrm{PGL}_2(\mathbb{F}_{q_i})$.

```
GeneratorOfPGL := function(G,p,qi)
  Gen := ElementOfOrder_p(G,p);
  Append(~Gen,ElementOfOrderN(G,qi-1));
  return Gen;
end function;
```

Soit G un groupe de la forme $G_{\beta,A}$ et p la caractéristique de son corps de base. Cette fonction renvoie une liste d'éléments d'ordre p et un élément n qui engendrent G.

```
GeneratorOfGbetaA := function(G,p)
  card := #G;
  Gen := ElementsOfOrder_p(G,p);
  np := #Gen*(p-1);
  n := Integers()!(card/(np+1));
  if n gt 1 then
    Append(~Gen,ElementOfOrderN(G,n));
  end if;
  return Gen;
end function;
```

Étant donné une courbe hyperelliptique $\mathcal{C}$, cette fonction retourne le nom du groupe d'automorphisme, G, de $\mathcal{C}$, une liste de générateurs et le cardinal de G. Cette fonction repose sur les résultats de [Hug05, p.26,27].

```
IdentifyHyperellipticGroup := function(C)
  Z := Integers();
  FF := BaseRing(C);
  p := Characteristic(FF);
  if p ne 0 then
   q := #FF;
  end if;
  f := HyperellipticPolynomials(C);
  FFk,G := CreationAutomorphismGroup(f);
  n := #G;
  if p eq 0 or (n mod p) ne 0 then
    L2 := ListOfElementsOfOrderN(G,2); /* Number of element of order at most 2 in G*/
    m := #L2;
    if m le 2 then /* The cyclic group has at most one element of order 2*/
      return "Cn",[ElementOfOrderN(G,n)],n;
    end if;

    n2 := Z!(n/2) + 1 + ((Z!(n/2)+1) mod 2);// if n is odd, G have to be cyclic so at this point r
    if m eq n2 then /* The dihedral group has n/2 + (n/2+1 mod 2) element of order two and one ele
      Eltn2 := ElementOfOrderN(G,Z!(n/2));
      if (Z!(n/2) mod 2) eq 1 then
        return "Dn",[Eltn2,ElementOfOrderN(G,2)],n;
      end if;
      return "Dn",[Eltn2,ElementOutOfOrditOfE(G,Eltn2)],n;
    end if;

      case(n):
        when 12:
/* The alternative group of order 4 has 12 elements and it is generated by
an element of order 2 and an element of order 3*/
          return "A4",[ElementOfOrderN(G,2),ElementOfOrderN(G,3)],n;

        when 24:
/* The symetric group of order 4 has 24 elements and it is genarated by
an element of order 2 and un element of order 4 such that the product is of order 3*/
          A2 := ElementOfOrderN(G,2);
          A4 := ElementOfOrderN(G,4);
          while IsScalar((A2*A4)^2) do
            Exclude(~G,A2);
            A2 := ElementOfOrderN(G,2);
          end while;
          return "S4",[A2,A4],n;

        when 60:
/* The alternative group of order 5 has 60 elements and it is generated by
 an element of order 3 and an element of order 5*/
          return "A5",[ElementOfOrderN(G,3),ElementOfOrderN(G,5)],n;
      end case;
    else

    // CAN BE IMPROVED, WE JUST HAVE A GENERATOR SYSTEM AND NOT A BASIS
      boo,qi := IsCardinalOfA_PGL2(n,p);
```

```
      if boo then
          if IsPrime(#FFk) then
/*PGL2 est engendre par la matrice de translation unitaire superieur
et la symétrie antidiagonale*/
            return "PGL2",[ChercheS(G),ChercheT(G)],n;
          end if;
          return "PGL2",GeneratorOfPGL(G,p,qi),n;
      end if;
      boo,qi := IsCardinalOfA_PSL2(n,p);
      if boo then
/*PSL2 est engendre par la matrice de translation unitaire supperieure
et la matrice de translation unitaire inferieure */
          if IsPrime(#FFk) then
            S := ChercheS(G);
            T := ChercheT(G);
            return "PSL2",[T,S*T*S],n;
          end if;
        return "PSL2",GeneratorOfPSL(G,p,qi),n;
      end if;
      if p eq 3 and n eq 60 and MaximalOrder(G) eq 5 then
/*SL2(F5) est isomorphe à A5*/
       return "SL2(F5)",[ElementOfOrderN(G,3),ElementOfOrderN(G,5)],n;
      end if;
      return "G_Beta_A",GeneratorOfGbetaA(G,p),n;
    end if;
    return "I don't know",G,n;
end function;
```

B.3 Preuves utilisant magma

B.3.1 Dans le paragraphe "Deux familles de dimension 1"

```
P1<j1,j2,j3>:=PolynomialRing(GF(5),3);
PP<x>:=PolynomialRing(P1);
t := 4 + 2^2*j1;
f := x^6+x^3+t;
II2:=IgusaInvariants(f);
rr:=ideal<P1 | j3*j1 + j2^3 + 3*j2*j1^3 + 2*j1^4, j3 + 3*j2^2*j1 + 4*j1^4 + 2*j1^3, j2 + 2*j1^2>;
(II2[2]-II2[1]^2*j1) in rr;
magma: true
(II2[3]-II2[1]^3*j2) in rr;
magma: true
(II2[5]-II2[1]^5*j3) in rr;
magma: true
```

B.3.2 Dans le paragraphe "Famille de dimension 2, cas où $R = 0$"

B.3.2.1 Cas où $u \neq 0$

```
FF := Rationals();
A<J4,J6,J10> := PolynomialRing(FF,3);
P<x> := PolynomialRing(A);
J2 := 1;
```

```
Au := J2^5*J4^2-64*J2^3*J4^3+1024*J2*J4^4+3*J2^6*J6-202*J2^4*J4*J6+4014*J2^2*J4^2*J6
-20160*J4^3*J6+666*J2^3*J6^2-20520*J2*J4*J6^2+48600*J6^3-30*J2^4*J10+2800*J2^2*J4*J10
-192000*J4^2*J10-360000*J2*J6*J10;

Bu := 2*J2^4*J4*J6-114*J2^2*J4^2*J6+1344*J4^3*J6+6*J2^3*J6^2+216*J2*J4*J6^2-3240*J6^3+
18*J2^4*J10-1040*J2^2*J4*J10+12800*J4^2*J10+4800*J2*J6*J10;

Av:=J2^6*J4^2-96*J2^4*J4^3+3072*J2^2*J4^4-32768*J4^5+3*J2^7*J6-164*J2^5*J4*J6
+1250*J2^3*J4^2*J6+29760*J2*J4^3*J6+858*J2^4*J6^2-22680*J2^2*J4*J6^2
-172800*J4^2*J6^2+81000*J2*J6^3+1176*J2^5*J10-79600*J2^3*J4*J10
+1344000*J2*J4^2*J10-72000*J2^2*J6*J10-12960000*J4*J6*J10-134400000*J10^2;

Bv:=3*J2^3*J4^2*J6-160*J2*J4^3*J6+J2^4*J6^2-36*J2^2*J4*J6^2+3456*J4^2*J6^2-1188*J2*J6^3
+24*J2^3*J4*J10-1280*J2*J4^2*J10+160*J2^2*J6*J10+105600*J4*J6*J10+640000*J10^2;

u := Au;
v := Av;
/*On supprime trous les denominateurs pour que f soit definie sur un anneau de polynome
 afin de pouvoir travailler sur l'ideal de la relation fourni par R=0*/
t    := v^2*Bu^3-4*u^3*Bv^2;
a0:= (Bu^3*v^2+Bu*Bv*u^2*v-2*u^3*Bv^2)*Bu^5*Bv^3;
a1:= 2*(u^2*Bv+3*v*Bu^2)*t*Bu^3*Bv^2;
a2:= (15*v^2*Bu^3-u^2*v*Bu*Bv-30*u^3*Bv^2)*t*Bu^2*Bv;
a3:= 4*(5*v*Bu^2-u^2*Bv)*t^2;

f := a0*x^6+a1*x^5+a2*x^4+a3*x^3+t*a2*x^2+t^2*a1*x+t^3*a0;
rr := ideal<A |
/*Relation R = 0*/
J2^6*J6^3 - 2*J2^5*J4^2*J6^2 - 72*J2^5*J4*J6*J10 - 432*J2^5*J10^2 + J2^4*J4^4*J6
+ 8*J2^4*J4^3*J10 - 72*J2^4*J4*J6^3 - 48*J2^4*J6^2*J10 + 136*J2^3*J4^3*J6^2
+ 4816*J2^3*J4^2*J6*J10 + 28800*J2^3*J4*J10^2 + 216*J2^3*J6^4 -
64*J2^2*J4^5*J6 - 512*J2^2*J4^4*J10 + 1080*J2^2*J4^2*J6^3 -
12960*J2^2*J4*J6^2*J10 - 96000*J2^2*J6*J10^2 - 2304*J2*J4^4*J6^2 -
84480*J2*J4^3*J6*J10 - 512000*J2*J4^2*J10^2 - 7776*J2*J4*J6^4 -
129600*J2*J6^3*J10 + 1024*J4^6*J6 + 8192*J4^5*J10 + 6912*J4^3*J6^3 +
691200*J4^2*J6^2*J10 + 11520000*J4*J6*J10^2 + 11664*J6^5 + 51200000*J10^3>;
I2,I4,I6,_,I10 := IgusaInvariants(f);

(J4*I2^2 -I4) in rr;
(J6*I2^3 -I6) in rr;
(J10*I2^5 -I10) in rr;
```

B.3.2.2 Cas où $u = 0$

```
FF := Rationals();
A<J4,J6,J10> := PolynomialRing(FF,3);
P<x> := PolynomialRing(A);
J2 := 1;

Au := 0;
```

```
Bu := 1;

Av:=J2^6*J4^2-96*J2^4*J4^3+3072*J2^2*J4^4-32768*J4^5+3*J2^7*J6-164*J2^5*J4*J6
+1250*J2^3*J4^2*J6+29760*J2*J4^3*J6+858*J2^4*J6^2-22680*J2^2*J4*J6^2
-172800*J4^2*J6^2+81000*J2*J6^3+1176*J2^5*J10-79600*J2^3*J4*J10
+1344000*J2*J4^2*J10-72000*J2^2*J6*J10-12960000*J4*J6*J10-134400000*J10^2;

Bv:=3*J2^3*J4^2*J6-160*J2*J4^3*J6+J2^4*J6^2-36*J2^2*J4*J6^2+3456*J4^2*J6^2-1188*J2*J6^3
+24*J2^3*J4*J10-1280*J2*J4^2*J10+160*J2^2*J6*J10+105600*J4*J6*J10+640000*J10^2;

u := Au;
v := Av;

t:=FF!1;
a0:=Bv+2*v;
a1:=2*(3*Bv-4*v);
a2:=15*Bv+14*v;
a3:=4*(5*Bv-4*v);

f := a0*x^6+a1*x^5+a2*x^4+a3*x^3+t*a2*x^2+t^2*a1*x+t^3*a0;
rr := ideal<A |
/*Relation R = 0*/
J2^6*J6^3 - 2*J2^5*J4^2*J6^2 - 72*J2^5*J4*J6*J10 - 432*J2^5*J10^2 + J2^4*J4^4*J6
+ 8*J2^4*J4^3*J10 - 72*J2^4*J4*J6^3 - 48*J2^4*J6^2*J10 + 136*J2^3*J4^3*J6^2
+ 4816*J2^3*J4^2*J6*J10 + 28800*J2^3*J4*J10^2 + 216*J2^3*J6^4 -
64*J2^2*J4^5*J6 - 512*J2^2*J4^4*J10 + 1080*J2^2*J4^2*J6^3 -
12960*J2^2*J4*J6^2*J10 - 96000*J2^2*J6*J10^2 - 2304*J2*J4^4*J6^2 -
84480*J2*J4^3*J6*J10 - 512000*J2*J4^2*J10^2 - 7776*J2*J4*J6^4 -
129600*J2*J6^3*J10 + 1024*J4^6*J6 + 8192*J4^5*J10 + 6912*J4^3*J6^3 +
691200*J4^2*J6^2*J10 + 11520000*J4*J6*J10^2 + 11664*J6^5 + 51200000*J10^3,

/*Relation correspondante au cas u=0*/
J2^5*J4^2-64*J2^3*J4^3+1024*J2*J4^4+3*J2^6*J6-202*J2^4*J4*J6+4014*J2^2*J4^2*J6
-20160*J4^3*J6+666*J2^3*J6^2-20520*J2*J4*J6^2+48600*J6^3-30*J2^4*J10+2800*J2^2*J4*J10
-192000*J4^2*J10-360000*J2*J6*J10>;
I2,I4,I6,_,I10 := IgusaInvariants(f);

(J4*I2^2 -I4) in rr;
(J6*I2^3 -I6) in rr;
(J10*I2^5 -I10) in rr;
```

B.3.3 Calcul des coefficients A_{ij} et a_{ijk}

```
A11 := Transvectant([*q1,3,2*],[*q1,3,2*],2)[1];
A12 := Transvectant([*q1,3,2*],[*q2,5,2*],2)[1];
A13 := Transvectant([*q1,3,2*],[*q3,7,2*],2)[1];
A22 := Transvectant([*q2,5,2*],[*q2,5,2*],2)[1];
A23 := Transvectant([*q2,5,2*],[*q3,7,2*],2)[1];
A33 := Transvectant([*q3,7,2*],[*q3,7,2*],2)[1];

a111 := MestreProduct3_2(f,q1,q1,q1);
```

```
a112 := MestreProduct3_2(f,q1,q1,q2);
a113 := MestreProduct3_2(f,q1,q1,q3);
a122 := MestreProduct3_2(f,q1,q2,q2);
a123 := MestreProduct3_2(f,q1,q2,q3);
a133 := MestreProduct3_2(f,q1,q3,q3);
a222 := MestreProduct3_2(f,q2,q2,q2);
a223 := MestreProduct3_2(f,q2,q2,q3);
a233 := MestreProduct3_2(f,q2,q3,q3);
a333 := MestreProduct3_2(f,q3,q3,q3);
```

B.3.4 Expression d'un invariant en fonction des J_i et $\mathcal{R}$

B.3.4.1 Pour la méthode de Geyer Sturmfels

```
EvaluationGeyer := function(I,L)
x1 :=L[1];x2 :=L[2];x3 :=L[3];x4 :=L[4];x5 :=L[5];x6 :=L[6];
t0 := (x2-x1)*(x4-x3)*(x6-x5);
t1 := (x4-x1)*(x3-x2)*(x6-x5);
t2 := (x6-x1)*(x3-x2)*(x5-x4);
t3 := (x6-x1)*(x5-x2)*(x4-x3);
t4 := (x2-x1)*(x6-x3)*(x5-x4);
return Evaluate(I,[t0,t1,t2,t3,t4]);
end function;
```

Cette fonction renvoie une sextique aléatoire sur un corps de caractéristique nulle ainsi que ses racines.

```
RandomSexticOverFF := function(FF)
P<x> := PolynomialRing(FF);
        L := [];
        a := Random(FF);
Append(~L,a);
        f := x-a;
while #L ne 6 do
a := Random(FF);
if not (a in L) then
Append(~L,a);
f := f*(x-a);
end if;
end while;
return f,L;
end function;
```

Étant donné une liste de polynômes multivariés homogène `B` ainsi qu'un entier `n`, cette fonction renvoie l'ensemble des monômes de degrés `n` que l'on peut produire comme produits d'éléments de `B`.

```
Monomes := function(B,n)
D := [Degree(b): b in B];
P := PolynomialRing(Rationals(),D);
PP:= ProjectiveSpace(P);
L := LinearSystem(PP,n);
return [Evaluate(l,B): l in Sections(L)];
end function;
```

Les deux fonctions suivantes servent à calculer l'invariant $\mathcal{R}$ de la section 6.4.

```
Evaluat := function(D,L)
  x1,x2,x3,x4,x5,x6 := Explode(L);
  A := Parent(x1);
  return Determinant(Matrix(A,3,3,[[x1+x2,1,-x1*x2],[x3+x4,1,-x3*x4],[x5+x6,1,-x5*x6]]));
end function;

RInvariant := function(f)
  P:=Parent(f);
  FF := BaseRing(f);
  a0,a1,a2,a3,a4,a5,a6 := Explode(Coefficients(f));
  P<x1,x2,x3,x4,x5,x6> := PolynomialRing(FF,6);
  D := Determinant(Matrix(P,3,3,[[x1+x2,1,-x1*x2],[x3+x4,1,-x3*x4],[x5+x6,1,-x5*x6]]));
  Rx:= D*Evaluat(D,[x1,x2,x3,x5,x4,x6])
      *Evaluat(D,[x1,x2,x3,x6,x5,x4])
      *Evaluat(D,[x1,x3,x2,x4,x5,x6])
      *Evaluat(D,[x1,x3,x2,x5,x4,x6])
      *Evaluat(D,[x1,x3,x2,x6,x5,x4])
      *Evaluat(D,[x1,x4,x2,x3,x5,x6])
      *Evaluat(D,[x1,x4,x2,x5,x3,x6])
      *Evaluat(D,[x1,x4,x2,x6,x5,x3])
      *Evaluat(D,[x1,x5,x2,x3,x4,x6])
      *Evaluat(D,[x1,x5,x2,x4,x3,x6])
      *Evaluat(D,[x1,x5,x2,x6,x4,x3])
      *Evaluat(D,[x1,x6,x2,x3,x4,x5])
      *Evaluat(D,[x1,x6,x2,x4,x3,x5])
      *Evaluat(D,[x1,x6,x2,x5,x4,x3]);
    boo,R := IsSymmetric(Rx);
  return Evaluate(R,[-a5/a6,a4/a6,-a3/a6,a2/a6,-a1/a6,a0/a6])*a6^(15);
end function;
```

Étant donné un invariant `Inv`, cette fonction calcule des coefficients $\lambda_1, \ldots, \lambda_m$ tels que

$$\texttt{Inv} = \sum_{i=(i_1,i_2,i_3,i_4,i_5)} \lambda_i J_2^{i_1} J_4^{i_2} J_6^{i_3} J_{10}^{i_4} \mathcal{R}^{i_5}$$

avec $i_1 + i_2 + i_3 + i_4 + i_5 = degre(\texttt{Inv})$, J_i les invariants d'Igusa et $\mathcal{R}$ de la section 6.4. Cette fonction effectue cela par évaluation. La fonction suivante vérifie formellement que les constantes $\lambda_1, \ldots, \lambda_m$ sont exactes.

```
ExpressionIgusaInvariantInv := function(FF,Inv)
    d := Degree(Inv);
    Racine := [];
    Monnos := [];
A<a0,a1,a2,a3,a4,a5,a6> := PolynomialRing(FF,7);
P<x> := PolynomialRing(A);
f := a0 + a1*x + a2*x^2 + a3*x^3 + a4*x^4 + a5*x^5 + a6*x^6;
J2,J4,J6,_,J10 := Explode(IgusaInvariants(f));
if (d mod 2) eq 1 then
R := RInvariant(f);
    Mon := Monomes([J2,J4,J6,J10,R],d);
else
   Mon := Monomes([J2,J4,J6,J10],d);
```

```
end if;
l := #Mon;
// nombre de monome de degre d que l'on peut faire avec les invariants d'Igusa et R
b := false;
while b eq false do
    for i in [1..l] do
        f,L := RandomSexticOverFF(FF);
        Coe := Coefficients(f);
        Append(~Racine,L);
        Append(~Monnos,[Evaluate(mon,Coe): mon in Mon]);
    end for;
MI := Matrix(FF,l,l,Monnos);
b,M := IsInvertible(MI);
end while;
v := Vector([EvaluationGeyer(Inv,L): L in Racine]);
return v*Transpose(M);
end function;

VerificationConstantesGeyer := function(v,Inv,FF)
    d := Degree(Inv);
A<x1,x2,x3,x4,x5,x6> := PolynomialRing(FF,6);
P<x> := PolynomialRing(A);
f := (x-x1)*(x-x2)*(x-x3)*(x-x4)*(x-x5)*(x-x6);
t0 := (x2-x1)*(x4-x3)*(x6-x5);
t1 := (x4-x1)*(x3-x2)*(x6-x5);
t2 := (x6-x1)*(x3-x2)*(x5-x4);
t3 := (x6-x1)*(x5-x2)*(x4-x3);
t4 := (x2-x1)*(x6-x3)*(x5-x4);
J2,J4,J6,_,J10 := Explode(IgusaInvariants(f));
Mon := Monomes([J2,J4,J6,J10],3*d);
// Les invariants sont en fonction des racines donc
// de degre trois fois leur degre en fonction des coef cf lemme 6.4.0.1
taille := #Mon;
Exp := 0;
for i in [1..taille] do
     Exp := v[i]*Mon[i];
end for;
return Exp eq Evaluate(Inv,[t0,t1,t2,t3,t4]);
end function;
```

B.3.4.2 Pour retrouver les expressions des coniques et cubiques dans la méthode de Mestre

```
coef := a111; // coefficient que l'on veut exprimer en fonction des Ji et R
n := 10; //degre de ce coef
v := LinearCombinaisonMonomial([J2,J4,J6,J10,R)],coef,n);
P<J2,J4,J6,J10,R>:=PolynomialRing(Rationals(),[2,4,6,10,15]);
PP:=ProjectiveSpace(P);
L:=LinearSystem(PP,Degree(coef));
Sec := Sections(L);

tmp := 0;
taille := #Sec;
```

```
for i in [1..taille] do
tmp := tmp + Integers()!(v[i])*Sec[i];
end for;
tmp;
```

B.3.5 Fonctions auxilaires

Cette fonction calcule le transvectant de deux covariants f et g vues comme polynômes à une indéterminées. `F` (resp. `G`) est une liste contenant le polynôme f (resp. g) le degré en les coefficients de f (resp. g) ainsi que l'ordre de f (resp. g).

```
function Transvectant(F, G, r : scaled := true)
    Q, Qdeg, n := Explode(F);
    R, Rdeg, m := Explode(G);
    n := IntegerRing()!n;
    m := IntegerRing()!m;
    K := BaseRing(Parent(Q));
    h := Parent(Q)!0;
    for k := 0 to r do
h +:= (-1)^k
    * Binomial(m-k,r-k)  * Derivative(Q, r-k)
    * Binomial(n-r+k, k) * Derivative(R, k);
    end for;
    if scaled eq true then
        coef := Factorial(r) * Factorial(m-r) * Factorial(n-r) / Factorial(m) / Factorial(n);
h := (K!coef) * h;
    end if;
    return [* h, Qdeg + Rdeg, n + m - 2*r *];
end function;

Monomes := function(B,n)
  D := [Degree(b): b in B];
  P := PolynomialRing(Rationals(),D);
  PP:= ProjectiveSpace(P);
  L := LinearSystem(PP,n);
  return [Evaluate(l,B): l in Sections(L)];
end function;

LinearCombinaisonMonomial := function(B,b,Nbvar)
  FF := BaseRing(Parent(b));
  IsFF := false;
  if Type(FF) eq FldFin then
    FF := ext<FF|2>;
    IsFF := true;
  end if;

  n := Degree(b);
  Mo:= Monomes(B,n);
  m := #Mo;
  boo := false;
  while boo eq false do
    JeuCoef := [];
    JeuEltMo:= [];
```

```
    for i in [1..m] do
      if IsFF then
        L := [Random(FF): i in [1..Nbvar]];
      else
        L := [FF!Random(100): i in [1..Nbvar]];
      end if;

      Append(~JeuCoef,L);
      LB:=[];
      for eltMo in Mo do
        Append(~LB,Evaluate(eltMo,L));
      end for;

      Append(~JeuEltMo,LB);
    end for;

    MB := Matrix(FF,m,m,JeuEltMo);
    boo,M := IsInvertible(MB);
    printf("1");
  end while;

  v := Vector([Evaluate(b,coef): coef in JeuCoef]);
  return Vector(M*Transpose(Matrix(v)));
end function;

MestreProduct3_2 := function(g,c1,c2,c3)
Cst := BaseRing(Parent(g));
P2<X,Z> := PolynomialRing(Cst,2);
C1 := P2!(Evaluate(c1,X/Z)*Z^Degree(c1));
C2 := P2!(Evaluate(c2,X/Z)*Z^Degree(c2));
C3 := P2!(Evaluate(c3,X/Z)*Z^Degree(c3));
f  := P2!(Evaluate(g,X/Z)*Z^Degree(g));
return
Evaluate(
Derivative(f,6,X)*Derivative(C1,2,Z)*Derivative(C2,2,Z)*Derivative(C3,2,Z) +
Derivative(Derivative(f,4,X),2,Z)*Derivative(C1,2,Z)*Derivative(C2,2,X)*
Derivative(C3,2,Z) -
2*Derivative(Derivative(f,5,X),1,Z)*Derivative(C1,2,Z)*
Derivative(Derivative(C2,X),Z)*Derivative(C3,2,Z) +
Derivative(Derivative(f,4,X),2,Z)*Derivative(C1,2,X)*Derivative(C2,2,Z)*
Derivative(C3,2,Z) +
Derivative(Derivative(f,2,X),4,Z)*Derivative(C1,2,X)*Derivative(C2,2,X)*
Derivative(C3,2,Z) -
2*Derivative(Derivative(f,3,X),3,Z)*Derivative(C1,2,X)*
Derivative(Derivative(C2,X),Z)*Derivative(C3,2,Z) - 2*(
Derivative(Derivative(f,5,X),1,Z)*Derivative(Derivative(C1,X),Z)*
Derivative(C2,2,Z)*Derivative(C3,2,Z) +
Derivative(Derivative(f,3,X),3,Z)*Derivative(Derivative(C1,X),Z)*
Derivative(C2,2,X)*Derivative(C3,2,Z) -
2*Derivative(Derivative(f,4,X),2,Z)*Derivative(Derivative(C1,X),Z)*
Derivative(Derivative(C2,X),Z)*Derivative(C3,2,Z)) +

Derivative(Derivative(f,4,X),2,Z)*Derivative(C1,2,Z)*Derivative(C2,2,Z)*
```

```
Derivative(C3,2,X) +
Derivative(Derivative(f,2,X),4,Z)*Derivative(C1,2,Z)*Derivative(C2,2,X)*
Derivative(C3,2,X) -
2*Derivative(Derivative(f,3,X),3,Z)*Derivative(C1,2,Z)*
Derivative(Derivative(C2,X),Z)*Derivative(C3,2,X) +
Derivative(Derivative(f,2,X),4,Z)*Derivative(C1,2,X)*Derivative(C2,2,Z)*
Derivative(C3,2,X) +
Derivative(f,6,Z)*Derivative(C1,2,X)*Derivative(C2,2,X)*Derivative(C3,2,X) -
2*Derivative(Derivative(f,1,X),5,Z)*Derivative(C1,2,X)*
Derivative(Derivative(C2,X),Z)*Derivative(C3,2,X) - 2*(
Derivative(Derivative(f,3,X),3,Z)*Derivative(Derivative(C1,X),Z)*
Derivative(C2,2,Z)*Derivative(C3,2,X) +
Derivative(Derivative(f,1,X),5,Z)*Derivative(Derivative(C1,X),Z)*
Derivative(C2,2,X)*Derivative(C3,2,X) -
2*Derivative(Derivative(f,2,X),4,Z)*Derivative(Derivative(C1,X),Z)*
Derivative(Derivative(C2,X),Z)*Derivative(C3,2,X)) -2*(

Derivative(Derivative(f,5,X),Z)*Derivative(C1,2,Z)*Derivative(C2,2,Z)*
Derivative(Derivative(C3,X),Z) +
Derivative(Derivative(f,3,X),3,Z)*Derivative(C1,2,Z)*Derivative(C2,2,X)*
Derivative(Derivative(C3,X),Z) -
2*Derivative(Derivative(f,4,X),2,Z)*Derivative(C1,2,Z)*Derivative(Derivative(C2,X),Z)*
Derivative(Derivative(C3,X),Z) +
Derivative(Derivative(f,3,X),3,Z)*Derivative(C1,2,X)*Derivative(C2,2,Z)*
Derivative(Derivative(C3,X),Z) +
Derivative(Derivative(f,X),5,Z)*Derivative(C1,2,X)*Derivative(C2,2,X)*
Derivative(Derivative(C3,X),Z) -
2*Derivative(Derivative(f,2,X),4,Z)*Derivative(C1,2,X)*Derivative(Derivative(C2,X),Z)*
Derivative(Derivative(C3,X),Z) - 2*(
Derivative(Derivative(f,4,X),2,Z)*Derivative(Derivative(C1,X),Z)*Derivative(C2,2,Z)*
Derivative(Derivative(C3,X),Z) +
Derivative(Derivative(f,2,X),4,Z)*Derivative(Derivative(C1,X),Z)*Derivative(C2,2,X)*
Derivative(Derivative(C3,X),Z) -
2*Derivative(Derivative(f,3,X),3,Z)*Derivative(Derivative(C1,X),Z)*
Derivative(Derivative(C2,X),Z)*Derivative(Derivative(C3,X),Z))),[0,0]);

end function;
```

Appendice C

L'article sur la paramétrisation de l'espace de modules des quartiques planes lisses

Submitted exclusively to the London Mathematical Society
doi:10.1112/0000/000000

Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields

Reynald Lercier, Christophe Ritzenthaler, Florent Rovetta and Jeroen Sijsling

Abstract

We study new families of curves that are suitable for efficiently parametrizing their moduli spaces. We explicitly construct such families for smooth plane quartics in order to determine unique representatives for the isomorphism classes of smooth plane quartics over finite fields. In this way, we can visualize the distributions of their traces of Frobenius. This leads to new observations on fluctuations with respect to the limiting symmetry imposed by the theory of Katz and Sarnak.

1. *Introduction*

One of the central notions in arithmetic geometry is the *(coarse) moduli space of curves* of a given genus g, denoted M_g. These are algebraic varieties whose geometric points classify these curves up to isomorphism. The main difficulty when dealing with moduli spaces – without extra structure – is the non-existence of *universal families*, whose construction would allow one to explicitly write down the curve corresponding to a point of this space. Over finite fields, the existence of a universal family would lead to optimal algorithms to write down isomorphism classes of curves. Having these classes at one's disposal is useful in many applications. For instance, it serves for constructing curves with many points using class field theory [**31**] or for enlarging the set of curves useful for pairing-based cryptography as illustrated in genus 2 by [**9**, **13**, **32**]. More theoretically, it was used in [**5**] to compute the cohomology of moduli spaces. We were ourselves drawn to this subject by the study of Serre's obstruction for smooth plane quartics (see Section 5.4).

The purpose of this paper is to introduce three substitutes for the notion of a universal family. The best replacement for a universal family seems to be that of a *representative family*, which we define in Section 2. This is a family of curves $\mathcal{C} \to \mathcal{S}$ whose points are in natural bijection with those of a given subvariety S of the moduli space. Often the scheme $\mathcal{S}$ turns out to be isomorphic to S, but the notion is flexible enough to still give worthwhile results when this is not the case. Another interesting feature of these families is that they can be made explicit in many cases when S is a stratum of curves with a given automorphism group. We focus here on the case of non-hyperelliptic genus 3 curves, canonically realized as *smooth plane quartics*.

The overview of this paper is as follows. In Section 2 we introduce and study three new notions of families of curves. We indicate the connections with known constructions from the literature. In Proposition 2.3 and Proposition 2.4, we also uncover a link between the existence of a representative family and the question of whether the field of moduli of a curve is a field of definition. In Section 3 we restrict our considerations to the moduli space of smooth plane

---

2000 *Mathematics Subject Classification* 14Q05 (primary), 13A50, 14H10, 14H37 (secondary).

Research supported by the French National Research Agency (ANR) through the project PEACE (ANR-12-BS01-0010-01). The fourth author was additionally supported by the Marie Curie Fellowship IEF-GA-2011-299887.

quartics. After a review of the stratification of this moduli space by automorphism groups, our main result in this section is Theorem 3.3. There we construct representative families for all but the two largest of these strata by applying the technique of Galois descent. For the remaining strata we improve on the results in the literature by constructing families with fewer parameters, but here much room for improvement remains. In particular, it would be nice to see an explicit representative (and in this case universal) family over the stratum of smooth plane quartics with trivial automorphism group.

Parametrizing by using our families, we get one representative curve per $\bar{k}$-isomorphism class. Section 4 refines these into k-isomorphism classes by constructing the *twists* of the corresponding curves over finite fields k. Finally, Section 5 concludes the paper by describing the implementation of our enumeration of smooth plane quartics over finite fields, along with the experimental results obtained on distributions of traces of Frobenius for these curves over $\mathbb{F}_p$ with $11 \leq p \leq 53$. In order to obtain exactly one representative for every isomorphism class of curves, we use the previous results combined with an iterative strategy that constructs a complete database of such representatives by ascending up the automorphism strata[†].

Notations. Throughout, we denote by k an arbitrary field of characteristic $p \geq 0$, with algebraic closure $\overline{k}$. We use K to denote a general algebraically closed field. By ζ_n, we denote a fixed choice of n-th root of unity in $\overline{k}$ or K; these roots are chosen in such a way to respect the standard compatibility conditions when raising to powers. Given k, a *curve* over k will be a smooth and proper absolutely irreducible variety of dimension 1 and genus $g > 1$ over k.

In agreement with [**23**], we keep the notation $\mathbf{C}_n$ (resp. $\mathbf{D}_{2n}$, resp. $\mathbf{A}_n$, resp. $\mathbf{S}_n$) for the cyclic group of order n (resp. the dihedral group of order $2n$, resp. the alternating group of order $n!/2$, resp. the symmetric group of order $n!$). We will also encounter $\mathbf{G}_{16}$, a group of 16 elements that is a direct product $\mathbf{C}_4 \times \mathbf{D}_4$, $\mathbf{G}_{48}$, a group of 48 elements that is a central extension of $\mathbf{A}_4$ by $\mathbf{C}_4$, $\mathbf{G}_{96}$, a group of 96 elements that is a semidirect product $(\mathbf{C}_4 \times \mathbf{C}_4) \rtimes \mathbf{S}_3$ and $\mathbf{G}_{168}$, which is a group of 168 elements isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$.

Acknowledgements. We would like to thank Jonas Bergström, Bas Edixhoven, Everett Howe, Frans Oort and Matthieu Romagny for their generous help during the writing of this paper. Also, we warmly thank the anonymous referees for carefully reading this work and for suggestions.

2. *Families of curves*

Let $g > 1$ be an integer, and let k be a field of characteristic $p = 0$ or $p > 2g + 1$. For $\mathcal{S}$ a scheme over k, we define a *curve of genus g* over $\mathcal{S}$ to be a morphism of schemes $\mathcal{C} \to \mathcal{S}$ that is proper and smooth with geometrically irreducible fibers of dimension 1 and genus g. Let M_g be the coarse moduli space of curves of genus g whose geometric points over algebraically closed extensions K of k correspond with the K-isomorphism classes of curves C over K.

We are interested in studying the subvarieties of M_g where the corresponding curves have an automorphism group isomorphic with a given group. The subtlety then arises that these subvarieties are not necessarily irreducible. This problem was also mentioned and studied in [**25**], and resolved by using Hurwitz schemes; but in this section we prefer another way around the problem, due to Lønsted in [**24**].

[†]Databases and statistics summarizing our results can be found at `http://perso.univ-rennes1.fr/christophe.ritzenthaler/programme/qdbstats-v3_0.tgz`.

In [**24**, Sec.6] the moduli space M_g is stratified in a finer way, namely by using 'rigidified actions' of automorphism groups. Given an automorphism group G, Lønsted defines subschemes of M_g that we shall call *strata*. Let ℓ be a prime different from p, and let $\Gamma_\ell = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. Then the points of a given stratum S correspond to those curves C for which the induced embedding of G into the group ($\cong \Gamma_\ell$) of polarized automorphisms of $\mathrm{Jac}(C)[\ell]$ is Γ_ℓ-conjugate to a given group. Combining [**17**, Th.1] with [**24**, Th.6.5] now shows that under our hypotheses on p, such a stratum is a locally closed, connected and smooth subscheme of M_g. If k is perfect, such a connected stratum is therefore defined over k if only one rigidification is possible for a given abstract automorphism group. As was also observed in [**25**], this is not always the case; and as we will see in Remark 3.2, in the case of plane quartics these subtleties are only narrowly avoided.

We return to the general theory. Over the strata S of M_g with non-trivial automorphism group, the usual notion of a universal family (as in [**27**, p.25]) is of little use. Indeed, no universal family can exist on the non-trivial strata; by [**1**, Sec.14], S is a fine moduli space (and hence admits a universal family) if and only if the automorphism group is trivial. In the definition that follows, we weaken this notion to that of a *representative family*. While such families coincide with the usual universal family on the trivial stratum, it will turn out (see Theorem 3.3) that they can also be constructed for the strata with non-trivial automorphism group. Moreover, they still have sufficiently strong properties to enable us to effectively parametrize the moduli space.

DEFINITION 2.1. *Let $S \subset \mathsf{M}_g$ be a subvariety of M_g that is defined over k. Let $\mathcal{C} \to \mathcal{S}$ be a family of curves whose geometric fibers correspond to points of the subvariety S, and let $f_{\mathcal{C}} : \mathcal{S} \to S$ be the associated morphism.*

(i) *The family $\mathcal{C} \to \mathcal{S}$ is* geometrically surjective *(for S) if the map $f_{\mathcal{C}}$ is surjective on K-points for every algebraically closed extension K of k.*
(ii) *The family $\mathcal{C} \to \mathcal{S}$ is* arithmetically surjective *(for S) if the map $f_{\mathcal{C}}$ is surjective on k'-points for every finite extension k' of k.*
(iii) *The family $\mathcal{C} \to \mathcal{S}$ is* quasifinite *(for S) if it is geometrically surjective and $f_{\mathcal{C}}$ is quasifinite.*
(iv) *The family $\mathcal{C} \to \mathcal{S}$ is* representative *(for S) if $f_{\mathcal{C}}$ is bijective on K-points for every algebraically closed extension K of k.*

REMARK 2.2. A family $\mathcal{C} \to \mathcal{S}$ is geometrically surjective if and only if the corresponding morphism of schemes $\mathcal{S} \to S$ is surjective.

Due to inseparability issues, the morphism $f_{\mathcal{C}}$ associated to a representative family need not induce bijections on points over arbitrary extensions of k.

Note that if a representative family $\mathcal{S}$ is absolutely irreducible, then since S is normal, we actually get that $f_{\mathcal{C}}$ is an isomorphism by Zariski's Main Theorem. However, there are cases where we were unable to find such an $\mathcal{S}$ given a stratum S (see Remark 3.4).

The notions of being geometrically surjective, quasifinite and representative are stable under extension of the base field k. On the other hand, being arithmetically surjective can strongly depend on the base field, as for example in Proposition 3.5.

To prove that quasifinite families exist, one typically considers the universal family over $\mathsf{M}_g^{(\ell)}$ (the moduli space of curves of genus g with full level-ℓ structure, for a prime $\ell > 2$ different from p, see [**1**, Th.13.2]). This gives a quasifinite family over M_g by the forgetful (and in fact quotient) map $\mathsf{M}_g^{(\ell)} \to \mathsf{M}_g$ that we will denote π_ℓ when using it in our constructions below.

Let K be an algebraically closed extension of k. Given a curve C over K, recall that an intermediate field $k \subset L \subset K$ is a *field of definition* of C if there exists a curve C_0/L such that C_0 is K-isomorphic to C. The concept of representative families is related with the question of whether the *field of moduli* $\mathbf{M}_C$ of the curve C, which is by definition the intersection of the fields of definition of C, is itself a field of definition. Since we assumed that $p > 2g+1$ or $p = 0$, the field $\mathbf{M}_C$ then can be recovered more classically as the residue field of the moduli space M_g at the point $[C]$ corresponding to C by [**33**, Cor.1.11]. This allows us to prove the following.

PROPOSITION 2.3. *Let S be a subvariety of M_g defined over k that admits a representative family $\mathcal{C} \to \mathcal{S}$. Let C be a curve over an algebraically closed extension K of k such that the point $[C]$ of $\mathsf{M}_g(K)$ belongs to S. Then C descends to its field of moduli $\mathbf{M}_C$. In case k is perfect and $K = \overline{k}$, then C even corresponds to an element of $\mathcal{S}(\mathbf{M}_C)$.*

Proof. First we consider the case where $k = \mathbf{M}_C$ and K is a Galois extension of k. Let $x \in \mathcal{S}(K)$ be the preimage of $[C]$ under $f_{\mathcal{C}}$. For every $\sigma \in \mathrm{Gal}(K/k)$ it makes sense to consider $x^\sigma \in \mathcal{S}(K)$, since the family $\mathcal{C}$ is defined over k. Now since $f_{\mathcal{C}}$ is defined over k, we get $f_{\mathcal{C}}(x) = f_{\mathcal{C}}(x^\sigma) = s$. By uniqueness of the representative in the family, we get $x = x^\sigma$. Since σ was arbitrary and K/k is Galois, we therefore have $x \in \mathcal{S}(k)$, which gives a model for C over k by taking the corresponding fiber for the family $\mathcal{C} \to \mathcal{S}$. This already proves the final statement of the proposition.

Since the notion of being representative is stable under changing the base field k, the argument in the Galois case gives us enough leverage to treat the general case (where K/k is possibly transcendental or inseparable) by appealing to [**19**, Th.1.6.9]. □

Conversely, we have the following result. A construction similar to it will be used in the proof of Theorem 3.3.

PROPOSITION 2.4. *Let S be a stratum defined over a field k. Suppose that for every finite Galois extension $F \supset E$ of field extensions of k, the field of moduli of the curve corresponding to a point in $S(E)$ equals E. Then there exists a representative family $\mathcal{C}_U \to U$ over a dense open subset of S. If k is perfect, this family extends to a possibly disconnected representative family $\mathcal{C} \to \mathcal{S}$ for the stratum S.*

Proof. Let η be the generic point of S and again let $\pi_\ell : \mathsf{M}_g^{(\ell)} \to \mathsf{M}_g$ be the forgetful map obtained by adding level structure at a prime $\ell > 2$ different from p. Note that as a quotient by a finite group, π_ℓ is a finite Galois cover. Let ν be a generic point in the preimage of η by π_ℓ and $\mathcal{C} \to \nu$ be the universal family defined over $k(\nu)$. By definition the field of moduli $\mathbf{M}_{\mathcal{C}}$ is equal to $k(\nu)$ and as $k(\nu)$ is a field of definition there exists a family $\mathcal{C}_0 \to k(\nu)$ geometrically isomorphic to $\mathcal{C}$. Since $k(\nu) \supset k(\eta)$ is a Galois extension, we can argue as in the proof of Proposition 2.3 to descend to $k(\eta)$, and hence by a spreading-out argument we can conclude that $\mathcal{C}_0$ is a representative family on a dense open subset U of S. Proceeding by induction over the (finite) union of the Galois conjugates of the finitely many irreducible components of the complement of U, which is again defined over k, one obtains the second part of the proposition. □

Whereas the universal family $\mathcal{C} \to \mathsf{M}_g^{(\ell)}$ is sometimes easy to construct, it seems hard to work out $\mathcal{C}_0$ directly by explicit Galois descent; the Galois group of the covering $\mathsf{M}_g^{(\ell)} \to \mathsf{M}_g$ is

$\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$, which is a group of large cardinality $\ell^{g^2}\prod_{i=1}^{g}(\ell^{2i}-1)$ whose quotient by its center is simple. Moreover, for enumeration purposes, it is necessary for the scheme $\mathcal{S}$ to be as simple as possible. Typically one would wish for it to be rational, as fortunately turns out always to be the case for plane quartics. On the other hand, for moduli spaces of *general type* that admit no rational curves, such as M_g with $g > 23$, there does not even exist a rational family of curves with a single parameter [**15**].

3. *Families of smooth plane quartics*

3.1. *Review : automorphism groups*

Let C be a smooth plane quartic over an algebraically closed field K of characteristic $p \geq 0$. Then since C coincides up to a choice of basis with its canonical embedding, the automorphism $\mathrm{Aut}(C)$ can be considered as a conjugacy class of subgroups $\mathrm{PGL}_3(K)$ (and in fact of $\mathrm{GL}_3(K)$) by using the action on its non-zero differentials.

The classification of the possible automorphism groups of C as subgroup of $\mathrm{PGL}_3(K)$, as well as the construction of some geometrically complete families, can be found in several articles, such as [**16**, 2.88], [**38**, p.62], [**25**], [**3**] and [**8**] (in chronological order), in which it is often assumed that $p = 0$. We have verified these results independently, essentially by checking which finite subgroups of $\mathrm{PGL}_3(K)$ (as classified in [**19**, Lem.2.3.7]) can occur for plane quartics. It turns out that the classification in characteristic 0 extends to algebraically closed fields K of prime characteristic $p \geq 5$. In the following theorem, we do not indicate the open non-degeneracy conditions on the affine parameters, since we shall not have need of them.

THEOREM 3.1. *Let K be an algebraically closed field whose characteristic p satisfies $p = 0$ or $p \geq 5$. Let C be a genus 3 non-hyperelliptic curve over K. The following are the possible automorphism groups of C, along with geometrically surjective families for the corresponding strata:*

(i) $\{1\}$, *with family* $q_4(x, y, z) = 0$, *where* q_4 *is a homogeneous polynomial of degree* 4;
(ii) $\mathbf{C}_2$, *with family* $x^4 + x^2q_2(y, z) + q_4(y, z) = 0$, *where* q_2 *and* q_4 *are homogeneous polynomials in* y *and* z *of degree* 2 *and* 4;
(iii) $\mathbf{D}_4$, *with family* $x^4 + y^4 + z^4 + rx^2y^2 + sy^2z^2 + tz^2x^2 = 0$;
(iv) $\mathbf{C}_3$, *with family* $x^3z + y(y - z)(y - rz)(y - sz) = 0$;
(v) $\mathbf{D}_8$, *with family* $x^4 + y^4 + z^4 + rx^2yz + sy^2z^2 = 0$;
(vi) $\mathbf{S}_3$, *with family* $x(y^3 + z^3) + y^2z^2 + rx^2yz + sx^4 = 0$;
(vii) $\mathbf{C}_6$, *with family* $x^3z + y^4 + ry^2z^2 + z^4 = 0$;
(viii) $\mathbf{G}_{16}$, *with family* $x^4 + y^4 + z^4 + ry^2z^2 = 0$;
(ix) $\mathbf{S}_4$, *with family* $x^4 + y^4 + z^4 + r(x^2y^2 + y^2z^2 + z^2x^2) = 0$;
(x) $\mathbf{C}_9$, *represented by the quartic* $x^3y + y^3z + z^4 = 0$;
(xi) $\mathbf{G}_{48}$, *represented by the quartic* $x^4 + (y^3 - z^3)z = 0$;
(xii) $\mathbf{G}_{96}$, *represented by the Fermat quartic* $x^4 + y^4 + z^4 = 0$;
(xiii) *(if* $p \neq 7$*)* $\mathbf{G}_{168}$, *represented by the Klein quartic* $x^3y + y^3z + z^3x = 0$.

The families in Theorem 3.1 are geometrically surjective. Moreover, they are irreducible and quasifinite (as we will see in the proof of Theorem 3.3) for all groups except the trivial group and $\mathbf{C}_2$. The embeddings of the automorphism group of these curves into $\mathrm{PGL}_3(K)$ can be

found in Theorem A.1 in Appendix A. Because of the irreducibility properties mentioned in the previous paragraph, each of the corresponding subvarieties serendipitously describes an actual stratum in the moduli space $\mathsf{M}_3^{\mathrm{nh}} \subset \mathsf{M}_3$ of genus 3 non-hyperelliptic curves as defined in Section 2 (see Remark 3.2 below). From the descriptions in A.1, one derives the inclusions between the strata indicated in Figure 1, as also obtained in [**38**, p.65].

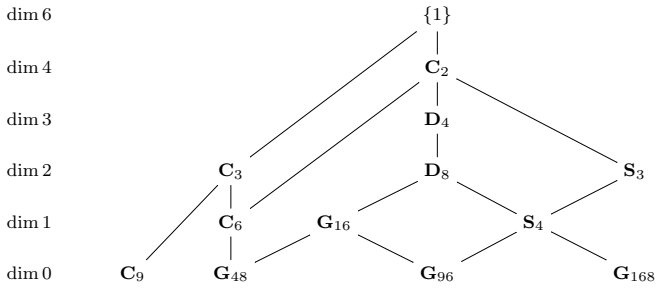


Figure 1: Automorphism groups

Remark 3.2. As promised at the beginning of Section 2, we now indicate two different possible rigidifications of an action of a finite group on plane quartics. Consider the group $\mathbf{C}_3$. Up to conjugation, this group can be embedded into $\mathrm{PGL}_3(K)$ in exactly two ways; as a diagonal matrix with entries proportional to $(\zeta_3, 1, 1)$ or $(\zeta_3^2, \zeta_3, 1)$. This gives rise to two rigidifications in the sense of Lønsted.

While for plane curves of sufficiently high degree, this indeed leads to two families with generic automorphism group $\mathbf{C}_3$, the plane quartics admitting the latter rigidification always admit an extra involution, so that the full automorphism group contains $\mathbf{S}_3$. It is this fortunate phenomenon that still makes a naive stratification by automorphism groups possible for plane quartics. For the same reason, the stratum for the group $\mathbf{S}_3$ is not included in that for $\mathbf{C}_3$, as is claimed incorrectly in [**3**].

3.2. *Construction of representative families*

We now describe how to apply Galois descent to extensions of function fields to determine representative families for the strata in Theorem 3.1 with $|G| > 2$. By Proposition 2.3, this shows that the descent obstruction always vanishes for these strata.

Our constructions lead to families that parametrize the strata much more efficiently; for the case $\mathbf{D}_4$, the family in Theorem 3.1 contains as much as 24 distinct fibers isomorphic with a given curve. Moreover, by Proposition 2.3, in order to write down a complete list of the $\overline{k}$-isomorphism classes of smooth plane quartics defined over a perfect field k we need only consider the k-rational fibers of the new families.

As in Theorem 3.1, we do not specify the condition on the parameters that avoid degenerations (*i.e.* singular curves or a larger automorphism group), but such degenerations will be taken into account in our enumeration strategy in Section 5.

Theorem 3.3. *Let k be a field whose characteristic p satisfies $p = 0$ or $p \geq 7$. The following are representative families for the strata of smooth plane quartics with $|G| > 2$.*

– $G \simeq \mathbf{D}_4$:

$$(a+3)x^4 + (4a^2 - 8b + 4a)x^3y + (12c + 4b)x^3z + (6a^3 - 18ab + 18c + 2a^2)x^2y^2 + (12ac + 4ab)x^2yz + (6bc + 2b^2)x^2z^2 + (4a^4 - 16a^2b + 8b^2 + 16ac + 2ab - 6c)xy^3 + (12a^2c - 24bc + 2a^2b - 4b^2 + 6ac)xy^2z + (36c^2 + 2ab^2 - 4a^2c + 6bc)xyz^2 + (4b^2c - 8ac^2 + 2abc - 6c^2)xz^3 + (a^5 - 5a^3b + 5ab^2 + 5a^2c - 5bc + b^2 - 2ac)y^4 + (4a^3c - 12abc + 12c^2 + 4a^2c - 8bc)y^3z + (6ac^2 + a^2b^2 - 2b^3 - 2a^3c + 4abc + 9c^2)y^2z^2 + (4bc^2 + 4b^2c - 8ac^2)yz^3 + (b^3c - 3abc^2 + 3c^3 + a^2c^2 - 2bc^2)z^4 = 0$$

along with

$$x^4 + 2x^2y^2 + 2ax^2yz + (a^2 - 2b)x^2z^2 + ay^4 + 4(a^2 - 2b)y^3z + 6(a^3 - 3ab)y^2z^2 + 4(a^4 - 4a^2b + 2b^2)yz^3 + (a^5 - 5a^3b + 5ab^2)z^4 = 0.$$

– $G \simeq \mathbf{C}_3$: $x^3z + y^4 + ay^2z^2 + ayz^3 + bz^4 = 0$ *along with* $x^3z + y^4 + ayz^3 + az^4 = 0$;
– $G \simeq \mathbf{D}_8$: $x^4 + x^2yz + y^4 + ay^2z^2 + bz^4 = 0$;
– $G \simeq \mathbf{S}_3$: $x^3z + y^3z + x^2y^2 + axyz^2 + bz^4 = 0$;
– $G \simeq \mathbf{C}_6$: $x^3z + ay^4 + ay^2z^2 + z^4 = 0$;
– $G \simeq \mathbf{G}_{16}$: $x^4 + (y^3 + ayz^2 + az^3)z = 0$;
– $G \simeq \mathbf{S}_4$: $x^4 + y^4 + z^4 + a(x^2y^2 + y^2z^2 + z^2x^2) = 0$;
– $G \simeq \mathbf{C}_9$: $x^3y + y^3z + z^4 = 0$;
– $G \simeq \mathbf{G}_{48}$: $x^4 + (y^3 - z^3)z = 0$;
– $G \simeq \mathbf{G}_{96}$: $x^4 + y^4 + z^4 = 0$;
– *(if* $p \neq 7$*)* $G \simeq \mathbf{G}_{168}$: $x^3y + y^3z + z^3x = 0$.

We do not give the full proof of this theorem, but content ourselves with some families that illustrate the most important ideas therein. Let K be an algebraically closed extension of k. The key fact that we use, which can be observed from the description in Theorem A.1, is that the fibers of the families in Theorem 3.1 all have the same automorphism group G as a subgroup of $\mathrm{PGL}_3(K)$. Except for the zero-dimensional cases, which are a one-off verification, one then proceeds as follows.

(1) The key fact above implies that any isomorphism between two curves in the family is necessarily induced by an element of the normalizer N of G in $\mathrm{PGL}_3(K)$. So one considers the action of this group on the family given in Theorem 3.1.
(2) One determines the subgroup N' of N that sends the family to itself again. The action of N' factors through a faithful action of $Q = N'/G$. By explicit calculation, it turns out that Q is finite for the families in Theorem 3.1 with $|G| > 2$. This shows in particular that these families are already quasifinite on these strata.
(3) One then takes the quotient by the finite action of Q, which is done one the level of function fields over K by using Galois descent. By construction, the resulting family will be representative. For the general theory of Galois descent, we refer to [**40**] and [**37**, App.A].

We now treat some representative cases to illustrate this procedure. In what follows, we use the notation from Theorem A.1 to denote elements and subgroups of the normalizers involved.

Proof. **The case** $G \simeq \mathbf{S}_3$. Here $N = T(K)\widetilde{\mathbf{S}}_3$ contains the group of diagonal matrices $T(K)$. Transforming, one verifies that the subgroup $N' \subsetneq N$ equals $\widetilde{\mathbf{S}_3}$; indeed, since $\widetilde{\mathbf{S}}_3$ fixes the family pointwise, we can restrict to the elements $T(K)$. But then preserving the trivial proportionality of the coefficients in front of x^3z, y^3z, and x^2y^2 forces such a diagonal matrix to be scalar. This implies the result; the group Q is trivial in $\mathrm{PGL}_3(K)$, so we need not adapt our old family since it is geometrically surjective and contains no geometrically isomorphic fibers. A similar argument works for the case $G \cong \mathbf{S}_4$.

The case $G \simeq \mathbf{C}_6$. This time we have to consider the action of the group $D(K)$ on the family $x^3z + y^4 + ry^2z^2 + z^4 = 0$ from Theorem 3.1. After the action of a diagonal matrix with entries $\lambda, \mu, 1$, one obtains the curve $\lambda^3x^3z + \mu^4y^4 + \mu^2ry^2z^2 + z^4 = 0$. We see that we get a new curve in the family if $\lambda^3 = 1$ and $\mu^4 = 1$, in which case the new value for r equals μr. But this equals $\pm r$ since $(\mu^2)^2 = 1$. The degree of the morphism to M_3 induced by this family therefore equals 2. This also follows from the fact that the subgroup N' that we just described contains G as a subgroup of index 2, so that $Q \cong \mathbf{C}_2$.

We have a family over $L = K(r)$ whose fibers over r and $-r$ are isomorphic, and we want to descend this family to $K(a)$, where $a = r^2$ generates the invariant subfield under the automorphism $r \to -r$. This is a problem of Galois descent for the group $Q \cong \mathbf{C}_2$ and the field extension $M \supset L$, with $M = K(r)$ and $L = K(a)$. The curve C over M that we wish to descend to L is given by $x^3z + y^4 + ry^2z^2 + z^4 = 0$. Consider the conjugate curve $C^\sigma : x^3z + y^4 - ry^2z^2 + z^4 = 0$ and the isomorphism $\varphi : C \to C^\sigma$ given by $(x, y, z) \to (x, iy, z)$. Then we do not have $\varphi^\sigma\varphi = \mathrm{id}$. To trivialize the cocycle, we need a larger extension of our function field L.

Take $M' \supset M$ to be $M' = M(\rho)$, with $\rho^2 = r$. Let τ be a generator of the cyclic Galois group of order 4 of the extension $M' \supset L$. Then τ restricts to σ in the extension $M \supset L$, and for $M' \supset L$ one now indeed obtains a Weil cocycle determined by the isomorphism $C \mapsto C^\tau = C^\sigma$ sending (x, y, z) to (x, iy, z). The corresponding coboundary is given by $(x, y, z) \mapsto (x, \rho y, z)$. Transforming, we end up with $x^3z + (\rho y)^4 + r(\rho y)^2z^2 + z^4 = x^3z + ay^4 + ay^2z^2 + z^4 = 0$, which is what we wanted to show. The case $G \cong \mathbf{D}_8$ can be dealt with in a similar way.

The case $G \simeq \mathbf{D}_4$. We start with the usual *Ciani family* from Theorem 3.1, given by $x^4 + y^4 + z^4 + rx^2y^2 + sy^2z^2 + tz^2x^2 = 0$. Using the $\widetilde{\mathbf{S}}_3$-elements from the normalizer $N = D(K)\widetilde{\mathbf{S}}_3$ induces the corresponding permutation group on (r, s, t). The diagonal matrices in $D(K)$ then remain, and they give rise to the transformations $(r, s, t) \mapsto (\pm r, \pm s, \pm t)$ with an even number of minus signs. This is slightly awkward, so we try to eliminate the latter transformations. This can be accomplished by moving the parameters in front of the factors x^4, y^4, z^4. So we instead split up $\mathcal{S}$ into a disjoint union of two irreducible subvarieties by considering the family

$$rx^4 + sy^4 + tz^4 + x^2y^2 + y^2z^2 + z^2x^2 = 0,$$

and its lower-dimensional complement

$$rx^4 + sy^4 + z^4 + x^2y^2 + y^2z^2 = 0.$$

Here the trivial coefficient in front of z^4 is obtained by scaling x, y, z by an appropriate factor in the family $rx^4 + sy^4 + tz^4 + x^2y^2 + y^2z^2 = 0$. Note that because of our description of the normalizer, the number of non-zero coefficients in front of the terms with quadratic factors depends only on the isomorphism class of the curve, and not on the given equation for it in the geometrically surjective Ciani family. This implies that the two families above do not have isomorphic fibers. Moreover, the a priori remaining family $rx^4 + y^4 + z^4 + y^2z^2 = 0$ has larger automorphism group, so we can discard it.

We only consider the first family, which is the most difficult case. As in the previous example, after our modification the elements of $N' \cap D(K)$ are in fact already in G. Therefore $Q = N'/G \subset D(K)\widetilde{\mathbf{S}}_3$ is a quotient of the remaining factor $\widetilde{\mathbf{S}}_3$, which clearly acts freely and is therefore isomorphic with Q. We obtain the invariant subfield $L = K(a, b, c)$ of $M = K(r, s, t)$, with $a = r + s + t$, $b = rs + st + tr$ and $c = rst$ the usual elementary symmetric functions. The cocycle for this extension is given by sending a permutation of (r, s, t) to its associated permutation matrix on (x, y, z). A coboundary is given by the isomorphism $(x, y, z) \mapsto (x + y + z, r\,x + s\,y + t\,z, st\,x + tr\,y + rs\,z)$. Note that this isomorphism is invertible as long as r, s, t are distinct, which we may assume since otherwise the automorphism group of the curve would be larger. Transforming by this coboundary, we get our result.

The case $G \simeq \mathbf{C}_3$. This case needs a slightly different argument. Consider the eigenspace decomposition of the space of quartic monomials in x, y, z under the action of the diagonal generator $(\zeta_3, 1, 1)$ of $\mathbf{C}_3$. The curves with this automorphism correspond to those quartic forms that are eigenforms for this automorphism, which is the case if and only if it is contained in one of the aforementioned eigenspaces. We only need consider the eigenspace spanned by the monomials x^3y, x^3z, y^4, y^3z, y^2z^2, yz^3, z^4; indeed, the quartic forms in the other eigenspaces are all multiples of x and hence give rise to reducible curves.

Using a linear transformation, one eliminates the term with x^3y, and a non-singularity argument shows that we can scale to the case $x^3z + y^4 + ry^3z + sy^2z^2 + tyz^3 + uz^4 = 0$. We can set $r = 0$ by another linear transformation, which then reduces N' to $D(K)$. Depending on whether $s = 0$ or not, one can then scale by these scalar matrices to an equation as in the theorem, which one verifies to be unique by using the same methods as above. The case $G \simeq \mathbf{G}_{16}$ can be proved in a completely similar way. □

REMARK 3.4. As mentioned in Remark 2.2, these constructions give rise to isomorphisms $\mathcal{S} \to S$ in all cases except $\mathbf{D}_4$, and $\mathbf{C}_3$. In these remaining cases, we have constructed a morphism $\mathcal{S} \to S$ that is bijective on points but not an isomorphism. It is possible that no family $\mathcal{C} \to S$ inducing such an isomorphism exists; see [**12**] for results in this direction for hyperelliptic curves.

3.3. *Remaining cases*

We have seen in Proposition 2.3 that if there exist a representative family over k over a given stratum, then the field of moduli needs to be a field of definition for all the curves in this stratum. In [**2**], it is shown that there exist $\mathbb{R}$-points in the stratum $\mathbf{C}_2$ for which the corresponding curve cannot be defined over $\mathbb{R}$. In fact we suspect that this argument can be adapted to show that representative families for this stratum fail to exist even if k is a finite field. However, we can still find arithmetically surjective families over finite fields.

PROPOSITION 3.5. *Let C be a smooth plane quartic with automorphism group $\mathbf{C}_2$ over a finite field k of characteristic different from 2. Let α be a non-square element in k. Then C is k-isomorphic to a curve of one of the following forms:*

$$x^4 + \epsilon x^2y^2 + ay^4 + \mu y^3z + by^2z^2 + cyz^3 + dz^4 = 0 \qquad \text{with } \epsilon = 1 \text{ or } \alpha \text{ and } \mu = 0 \text{ or } 1,$$
$$x^4 + x^2yz + ay^4 + \epsilon y^3z + by^2z^2 + cyz^3 + dz^4 = 0 \qquad \text{with } \epsilon = 0, 1 \text{ or } \alpha,$$
$$x^4 + x^2(y^2 - \alpha z^2) + ay^4 + by^3z + cy^2z^2 + dyz^3 + ez^4 = 0\,.$$

Proof. The involution on the quartic, being unique, is defined over k. Hence by choosing a basis in which this involution is a diagonal matrix, we can assume that it is given by $(x, y, z) \mapsto (-x, y, z)$. This shows that the family $x^4 + x^2q_2(y, z) + q_4(y, z) = 0$ of Theorem 3.1 is arithmetically surjective. We have $q_2(y, z) \neq 0$ since otherwise more automorphisms would exist over K. We now distinguish cases depending on the factorization of q_2 over k.

(i) If q_2 has a multiple root, then we may assume that $q_2(y, z) = ry^2$ where r equals 1 or α. Then either the coefficient b of y^3z in q_4 is 0, in which case we are done, or we can normalize it to 1 using the change of variable $z \mapsto z/b$.

(ii) If q_2 splits over k, then we may assume that $q_2(y, z) = yz$. Then either the coefficient b of y^3z in q_4 is 0, in which case we are done, or we attempt to normalize it by a change of variables $y \mapsto \lambda y$ and $z \mapsto z/\lambda$. This transforms by^3z into $b\lambda^2y^3z$. Hence we can assume b equals 1 or α.

(iii) If q_2 is irreducible over k, then we can normalize $q_2(y,z)$ as $y^2-\alpha z^2$ where α is a non-square in k. This gives us the final family with 5 coefficients.

□

REMARK 3.6. The same proof shows the existence of a quasifinite family for the stratum in Proposition 3.5, since over algebraically fields we can always reduce to the first or second case.

We have seen in Section 2 that a universal family exists for the stratum with trivial automorphism group. Moreover, as M_3 is rational [**20**], this family depends on 6 rational parameters. However, no representative (hence in this case universal) family seems to have been written down so far.

Classically, when the characteristic p is different from 2 or 3, there are at least two ways to construct quasifinite families for the generic stratum. The first method fixes bitangents of the quartic and leads to the so-called Riemann model; see [**?**, **29**, **39**] for relations between this construction, the moduli of 7 points in the projective plane and the moduli space $\mathsf{M}_3^{(2)}$. The other method uses flex points, as in [**35**, Prop.1]. In neither case can we get such models over the base field k, since for a general quartic, neither its bitangents nor its flex points are defined over k. We therefore content ourselves with the following result which was kindly provided to us by J. Bergström.

PROPOSITION 3.7 (Bergström). *Let C be a smooth plane quartic over a field k admitting a rational point over a field of characteristic $\neq 2$. Then C is isomorphic to a curve of one of the following forms:*

$$\begin{aligned}
m_1x^4+m_2x^3y+m_4x^2y^2+m_6x^2z^2+m_7xy^3+xy^2z+m_{11}y^4+m_{12}y^3z+y^2z^2+yz^3&=0,\\
m_1x^4+m_2x^3y+m_4x^2y^2+m_6x^2z^2+xy^3+m_{11}y^4+m_{12}y^3z+y^2z^2+yz^3&=0,\\
m_1x^4+m_2x^3y+m_4x^2y^2+m_6x^2z^2+m_{11}y^4+m_{12}y^3z+y^2z^2+yz^3&=0,\\
m_1x^4+m_2x^3y+m_4x^2y^2+m_6x^2z^2+xy^3+xy^2z+m_{11}y^4+m_{12}y^3z+yz^3&=0,\\
m_1x^4+m_2x^3y+m_4x^2y^2+m_6x^2z^2+xy^2z+m_{11}y^4+m_{12}y^3z+yz^3&=0,\\
x^4+m_2x^3y+m_4x^2y^2+m_6x^2z^2+m_7xy^3+m_{11}y^4+m_{12}y^3z+yz^3&=0,\\
m_2x^3y+m_4x^2y^2+m_6x^2z^2+m_7xy^3+m_{11}y^4+m_{12}y^3z+yz^3&=0,\\
x^3z+m_4x^2y^2+m_7xy^3+m_8xy^2z+xyz^2+m_{11}y^4+m_{12}y^3z+m_{13}y^2z^2+yz^3&=0,\\
x^3z+m_4x^2y^2+m_7xy^3+m_8xy^2z+m_{11}y^4+m_{12}y^3z+m_{13}y^2z^2+yz^3&=0,\\
x^4+m_4x^2y^2+m_5x^2yz+m_7xy^3+m_8xy^2z+m_{11}y^4+m_{12}y^3z+yz^3&=0.
\end{aligned}$$

Proof. We denote by $m_1,\dots,m_{15}$ the coefficients of the quartic C, with its monomials ordered as

$$x^4,x^3y,x^3z,x^2y^2,x^2yz,x^2z^2,xy^3,xy^2z,xyz^2,xz^3,y^4,y^3z,y^2z^2,yz^3,z^4. \tag{3.1}$$

As there is a rational point on the curve, we can transform this point to be $(0:0:1)$ with tangent equal to $y=0$. We then have $m_{15}=m_{10}=0$, and we can scale to ensure that $m_{14}=1$. The proof now divides into cases.

Case 1: $m_6\neq 0$. Consider the terms $m_6x^2(z^2+m_3/m_6xz)$. Then by a further change of variables $z\to z+m_3\,x/(2m_6)$ we can assume $m_3=0$ without perturbing the previous conditions. Starting with this new equation, we can now cancel m_5 in the same way, and finally m_9 (note that the order in which we cancel the coefficients m_3,m_5,m_9 is important, so as to avoid re-introducing non-zero coefficients).

(i) If m_8 and m_{13} are non-zero, then we can ensure that $m_8=m_{13}=1$ by changing variables $(x:y:z)\to(rx:sy:tz)$ such that $m_8rs^2t=\alpha,\quad m_{13}s^2t^2=\alpha,\quad st^3=\alpha$ for

a given $\alpha \neq 0$ and then divide the whole equation by α. One calculates that it is indeed possible to find a solution (r, s, t, α) to these equations in k^4.

(ii) If $m_8 = 0, m_{13} \neq 0, m_7 \neq 0$, then we can transform to $m_{13} = m_7 = 1$ as above;
(iii) If $m_8 = 0, m_{13} \neq 0, m_7 = 0$, then we can transform to $m_{13} = 1$;
(iv) If $m_8 \neq 0, m_{13} = 0, m_7 \neq 0$, then we can transform to $m_8 = m_7 = 1$;
(v) If $m_8 \neq 0, m_7 = m_{13} = 0$, then we can transform to $m_8 = 1$;
(vi) If $m_{13} = m_8 = 0, m_1 \neq 0$, then we can transform to $m_1 = 1$;
(vii) If $m_{13} = m_8 = m_1 = 0$, then we need not do anything.

Case 2: $m_6 = 0, m_3 \neq 0$**.** As before, working in the correct order we can ensure that $m_1 = m_2 = m_5 = 0$ by using the non-zero coefficient m_3.

(viii) If $m_9 \neq 0$, we can transform to $m_3 = m_9 = 1$;
(ix) If $m_9 = 0$, we can transform to $m_3 = 1$.

Case 3: $m_6 = m_3 = 0$**.**

(x) If $m_1 \neq 0$, then put $m_1 = 1$. Using m_{14}, we can transform to $m_9 = m_{13} = 0$ and using m_1, we can transform to $m_2 = 0$.

The proof is now concluded by noting that if $m_1 = m_3 = m_6 = m_{10} = m_{15} = 0$, then the quartic is reducible. □

Bergström has also found models when rational points are not available, but these depend on as many as 9 coefficients. Using the Hasse-Weil-Serre bound, one shows that when k is a finite field with $\#k > 29$, the models in Proposition 3.7 constitute an arithmetically surjective family of dimension 7, one more than the dimension of the moduli space.

Over finite fields k of characteristic > 7 and with $\#k \leq 29$ there are always pointless curves [**18**]. Our experiments showed that except for one single example, these curves all have non-trivial automorphism group. As such, they already appear in the non-generic family. The exceptional pointless curve, defined over $\mathbb{F}_{11}$, is

$$7x^4 + 3x^3y + 10x^3z + 10x^2y^2 + 10x^2yz + 6x^2z^2 + 7xy^2z + xyz^2 + 4xz^3 + 9y^4 + 5y^3z + 8y^2z^2 + 9yz^3 + 9z^4 = 0\,.$$

4. *Computation of twists*

Let C be a smooth plane quartic defined over a finite field $k = \mathbb{F}_q$ of characteristic p. In this section we will explain how to compute the *twists* of C, *i.e.* the k-isomorphism classes of the curves isomorphic with C over $\overline{k}$.

Let $\mathrm{Twist}(C)$ be the set of twists of C. This set is in bijection with the cohomology set $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(C))$, (see [**36**, Chap.X.2]). More precisely, if $\beta : C' \to C$ is any $\overline{k}$-isomorphism, the corresponding element in $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(C))$ is given by $\sigma \mapsto \beta^\sigma \beta^{-1}$. Using the fact that $\mathrm{Gal}(\overline{k}/k)$ is pro-cyclic generated by the Frobenius morphism $\varphi : x \mapsto x^q$, computing $H^1(\mathrm{Gal}(\overline{k}/k), \mathrm{Aut}(C))$ boils down to computing the equivalence classes of $\mathrm{Aut}(C)$ for the relation

$$g \sim h \iff \exists \alpha \in \mathrm{Aut}(C),\ g\alpha = \alpha^\varphi h,$$

as in [**26**, Prop.9]. For a representative α of such a *Frobenius conjugacy class*, there will then exist a curve C_α and an isomorphism $\beta : C_\alpha \to C$ such that $\beta^\varphi \beta^{-1} = \alpha$.

As isomorphisms between smooth plane quartics are linear [**8**, 6.5.1], β lifts to an automorphism of $\mathbb{P}^2$, represented by an element B of $\mathrm{GL}_3(\overline{k})$, and we will then have that

$C_\alpha = B^{-1}(C)$ as subvarieties of $\mathbb{P}^2$. This is the curve defined by the equation obtained by substituting $B(x,y,z)^t$ for the transposed vector $(x,y,z)^t$ in the quartic relations defining C.

4.1. *Algorithm to compute the twists of a smooth plane quartic*

We first introduce a probabilistic algorithm to calculate the twists of C. It is based on the explicit form of Hilbert 90 (see [**34**] and [**11**]).

Let $\alpha \in \mathrm{Aut}(C)$ defined over a minimal extension $\mathbb{F}_{q^n}$ of $k = \mathbb{F}_q$ for some $n \geq 1$, and let C_α be the twist of C corresponding to α. We construct the transformation B from the previous section by solving the equation $B^\varphi = AB$ for a suitable matrix representation A of α. Since the curve is canonically embedded in $\mathbb{P}^2$, the representation of the action of $\mathrm{Aut}(C)$ on the regular differentials gives a natural embedding of $\mathrm{Aut}(C)$ in $\mathrm{GL}_3(\mathbb{F}_{q^n})$. We let A be the corresponding lift of α in this representation. As $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is topologically generated by φ and α is defined over a finite extension of $\mathbb{F}_q$, there exists an integer m such that the cocycle relation $\alpha_{\sigma\tau} = \alpha_\tau^\sigma \alpha_\sigma$ reduces to the equality $A^{\varphi^{m-1}} \cdots A^\varphi A = \mathrm{Id}$. Using the multiplicative form of Hilbert's Theorem 90, we let

$$B = P + \sum_{i=1}^{m-1} P^{\varphi^i} A^{\varphi^{i-1}} \cdots A^\varphi A$$

with P a random matrix 3×3 with coefficients in $\mathbb{F}_{q^m}$ chosen in such a way that at the end B is invertible. We will then have $B^\varphi = BA^{-1}$, the inverse of the relation above, so that we can apply B directly to the defining equation of the quartic. Note that the probability of success of the algorithm is bigger than $1/4$ (see [**11**, Prop.1.3]).

To estimate the complexity, we need to show that m is not too large compared with n. We have the following estimate.

LEMMA 4.1. *Let e be the exponent of $\mathrm{Aut}(C)$. Then $m \leq ne$.*

Proof. By definition of n we have $\alpha^{\varphi^n} = \alpha$. Let $\gamma = \alpha^{\varphi^{n-1}} \cdots \alpha^\varphi \alpha$, and let N be the order of γ in $\mathrm{Aut}_{\mathbb{F}_{q^n}}(C)$. Since $\gamma^{\varphi^n} = \gamma$ and $\mathrm{Id} = \gamma^N = \alpha^{\varphi^{Nn-1}} \cdots \alpha^\varphi \alpha$, we can take $m \leq nN \leq ne$. □

In practice we compute m as the smallest integer such that $\alpha^{\varphi^{m-1}} \cdots \alpha^\varphi \alpha$ is the identity.

4.2. *How to compute the twists by hand when $\#\,\mathrm{Aut}(C)$ is small*

When the automorphism group is not too complicated, it is often possible to obtain representatives of the classes in $H^1(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), \mathrm{Aut}(C))$ and then to compute the twists by hand, a method used in genus 2 in [**6**]. We did this for $\mathrm{Aut}(C) = \mathbf{C}_2, \mathbf{D}_4, \mathbf{C}_3, \mathbf{D}_8, \mathbf{S}_3$.

Let us illustrate this in the case of $\mathbf{D}_8$. As we have seen in Theorem 3.3, any curve $C/\mathbb{F}_q$ with $\mathrm{Aut}(C) \simeq \mathbf{D}_8$ is $\overline{\mathbb{F}}_q$-isomorphic with some curve $x^4 + x^2yz + y^4 + ay^2z^2 + bz^4$ with $a, b \in \mathbb{F}_q$. The problem splits up into several cases according to congruences of $q - 1 \pmod 4$ and the class of $b \in \mathbb{F}_q^*/(\mathbb{F}_q^*)^4$. We will assume that $4 \mid (q-1)$ and b is a fourth power, say $b = r^4$ in $\mathbb{F}_q$. The 8 automorphisms are then defined over $\mathbb{F}_q$: if i is a square root of -1, the automorphism group is generated by

$$S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -i \end{bmatrix} \text{ and } T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & r \\ 0 & r^{-1} & 0 \end{bmatrix}.$$

Representatives of the Frobenius conjugacy classes (which in this case reduce to the usual conjugacy classes) are then Id, S, S^2, T and ST. So there are 5 twists.

Let us give details for the computation of the twist corresponding to the class of T. We are looking for a matrix B such that $TB = B^\varphi$ up to scalars. We choose B such that $B(x, y, z)^t = (x, \alpha y + \beta z, \gamma y + \delta z)^t$. Then we need to solve the following system:

$$\alpha^\varphi = r\gamma\,, \beta^\varphi = r\delta\,, \gamma^\varphi = r^{-1}\alpha\,, \delta^\varphi = r^{-1}\beta.$$

The first equation already determines γ in terms of α. So we need only satisfy the compatibility condition given by the second equation. Applying φ, we get $\alpha^{\varphi^2} = (r\gamma)^\varphi = r\gamma^\varphi = r(\alpha/r) = \alpha$. Reasoning similarly for β and δ, we see that it suffices to find α and β in $\mathbb{F}_{q^2}$ such that $\det \begin{pmatrix} \alpha & \beta \\ \alpha^\varphi/r & \beta^\varphi/r \end{pmatrix} \neq 0$. We can take $\alpha = \sqrt{\tau}$ and $\beta = 1$, with τ a primitive element of $\mathbb{F}_q^*$. Transforming, we get the twist

$$x^4 + rx^2y^2 - r\tau x^2z^2 + (ar^2 + 2r^4)y^4 + (-2ar^2\tau + 12r^4\tau)y^2z^2 + (ar^2\tau^2 + 2r^4\tau^2)z^4 = 0.$$

5. *Implementation and experiments*

We combine the results obtained in Sections 3 and 4 to compute a database of representatives of k-isomorphism classes of genus 3 non-hyperelliptic curves when $k = \mathbb{F}_p$ is a prime field of small characteristic $p > 7$.

5.1. *The general strategy*

We proceed in two steps. The hardest one is to compute one representative defined over k for each $\bar{k}$-isomorphism class, keeping track of its automorphism group. Once this is done, one can apply the techniques of Section 4 to get one representative for each isomorphism class.

In order to work out the computation of representatives for the $\bar{k}$-isomorphism classes, the naive approach would start by enumerating all plane quartics over k by using the 15 monomial coefficients $m_1, \ldots, m_{15}$ ordered as in Equation (3.1) and for each new curve to check whether it is smooth and not $\bar{k}$-isomorphic to the curves we already kept as representatives. This would have to be done for up to p^{15} curves. For $p > 29$, a better option is to use Proposition 3.7 to reduce to a family with 7 parameters.

In both cases, checking for $\bar{k}$-isomorphism is relatively fast as we make use of the so-called 13 *Dixmier-Ohno invariants*. These are generators for the algebra of invariants of ternary quartics forms under the action of $\mathrm{SL}_3(\mathbb{C})$. Among them 7 are denoted I_3, I_6, I_9, I_{12}, I_{15}, I_{18} and I_{27} (of respective degree 3, 6, ..., 27 in the m_i's) and are due to Dixmier [**7**]; one also needs 6 additional invariants that are denoted J_9, J_{12}, J_{15}, J_{18}, I_{21} and J_{21} (of respective degree 9, 12, ..., 21 in the m_i's) and that are due to Ohno [**28**, **10**]. These invariants behave well after reduction to $\mathbb{F}_p$ for $p > 7$ and the discriminant I_{27} is 0 if and only if the quartic is singular. Moreover, if two quartics have different Dixmier-Ohno invariants (seen as points in the corresponding weighted projective space, see for instance [**22**]) then they are not $\bar{k}$-isomorphic. We suspect that the converse is also true (as it is over $\mathbb{C}$). This is at least confirmed for our values of p since at the end we obtain $p^6 + 1$ $\overline{\mathbb{F}}_p$-isomorphism classes, as predicted by [**4**].

The real drawback of this approach is that we cannot keep track of the automorphism groups of the curves, which we need in order to compute the twists. Unlike the hyperelliptic curves of genus 3 [**22**], for which one can read off the automorphism group from the invariants of the curve, we lack such a dictionary for the larger strata of plane smooth quartics.

We therefore proceed by ascending up the strata, as summarized in Algorithm 1. In light of Proposition 2.3, we first determine the $\bar{k}$-isomorphism classes for quartics in the small strata by using the representative families of Theorem 3.3. In this case, the parametrizing is done in an optimal way and the automorphism group is explicitly known. Once a stratum is enumerated, we consider a higher one and keep a curve in this new stratum if and only if its Dixmier-Ohno invariants have not already appeared. As mentioned at the end of Section 3, this approach still

finds all pointless curves (except one for $\mathbb{F}_{11}$) for $p \leq 29$. We can then use the generic families in Proposition 3.5 and Proposition 3.7.

Algorithm 1: Database of representatives for $\mathbb{F}_p$-isomorphism classes of smooth plane quartics

Input : A prime characteristic $p > 7$.
Output: A list $\mathcal{L}_p$ of mutually non-$\mathbb{F}_p$-isomorphic quartics representing all isomorphism classes of smooth plane quartics over $\mathbb{F}_p$.

1 $\mathcal{L}_p := \emptyset$;
2 **for** $\mathbf{G} :=$
$\mathbf{G_{168}}, \mathbf{G_{96}}, \mathbf{G_{48}}, \mathbf{C_9}$, *// Dim. 0 strata (first)*
$\mathbf{C_6}, \mathbf{S_4}, \mathbf{G_{16}}$, *// Dim. 1 strata (then)*
$\mathbf{S_3}, \mathbf{C_3}, \mathbf{D_8}$, *// Dim. 2 strata (then)*
$\mathbf{D_4}, \mathbf{C_2}, \{\mathbf{1}\}$ *// Dim. 3, 4 and 5 strata (finally)*
do
3 **forall the** *quartics Q defined by the families of*
Theorem 3.3 *if* $\mathbf{G}$ *defines a stratum of dim.* ≤ 3,
Proposition 3.5 *if* $\mathbf{G} = \mathbf{C}_2$,
Proposition 3.7 *if* $\mathbf{G} = \{1\}$
do
4 $(I_3 : I_6 : \ldots : J_{21} : I_{27}) :=$ Dixmier-Ohno invariants of Q;
5 **if** $\mathcal{L}_p(I_3 : I_6 : \ldots : J_{21} : I_{27})$ *is not defined* **then**
6 $\mathcal{L}_p(I_3 : I_6 : \ldots : J_{21} : I_{27}) := \{Q$ and its twists$\}$ `// cf. Section 4`
7 **if** $\mathcal{L}_p$ *contains* $p^6 + 1$ *entries* **then return** $\mathcal{L}_p$;

5.2. *Implementation details*

We split our implementation of Algorithm 1 into two parts. The first one, developed with the Magma computer algebra software, handles quartics in the strata of dimension 0, 1, 2 and 3. These strata have many fewer points than the ones with geometric automorphism group $\mathbf{C}_2$ and $\{1\}$ but need linear algebra routines to compute twists. The second part has been developed in the C-language for two reasons: to efficiently compute the Dixmier-Ohno invariants in the corresponding strata and to decrease the memory needed. We now discuss these two issues.

5.2.1. *Data structures.* We decided to encode elements of $\mathbb{F}_p$ in bytes. This limits us to $p < 256$, but this is not a real constraint since larger p seem as yet infeasible (even considering the storage issue). As most of the time is spent computing Dixmier-Ohno invariants, we group the multiplications and additions that occur in these calculations as much as possible in 64-bit microprocessor words before reducing modulo p. This decreases the number of divisions as much as possible.

To deal with storage issues in Step 6 of Algorithm 1, only the 13 Dixmier-Ohno invariants of the quartics are made fully accessible in memory; we store the full entries in a compressed file. These entries are sorted by these invariants and additionally list the automorphism group, the number of twists, and for each twist, the coefficients of a representative quartic, its automorphism group and its number of points.

5.2.2. *Size of the hash table.* We make use of an open addressing hash table to store the list $\mathcal{L}_p$ from Algorithm 1. This hash table indexes p^5 buckets, all of equal size $(1 + \varepsilon) \times p$ for some overhead ε. Given a Dixmier-Ohno 13-tuple of invariants, its first five elements (eventually modified by a bijective linear combination of the others to get a more uniform distribution)

give us the address of one bucket of the table of invariants. We then store the last eight elements of the Dixmier-Ohno 13-tuple at the first free slot in this bucket. The total size of the table is thus $8\,(1+\varepsilon)\times p^6$ bytes.

All the buckets do not contain the same number of invariants at the end of the enumeration, and we need to fix ε such that it is very unlikely that one bucket in the hash table goes over its allocated room. To this end, we assume that Dixmier-Ohno invariants behave like random 13-tuples, *i.e.* each of them has probability $1/p^5$ to address a bucket. Experimentally, this assumption seems to be true. Therefore the probability that one bucket $\mathcal{B}$ contains n invariants after k trials follows a binomial distribution,

$$\mathrm{P}(\mathcal{B}=n)=\binom{n}{k}\times\frac{(p^5-1)^{k-n}}{(p^5)^k}=\binom{n}{k}\times\left(\frac{1}{p^5}\right)^n\times\left(1-\frac{1}{p^5}\right)^{k-n}.$$

Now let $k\approx p^6$. Then $k\times(1/p^5)\approx p$, which is a fixed small parameter. In this setting, Poisson approximation yields $\mathrm{P}(\mathcal{B}=n)\simeq p^n\,e^{-p}/n\,!$, so the average number of buckets that contain n entries at the end is about $p^5\ \mathrm{P}(\mathcal{B}=n)\simeq p^{5+n}\,e^{-p}/n\,!$ and it remains to choose $n=(1+\varepsilon)\,p$, and thus ε, such that this probability is negligible. We draw ε as a function of p when this probability is smaller than 10^{-3} in Figure 2. For $p=53$, this yields a hash table of 340 gigabytes.

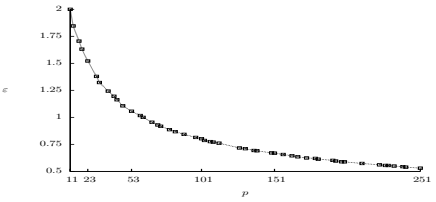


Figure 2: Overhead ε

5.3. *Results and first observations*

We have used our implementation of Algorithm 1 to compute the list $\mathcal{L}_p$ for primes p between 11 and 53. Table 1 gives the corresponding timings and database sizes (once stored in a compressed file). Because of their size, only the databases $\mathcal{L}_p$ for $p=11$ or $p=13$, and a program to use them, are available online[†].

Table 1: Calculation of $\mathcal{L}_p$ on a 32 AMD-Opteron 6272 based server

p	11	13	17	19	23	29	31	37	41	43	47	53
Time	42s	1m 48s	10m	20m 30s	1h 7m	4h 36m	6h 48m	22h 48m	1d 23h	2d 7h	5d 22h	7d 19
Db size	27Mb	68Mb	377Mb	748Mb	2.5Gb	11.5 Gb	16Gb	51Gb	97Gb	128Gb	224Gb	460Gb

As a first use of our database, and sanity check, we can try to interpolate formulas for the number of $\mathbb{F}_p$- or $\overline{\mathbb{F}}_p$-isomorphism classes of genus 3 plane quartics over $\mathbb{F}_p$ with given automorphism group. The resulting polynomials in p are given in Table 2. The '$+[a]_{\text{ condition}}$' notation means that a should be added if the 'condition' holds.

Most of these formulas can actually be proved (we **emphasize** the ones we are able to prove in Table 2). In particular, it is possible to derive the number of most of the $\#\overline{\mathbb{F}}_p$-isomorphic classes from the representative families given in Theorem 3.3; one merely needs to consider the degeneration conditions between the strata. For example, for the strata of dimension 1, the singularities at the boundaries of the strata of dimension 1 corresponding to strata with larger automorphism group are given by $\mathbb{F}_p$-points, except for the stratum $\mathbf{S}_4$. The latter stratum corresponds to singular curves for $a\in\{-2,-1,2\}$, and the Klein quartic corresponds to $a=0$. But the Fermat quartic corresponds to both roots of the equation $a^2+3a+18$ (note that the

[†] `http://perso.univ-rennes1.fr/christophe.ritzenthaler/programme/qdbstats-v3_0.tgz`.

Table 2: Number of isomorphism classes of plane quartics with given automorphism group

G	$\#\overline{\mathbb{F}}_p$-isomorphism classes	$\#\mathbb{F}_p$-isomorphism classes
$\mathbf{G_{168}}$	$\mathbf{1}$	$\mathbf{4} + [\mathbf{2}]_{\mathbf{p=1,2,4 \bmod 7}}$
$\mathbf{G_{96}}$	$\mathbf{1}$	$\mathbf{6} + [\mathbf{4}]_{\mathbf{p=1 \bmod 4}}$
$\mathbf{G}_{48}$	$\mathbf{1}$	$\mathbf{4} + [\mathbf{10}]_{\mathbf{p=1 \bmod 12}} + [\mathbf{2}]_{\mathbf{p=5 \bmod 12}} + [\mathbf{4}]_{\mathbf{p=7 \bmod 12}}$
$\mathbf{C_9}$	$\mathbf{1}$	$\mathbf{1} + [\mathbf{8}]_{\mathbf{p=1 \bmod 9}} + [\mathbf{2}]_{\mathbf{p=4 \bmod 9}} + [\mathbf{6}]_{\mathbf{p=7 \bmod 9}}$
$\mathbf{C_6}$	$\mathbf{p-2}$	$\mathbf{2} \times (\mathbf{1} + [\mathbf{2}]_{\mathbf{p=1 \bmod 3}}) \times \#\overline{\mathbb{F}}_\mathbf{p}$**-iso.**
$\mathbf{S}_4$	$\mathbf{p-4} - [\mathbf{2}]_{\mathbf{p=1,2,4 \bmod 7}}$	$\mathbf{5} \times \#\overline{\mathbb{F}}_\mathbf{p}$**-iso**.
$\mathbf{G}_{16}$	$\mathbf{p-2}$	$\mathbf{2} \times (\mathbf{2}\,(\mathbf{p-3}) + [\mathbf{p-2}]_{\mathbf{p=1 \bmod 4}})$
$\mathbf{S_3}$	$\mathbf{p^2 - 3\,p + 4} + [\mathbf{2}]_{\mathbf{p=1,2,4 \bmod 7}}$	$\mathbf{3} \times \#\overline{\mathbb{F}}_\mathbf{p}$**-iso.**
$\mathbf{C_3}$	$\mathbf{p^2 - p}$	$(\mathbf{1} + [\mathbf{2}]_{\mathbf{p=1 \bmod 3}}) \times \#\overline{\mathbb{F}}_\mathbf{p}$**-iso.**
$\mathbf{D_8}$	$\mathbf{p^2 - 4\,p + 6} + [\mathbf{2}]_{\mathbf{p=1,2,4 \bmod 7}}$	$\mathbf{4} \times \#\overline{\mathbb{F}}_\mathbf{p}$**-iso.**$-\mathbf{3\,p + 8}$
$\mathbf{D_4}$	$\mathbf{p^3 - 3\,p^2 + 5\,p - 5}$	$\mathbf{2\,p^3 - 8\,p^2 + 17\,p - 19}$
$\mathbf{C_2}$	$p^4 - 2\,p^3 + 2\,p^2 - 3\,p + 1 - [2]_{p=1,2,4 \bmod 7}$	$\mathbf{2} \times \#\overline{\mathbb{F}}_\mathbf{p}$**-iso.**
$\{\mathbf{1}\}$	$p^6 - p^4 + p^3 - 2\,p^2 + 3\,p - 1$	$\#\overline{\mathbb{F}}_\mathbf{p}$**-iso.**
Total	$\mathbf{p^6 + 1}$	$p^6 + p^4 - p^3 + 2\,p^2 - 4\,p - 1 + 2\,(p \bmod 4)$ $+2\,[p^2 + p + 2 - (p \bmod 4)]_{p=1,4,7 \bmod 9} + [6]_{p=1 \bmod 9}$ $+[2\,p + 6]_{p=1 \bmod 4} + [2]_{p=1,2,4 \bmod 7}$

family for the stratum $\mathbf{S}_4$ is no longer representative at that boundary point). The number of roots of this equation in $\mathbb{F}_p$ depends on the congruence class of p modulo 7.

One proceeds similarly for the other strata of small dimension; the above degeneration turns out to be the only one that gives a dependence on p. To our knowledge, the point counts for the strata $\mathbf{C}_2$ and $\{1\}$ are still unproved. Note that the total number of $\overline{\mathbb{F}}_p$-isomorphism classes is known to be $p^6 + 1$ by [**4**], so the number of points on one determines the one on the other.

Determining the number of twists is a much more cumbersome task, but can still be done by hand by making explicit the cohomology classes of Section 4. For the automorphism groups $\mathbf{G_{168}}$, $\mathbf{G_{96}}$, $\mathbf{G}_{48}$ and $\mathbf{S_4}$, we have recovered the results published by Meagher and Top in [**26**] (a small subset of the curves defined over $\mathbb{F}_p$ with automorphism group $\mathbf{G}_{16}$ was studied there as well).

5.4. *Distribution according to the number of points*

Once the lists $\mathcal{L}_p$ are determined, the most obvious invariant function on this set of isomorphism classes is the number of rational points of a representative of the class. To observe the distributions of these classes according to their number of points was the main motivation of our extensive computation. In Appendix B, we give some graphical interpretations of the results for prime field $\mathbb{F}_p$ with $11 \leq p \leq 53$[†].

Although we are still at an early stage of exploiting the data, we can make the following remarks:

(1) Among the curves whose number of points is maximal or minimal, there are only curves with non-trivial automorphism group, except for a pointless curve over $\mathbb{F}_{11}$ mentioned at the end of Section 3.3. While this phenomenon is not true in general (see for instance [**30**, Tab.2] using the form $43, \#1$ over $\mathbb{F}_{167}$), it shows that the usual recipe to construct

[†]The numerical values we exploited can be found at `http://perso.univ-rennes1.fr/christophe.ritzenthaler/programme/qdbstats-v3_0.tgz`.

maximal curves, namely by looking in families with large non-trivial automorphism groups, makes sense over small finite fields. It also shows that to observe the behavior of our distribution at the borders of the Hasse-Weil interval, we have to deal with curves with many automorphisms, which justifies the exhaustive search we made.

(2) Defining the trace t of a curve $C/\mathbb{F}_q$ by the usual formula $t = q + 1 - \#C(\mathbb{F}_q)$, one sees in Fig. B.1a that the "normalized trace" $\tau = t/\sqrt{q}$ accurately follows the asymptotic distribution predicted by the general theory of Katz-Sarnak [**21**]. For instance, the theory predicts that the mean normalized trace should converge to zero when q tends to infinity. We found the following estimates for $q = 11, 17, 23, 29, 37, 53$:

$$4 \cdot 10^{-3}, \quad 1 \cdot 10^{-3}, \quad 4 \cdot 10^{-4}, \quad 2 \cdot 10^{-4}, \quad 6 \cdot 10^{-5}, \quad 3 \cdot 10^{-5}.$$

(3) Our extensive computations enable us to spot possible fluctuations with respect to the symmetry of the limit distribution of the trace, a phenomenon that to our knowledge has not been encountered before (see Fig. B.1b). These fluctuations are related to the *Serre's obstruction* for genus 3 [**30**] and do not appear for genus ≤ 2 curves. Indeed, for these curves (and more generally for hyperelliptic curves of any genus), the existence of a quadratic twist makes the distribution completely symmetric. The fluctuations also cannot be predicted by the general theory of Katz and Sarnak, since this theory depends only on the monodromy group, which is the same for curves, hyperelliptic curves or abelian varieties of a given genus or dimension. Trying to understand this new phenomenon is a challenging task and indeed the initial purpose of constructing our database.

References

1. D. Abramovich and F. Oort. Alterations and resolution of singularities. In *Resolution of singularities (Obergurgl, 1997)*, volume 181 of *Progr. Math.*, pages 39–108. Birkhäuser, Basel, 2000.
2. M. Artebani and S. Quispe. Fields of moduli and fields of definition of odd signature curves. *Arch. Math.*, 99(4):333–344, 2012.
3. F. Bars. Automorphism groups of genus 3 curves. Notes del seminari Corbes de Gèneres 3, 2006.
4. J. Bergström. PhD thesis, Kungl. Tekniska Högskolan, Stockholm, 2001.
5. J. Bergström. Cohomology of moduli spaces of curves of genus three via point counts. *J. Reine Angew. Math.*, 622:155–187, 2008.
6. G. Cardona. On the number of curves of genus 2 over a finite field. *Finite Fields Appl.*, 9(4):505–526, 2003.
7. J. Dixmier. On the projective invariants of quartic plane curves. *Adv. in Math.*, 64:279–304, 1987.
8. I. V. Dolgachev. *Classical algebraic geometry*. Cambridge University Press, Cambridge, 2012. A modern view.
9. D. M. Freeman and T. Satoh. Constructing pairing-friendly hyperelliptic curves using Weil restriction. *J. of Number Theory*, 131(5):959–983, 2011.
10. M. Girard and D. R. Kohel. Classification of genus 3 curves in special strata of the moduli space. Hess, Florian (ed.) et al., Algorithmic number theory. 7th international symposium, ANTS-VII, Berlin, Germany, July 23–28, 2006. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 4076, 346-360 (2006)., 2006.
11. S. P. Glasby and R. B. Howlett. Writing representations over minimal fields. *Comm. Algebra*, 25(6):1703–1711, 1997.
12. S. Gorchinskiy and F. Viviani. Picard group of moduli of hyperelliptic curves. *Math. Z.*, 258(2):319–331, 2008.
13. A. Guillevic and D. Vergnaud. Genus 2 hyperelliptic curve families with explicit jacobian order evaluation and pairing-friendly constructions. In *Pairing-based cryptography—Pairing 2012*, volume 7708 of *Lecture Notes in Comput. Sci.*, pages 234–253. Springer, Berlin, 2012.
14. J. Harris and I. Morrison. *Moduli of curves*, volume 187 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.
15. J. Harris and D. Mumford. On the Kodaira dimension of the moduli space of curves. *Invent. Math.*, 67(1):23–88, 1982. With an appendix by William Fulton.
16. H.-W. Henn. Die Automorphismengruppen der algebraischen Funktionenkorper vom Geschlecht 3, 1976.
17. M. Homma. Automorphisms of prime order of curves. *Manuscripta Math.*, 33(1):99–109 (1980).

18. E. W. Howe, K. E. Lauter, and J. Top. Pointless curves of genus three and four. In *Algebra, Geometry, and Coding Theory (AGCT 2003) (Y. Aubry and G. Lachaud, eds.)*, volume 11 of *Séminaires et Congrès*. Société Mathématique de France, Paris, 2005.
19. B. Huggins. *Fields of moduli and fields of definition of curves*. PhD thesis, University of California, Berkeley, Berkeley, California, 2005. `http://arxiv.org/abs/math.NT/0610247`.
20. P. Katsylo. Rationality of the moduli variety of curves of genus 3. *Comment. Math. Helv.*, 71(4):507–524, 1996.
21. N. M. Katz and P. Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.
22. R. Lercier and C. Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.
23. R. Lercier, C. Ritzenthaler, and J. Sijsling. Fast computation of isomorphisms of hyperelliptic curves and explicit descent. In E. W. Howe and K. S. Kedlaya, editors, *Proceedings of the Tenth Algorithmic Number Theory Symposium*, pages 463–486. Mathematical Sciences Publishers, 2012.
24. K. Lønsted. The structure of some finite quotients and moduli for curves. *Comm. Algebra*, 8(14):1335–1370, 1980.
25. K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein. The locus of curves with prescribed automorphism group. Communications in arithmetic fundamental groups (Kyoto, 1999/2001). Sūrikaisekikenkyūsho Kōkyūroku No. 1267 (2002), 112–141.
26. S. Meagher and J. Top. Twists of genus three curves over finite fields. *Finite Fields Appl.*, 16(5):347–368, 2010.
27. P. E. Newstead. *Introduction to moduli problems and orbit spaces*, volume 51 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*. Tata Institute of Fundamental Research, Bombay, 1978.
28. T. Ohno. The graded ring of invariants of ternary quartics I, 2005? unpublished.
29. C. Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In *Algorithmic number theory*, volume 3076 of *Lecture Notes in Comput. Sci.*, pages 379–394. Springer, Berlin, 2004.
30. C. Ritzenthaler. Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves. *LMS J. Comput. Math.*, 13:192–207, 2010.
31. K. Rökaeus. Computer search for curves with many points among abelian covers of genus 2 curves. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 145–150. Amer. Math. Soc., Providence, RI, 2012.
32. T. Satoh. Generating genus two hyperelliptic curves over large characteristic finite fields. In *Advances in Cryptology: EUROCRYPT 2009, Cologne*, volume 5479, Berlin, 2009. Springer.
33. T. Sekiguchi. Wild ramification of moduli spaces for curves or for abelian varieties. *Compositio Math.*, 54:33–372, 1985.
34. J.-P. Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.
35. T. Shioda. Plane quartics and Mordell-Weil lattices of type E_7. *Comment. Math. Univ. St. Paul.*, 42(1):61–79, 1993.
36. J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
37. Y. Varshavsky. On the characterization of complex Shimura varieties. *Selecta Math. (N.S.)*, 8(2):283–314, 2002.
38. A. Vermeulen. *Weierstrass points of weight two on curves of genus three*. PhD thesis, university of Amsterdam, Amsterdam, 1983.
39. H. Weber. Theory of abelian functions of genus 3. (Theorie der Abel'schen Functionen vom Geschlecht 3.), 1876.
40. A. Weil. The field of definition of a variety. *American Journal of Mathematics*, 78:509–524, 1956.

Appendix A. *Generators and normalizers*

As mentioned in Remark 3.2, the automorphism groups in Theorem 3.1 have the property that their isomorphism class determines their conjugacy class in $\mathrm{PGL}_3(K)$. Accordingly, the families of curves in Theorem 3.1 have been chosen in such a way that they allow a common automorphism group as subgroup of $\mathrm{PGL}_3(K)$. We proceed to describe the generators and normalizers of these subgroups, that can be computed directly or by using [**19**, Lem.2.3.8].

In what follows, we consider $\mathrm{GL}_2(K)$ as a subgroup of $\mathrm{PGL}_3(K)$ via the map $A \mapsto \left[\begin{smallmatrix} 1 & 0 \\ 0 & A \end{smallmatrix}\right]$. The group $D(K)$ is the group of diagonal matrices in $\mathrm{PGL}_3(K)$, and $T(K)$ is its subgroup consisting of those matrices in $D(K)$ that are non-trivial only in the upper left corner. We consider $\mathbf{S}_3$ as a subgroup $\widetilde{\mathbf{S}}_3$ of $\mathrm{GL}_3(K)$ by the permutation action that it induces on the coordinate functions, and we denote by $\widetilde{\mathbf{S}}_4$ the degree 2 lift of $\mathbf{S}_4$ to $\mathrm{GL}_3(K)$ generated by the

matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \zeta_8 & 0 \\ 0 & 0 & \zeta_8^{-1} \end{bmatrix}, \quad \frac{-1}{i+1}\begin{bmatrix} 1 & 0 & 0 \\ 0 & i & -i \\ 0 & 1 & 1 \end{bmatrix}.$$

THEOREM A.1. *The following are generators for the automorphism groups G in Theorem 3.1, along with the isomorphism classes and generators of their normalizers N in* $\mathrm{PGL}_3(K)$.

(i) $\{1\}$ *is generated by the unit element.* $N = \mathrm{PGL}_3(K)$.
(ii) $\mathbf{C}_2 = \langle\alpha\rangle$, *where* $\alpha(x,y,z) = (-x,y,z)$. $N = \mathrm{GL}_2(K)$.
(iii) $\mathbf{D}_4 = \langle\alpha,\beta\rangle$, *where* $\alpha(x,y,z) = (-x,y,z)$ *and* $\beta(x,y,z) = (x,-y,z)$. $N = D(K)\widetilde{\mathbf{S}}_3$.
(iv) $\mathbf{C}_3 = \langle\alpha\rangle$, *where* $\alpha(x,y,z) = (\zeta_3 x,y,z)$. $N = \mathrm{GL}_2(K)$.
(v) $\mathbf{D}_8 = \langle\alpha,\beta\rangle$, *where* $\alpha(x,y,z) = (x,\zeta_4 y,\zeta_4^{-1}z)$ *and* $\beta(x,y,z) = (x,z,y)$. $N = T(K)\widetilde{\mathbf{S}}_4$.
(vi) $\mathbf{S}_3 = \langle\alpha,\beta\rangle$, *where* $\alpha(x,y,z) = (x,\zeta_3 y,\zeta_3^{-1}z)$ *and* $\beta(x,y,z) = (x,z,y)$. $N = T(K)\widetilde{\mathbf{S}}_3$.
(vii) $\mathbf{C}_6 = \langle\alpha\rangle$, *where* $\alpha(x,y,z) = (\zeta_3 x,-y,z)$. $N = D(K)$.
(viii) $\mathbf{G}_{16} = \langle\alpha,\beta,\gamma\rangle$, *where* $\alpha(x,y,z) = (\zeta_4 x,y,z)$, $\beta(x,y,z) = (x,-y,z)$, *and* $\gamma(x,y,z) = (x,z,y)$. $N = T(K)\widetilde{\mathbf{S}}_4$.
(ix) $\mathbf{S}_4 = \langle\alpha,\beta,\gamma\rangle$, *where* $\alpha(x,y,z) = (\zeta_4 x,y,z)$, $\beta(x,y,z) = (x,\zeta_3 y,z)$, *and* $\gamma(x,y,z) = (x,y+2z,y-z)$. N *is* $\mathrm{PGL}_3(K)$*-conjugate to* $N = T(K)\widetilde{\mathbf{S}}_4$.
(x) $\mathbf{C}_9 = \langle\alpha\rangle$, *where* $\alpha(x,y,z) = (\zeta_9 x,\zeta_9^3 y,\zeta_9^{-3}z)$. $N = D(K)$.
(xi) $\mathbf{G}_{48} = \langle\alpha,\beta,\gamma,\delta\rangle$, *where* $\alpha(x,y,z) = (-x,y,z)$, $\beta(x,y,z) = (x,-y,z)$, $\gamma(x,y,z) = (y,z,x)$, *and* $\delta(x,y,z) = (y,x,z)$. $N = G$.
(xii) $\mathbf{G}_{96} = \langle\alpha,\beta,\gamma,\delta\rangle$, *where* $\alpha(x,y,z) = (\zeta_4 x,y,z)$, $\beta(x,y,z) = (x,\zeta_4 y,z)$, $\gamma(x,y,z) = (y,z,x)$, *and* $\delta(x,y,z) = (y,x,z)$. $N = G$.
(xiii) $\mathbf{G}_{168} = \langle\alpha,\beta,\gamma\rangle$, *where* $\alpha(x,y,z) = (\zeta_7 x,\zeta_7^2 y,\zeta_7^4 z)$, $\beta(x,y,z) = (y,z,x)$, *and*

$$\begin{aligned}\gamma(x,y,z) = ((&\zeta_7^4-\zeta_7^3)x + (\zeta_7^2-\zeta_7^5)y + (\zeta_7-\zeta_7^6)z,\\ &(\zeta_7^2-\zeta_7^5)x + (\zeta_7-\zeta_7^6)y + (\zeta_7^4-\zeta_7^3)z,\\ &(\zeta_7-\zeta_7^6)x + (\zeta_7^4-\zeta_7^3)y + (\zeta_7^2-\zeta_7^5)z).\end{aligned}$$

$N = G$.

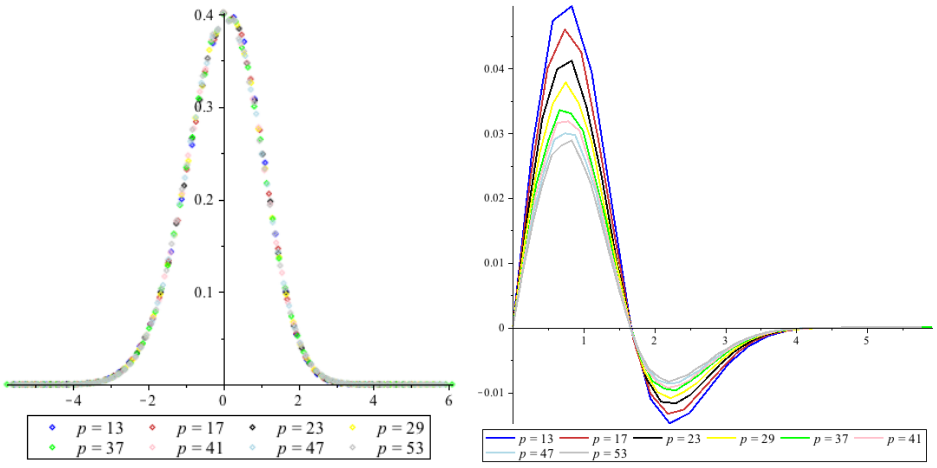
For lack of space, we do not give the mutual automorphism inclusions or the degenerations between the strata. Most of these can be found in [**25**].

Appendix B. *Numerical results*

Given a prime number p, we let $N_{p,3}(t)$ denote the number of $\mathbb{F}_p$-isomorphism classes of non-hyperelliptic curves of genus 3 over $\mathbb{F}_p$ whose trace equals t. Define

$$N_{p,3}^{\mathrm{KS}}(\tau) = \frac{\sqrt{p}}{\#\mathsf{M}_3(\mathbb{F}_p)} \cdot N_{p,3}(t), \quad t = \lfloor\sqrt{p}\cdot\tau\rfloor, \quad \tau \in [-6,6]$$

which is the normalization of the distribution of the trace as in [**21**]. Our numerical results are summarized on Fig. B.1.



(a) Graph of $N_{p,3}^{\mathrm{KS}}(\tau)$ (b) Graph of $N_{p,3}^{\mathrm{KS}}(\tau) - N_{p,3}^{\mathrm{KS}}(-\tau)$

Figure B.1: Trace distribution

Reynald Lercier

DGA MI,
La Roche Marguerite,
35174 Bruz

Institut de recherche mathématique,
Université de Rennes 1,
Campus de Beaulieu,
35042 Rennes

France.

reynald.lercier@m4x.org

Christophe Ritzenthaler

Institut de recherche mathématique,
Université de Rennes 1,
Campus de Beaulieu,
35042 Rennes

France.

christophe.ritzenthaler@univ-rennes1.fr

Florent Rovetta

Institut de Mathématiques de Luminy,
UMR 6206 du CNRS,
Luminy, Case 907,
13288 Marseille

France

florent.rovetta@univ-amu.fr

Jeroen Sijsling

Mathematics Institute,
Zeeman Building,
University of Warwick,
Coventry CV4 7AL

United Kingdom

sijsling@gmail.com

Appendice D

L'article sur ladistribution des traces de frobenius pour les quartiques plane lisse sur les corps finis

DISTRIBUTIONS OF TRACES OF FROBENIUS FOR SMOOTH PLANE CURVES OVER FINITE FIELDS

REYNALD LERCIER, CHRISTOPHE RITZENTHALER, FLORENT ROVETTA, JEROEN SIJSLING, AND BEN SMITH

Abstract. Extrapolating from the results on the distribution of traces of Frobenius for plane curves over a finite field $\mathbb{F}_q$ of large degree compared to q, we give a heuristic explanation for the shape of the graphs observed in [21].

1. Introduction

More than 30 years ago, Serre found closed formulae for the maximal number of rational points on a curve over a finite field $\mathbb{F}_q$ whose genus g is at most 2. In the same article [28] the problem of obtaining a similar formula for curve of genus 3 was considered. This problem is more involved, as was indeed noted by Serre at the time. The main obstruction to obtaining a close formula is the fact that a principally polarized abelian threefold over $\mathbb{F}_q$ that after base extension to $\bar{\mathbb{F}}_q$ becomes a Jacobian of a genus 3 curve need not itself be a Jacobian of such a curve over $\mathbb{F}_q$. The analogue of this statement is satisfied for curves of genus at most 2 because all such curves are hyperelliptic; it ceases to hold in genus 3 because of the presence of non-hyperelliptic curves, for which an obstruction to this descent exists.

There have been many computational and conceptual approaches to the descent obstruction above (which we shall call the *Serre obstruction*). Partial results can be found in [14, 20, 22, 27, 23, 24], while data for small fields can be found at `manypoints.org`. More general approaches were considered in [2, 18, 19]. However, so far none of these can be used to give a closed formula in the sense of [28].

More precisely, the issue is as follows. The number of rational points on a given curve C of genus g over a finite field q is given by

$$\#C(\mathbb{F}_q) = q + 1 - t,$$

where t is the trace of Frobenius acting on the first étale cohomology group $H^1(J_{\text{ét}}, \mathbb{Z}_\ell)$ associated to the Jacobian J of C for some ℓ coprime with q. The classical Hasse–Weil–Serre bound shows that the absolute value of t is bounded by $2g\sqrt{q}$, so the usual strategy is to construct a principally polarized abelian variety A over $\mathbb{F}_q$ with a trace t closed to $-2g\sqrt{q}$ to approach $q + 1 + 2g\sqrt{q}$ rational points as closely as possible. But Serre obstruction amounts to the fact that A is not necessarily the Jacobian of a curve C over $\mathbb{F}_q$. In this case, the quadratic twist of A will be but this quadratic twist changes the trace of Frobenius from t to $-t$, so that C will have few instead of many points.

The present article was motivated by a hope that a new inroad to the problem could be found not so much by studying all descent problems for individual abelian varieties, but rather by an indirect method, namely by proving that for large negative values of t there are more curves with trace t than with trace $-t$. More precisely, define $\mathcal{N}_{q,3}(t)$ to be the number of non-hyperelliptic genus 3 curves over $\mathbb{F}_q$ whose trace of Frobenius equals t. We are then interested in studying the difference

$$\mathcal{V}_{q,3}(t) = \mathcal{N}_{q,3}(t) - \mathcal{N}_{q,3}(-t) \tag{1.1}$$

Date: August 21, 2015.

2010 *Mathematics Subject Classification.* 14Q05 ; 14H10 ; 14H25 ; 14H37; ; 14H45 ; 14H50.

Key words and phrases. Genus 3 curves ; plane quartics ; moduli ; families ; enumeration ; finite fields.

The authors acknowledge support by grant ANR-09-BLAN-0020-01.

for $0 \leq t \leq 6\sqrt{q}$, and more specifically in proving that $\mathcal{V}_{q,3}(t) \leq 0$ for t large enough. Using [20], this would show that there always exists a curve C such that $\#C(\mathbb{F}_q) \geq q+1+3\lfloor 2\sqrt{q} \rfloor - 3$ (actually the precise maximal value could also be given, see [26, Prop.4.1.7]).

An enumerative approach to studying the function (1.1) was given in [21] for prime fields $\mathbb{F}_q$ with $11 \leq q \leq 53$. Over these fields, it was possible to construct all smooth non-hyperelliptic curves of genus 3, that is, all smooth plane quartics, up to isomorphism. The resulting functions $\mathcal{V}_{q,3}(t)$ had some remarkable properties; for $t > 1.7 \cdot \sqrt{q}$ it always appeared that $\mathcal{V}_{q,3}(t)$ was negative, so that the corresponding number of curves with many points was larger than that of the curves with few points. Our original hope that motivated this study turned out to be false in general, as was noted in [21]. Nevertheless, for all q the data obtained fitted a rather simple and pleasing graph, and moreover these graphs almost coincided after normalizing by an explicit power of q.

This phenomenon seemed interesting enough to merit further investigation. Moreover, it fits into a larger framework on results on the distribution of the number of rational points on curves over finite fields, as studied in [17, 6, 33, 7, 34, 9, 35, 8, 11] and especially [5]. The results by Bucur–David–Feigon–Lalín in *loc. cit.* show that the number of rationals points on plane curves of degree d over $\mathbb{F}_q$ is distributed according to an explicit and intuitive binomial law as long as d is large enough compared to q. We study this binomial law in Section 2, or rather the normalized variation of this law around its mean. By the central limit theorem, this variation converges to 0; however, we show that after multiplying by a factor $\sqrt{q}$ its behavior as q tends to infinity can be approximated by the function

$$\psi : x \mapsto \frac{1}{3\sqrt{2\pi}} x(3-x^2)e^{-x^2/2}.$$

In Section 3, we study the variation around the mean of the distribution of the number of rational points on plane curves (and on plane smooth curves) of degree d over $\mathbb{F}_q$ when $q \to \infty$. The results of [5] imply that this quantity (after normalization) fits on the graph of the function ψ when the degree d is sufficiently large with respect to q, as is shown in Corollary 3.5 and Proposition 3.7. Along the way, we use elementary techniques to show in Corollary 3.4 that the bound $d \geq q^2+q$ in [5, Prop.1.6] can be improved to $d \geq 2q-1$. We also note that in these cases (i.e when d is large compared to q); the fact that there are more curves with large negative trace t than with trace $-t$ basically comes down to the fact that a curve with large trace $-t > 0$ would have a negative number of points. So, our approach does not lead to new insights on this problem for large d neither.

In contrast with the approach above, we rather fix the particular small value $d = 4$, whereas we still want to let the cardinality q tend to ∞. Here it remains a challenge to prove any exact results but the comparisons with our experiences in [21] remain bluffing as illustrated in Section 4. Is it simply an illusion do to the fact that q is "small" in our experiments? We could also compare our results to those in [1], where it is conjectured that the distribution of the fraction of curves of genus g over a fixed finite field $\mathbb{F}_q$ whose number of points equals n tends to a Poisson distribution as g tends to infinity. More precisely, it is suggested as one runs over a set of curves over $\mathbb{F}_q$ that represent the $\mathbb{F}_q$-rational points of the moduli stack of curves M_g, one should have the following limit behavior:

$$\lim_{g\to\infty} \{\#C(\mathbb{F}_q) = n : C \in \mathsf{M}_g(\mathbf{F}_q)\} = \frac{\lambda^n e^{-\lambda}}{n!}$$

where $\lambda = q+1+\frac{1}{q-1}$. The same arguments as in the proof of Lem. 2.3 show that the variation around the mean gives rise to the same distribution that we obtain in our paper.

Acknowledgments. We are very grateful to Mohamed Barakat for helping us to find a neat proof of Proposition 3.2, and to Everett Howe for email exchanges which led us to the heuristic interpretation described in this article. We also want to thank Atilla Yilmaz for pointing out the link between our statistical result and Edgeworth series and Maasaki Homma for his short proof of Proposition 3.2.

2. Some remarks on the binomial distribution

We start this paper by analyzing the limit of certain sums of Bernoulli random variables, as well as the limit behavior of the resulting distributions around their mean, which seems to be less well-known. For each positive integer q, let us define q^2 independent and identically distributed (i.i.d.) Bernoulli random variables $B_{q,1}, \ldots, B_{q,q^2}$ that assume the value 1 with probability $1/q$ (and the value 0 with probability $1 - 1/q$). Then the sum $S_q = \sum_{i=1}^{q^2} B_{q,i}$ is described by the binomial probability mass function

$$b_q(m) := \mathrm{Prob}(S_q = m) = \binom{q^2}{m} \left(\frac{1}{q}\right)^m \left(1 - \frac{1}{q}\right)^{q^2-m}. \tag{2.1}$$

The mean M of the random variable S_q equals q, whereas its standard deviation σ equals $\sqrt{q^2(1/q)(1-1/q)} = \sqrt{q-1}$. As such, if we define the normalized average Y_q by

$$Y_q = \frac{S_q - M}{\sigma} \tag{2.2}$$

then the triangular central limit theorem [4, Th.27.3] shows that the sequence Y_q converges in law to the standard normal distribution, i.e. the cumulative distribution law of the random variable Y_q converges to the integral of the Gaussian density $\varphi : x \mapsto \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2}$.

This can also be deduced from the De Moivre-Laplace theorem [4, Ex.25.11] which claims that for any sequence of integers $(m_q)_q$ and x a real number such that $\frac{m_q - M}{\sigma}$ tends to x as q tends to infinity one has

$$\lim_{q\to\infty} \sigma \,\mathrm{Prob}(S_q = m_q) = \varphi(x). \tag{2.3}$$

We see that $Y_q(x) - Y_q(-x)$ tends to 0 when q tends to infinity. In order to study this more precisely, we will consider the expression $v_q(x) = \sigma \cdot (b_q(M - \sigma x) - b_q(M + \sigma x))$. We could equally well study the difference $v_q(-x)$ instead; our reasons for putting $b_q(M - \sigma x)$ first are related to the formula $q+1-t$ for the number of points on a curve over a finite field $\mathbb{F}_q$. Note that when $\sigma x > M$ we have $b_q(M - \sigma x) = 0$, which forces $v_q(x) \leq 0$. Intuitively, one could guess that $v_q(x) \geq 0$ for small x to compensate this defect. This will turn out to be true, and a careful analysis of this phenomenon is given below.

Before embarking on this, we will allow the parameters on which the random variables depend to be more general than the setting above, since this will be relevant for our applications in the next sections. We let N_q be a sequence of positive natural numbers whose asymptotic behavior is described by

$$N_q = q^2 + O(q). \tag{2.4}$$

Given q, we construct N_q i.i.d. Bernoulli random variables that assume the value 1 with the probability $\mu_q \sim \frac{1}{q}$ (and the value 0 with the probability $\nu = 1 - \mu$). We let b_q be the corresponding binomial mass function and we defined σ_q to be the standard deviation of b_q. Explicitly, we have

$$\sigma_q = \sqrt{N_q \mu_q (1 - \mu_q)} \sim \sqrt{q}. \tag{2.5}$$

We let $X_q : I_q \to \mathbb{R}$ be a real function from an interval I_q. Informally we think of X as a variable that corresponds with the normalized variation of the binomial mass function b_q above around its mean. We need one more bit of notation in order to deal with approximations in both q and x:

Definition 2.1. Let $f_q(x)$ and $g_q(x)$ be function of $x \in I_q$. We write $f_q = o(g_q)$ if for all $\epsilon > 0$ there exists a q_0 such that

$$\forall q > q_0 : \forall x \in I_q : |f_q(x)| \leq \epsilon |g_q(x)|. \tag{2.6}$$

The notation $f(q, x) = O(g(q, x))$ is defined similarly.

For $\alpha > 0$ any fixed real we define $I_q = [-\left(\sqrt{q}\right)^{1-\alpha}, \left(\sqrt{q}\right)^{1-\alpha}]$. We assume that our functions $X_q : I_q \to \mathbb{R}$ satisfy for all q

$$X_q(x) - x = o\left(\frac{1}{q}\right). \tag{2.7}$$

Example 2.2. With these notation, the example at the beginning of the section has the following parameters

$$N_q = q^2, \quad \mu_q = \frac{1}{q}, \quad \sigma_q = \sqrt{q-1}, \quad X_q = x.$$

In Corollary 3.5, we will need

$$N_q = q^2 + q + 1, \quad \mu_q = \frac{1}{q}, \sigma_q = \sqrt{q - 1/q^2}$$

and

$$X = -\frac{1}{q\sqrt{q}} + \sqrt{1 - \frac{1}{q^3}}x.$$

Finally in Proposition 3.7, we will need

$$N_q = q^2 + q + 1, \quad \mu_q = \frac{q+1}{q^2+q+1}, \quad \sigma = \sqrt{q(1 - \frac{q}{q^2+q+1})}$$

and

$$X = \sqrt{1 - \frac{q}{q^2+q+1}}x.$$

We define

$$m(q, x) = N(q)\mu(q) - \sigma(q)X(q, x) \tag{2.8}$$
$$n(q, x) = N(q)\nu(q) + \sigma(q)x = N(q) - m(q, x). \tag{2.9}$$

Then if q is large enough, we can define the continuous function

$$b(q, x) = \frac{\Gamma(N(q) + 1)}{\Gamma(n(q, x) + 1)\Gamma(m(q, x) + 1)}\mu(q)^{m(q,x)}\nu(q)^{n(q,x)}. \tag{2.10}$$

Note that if $m(q, x)$ happens to be integral, then we have

$$b(q, x) = b_q(m(q, x)) \tag{2.11}$$

for the binomial mass function b_q defined above. As such, $b(q, x)$ should be thought of as the collection of continuous interpolations of these values, with this difference that we have shifted to using the normalized parameter x instead of m.

Lemma 2.3. *With the notation above, we have for $x \in I_q$ the approximation*

$$\sigma \cdot (b(q, x) - b(q, -x)) = \left(\frac{1}{3\sqrt{2\pi}}x(3 - x^2)e^{-\frac{x^2}{2}}\right)\frac{1}{\sqrt{q}} + o\left(\frac{1}{\sqrt{q}}\right). \tag{2.12}$$

As the proof is a bit long and technical, we postpone it to Section 5.

Remark 2.4. The error terms in the central limit theorem is of course a well-studied question and we found in the literature powerful tools to deal with it. In particular Edgeworth series seemed to be well suited for our problem since formally they give the same answer with a larger interval for the variable x. It also shows that the polynomial $x(3 - x^2)$ which appears is simply the opposite of the third Hermite polynomial [16, Sec.3.4]. Unfortunately, after asking several statisticians, it seems that we cannot fulfill the hypotheses of any theorems on Edgeworth series we could find in the literature and this is why we addressed the problem in an elementary way.

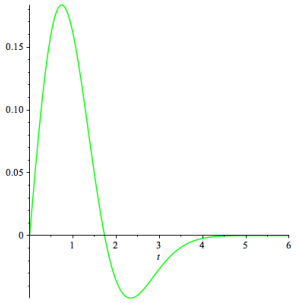


FIGURE 1. The graph of the approximation $\psi : x \mapsto \frac{1}{3\sqrt{2\pi}} x(x^2-3)e^{-x^2/2}$.

3. Relation with the number of points on plane curves over finite fields.

The relation between the considerations in the previous section and the distribution of traces of Frobenius on plane curves over finite fields $\mathbb{F}_q$ of characteristic p was first described in [5]. Let C be a curve defined by a homogeneous polynomial $f \in \mathbb{F}_q[x,y,z]$. Then intuitively the probability for a given point $P \in \mathbb{P}^2(\mathbb{F}_q)$ to be on C should equal $1/q$, since *a priori* the set of possible values for f at P has q elements. Supposing furthermore that the probability are independent as P varies, we essentially find ourselves in the situation of Section 2.

More precisely, let $R = \mathbb{F}_q[x,y,z]$ be the homogeneous coordinate ring of $\mathbb{P}^2_{\mathbb{F}_q}$, and let $f \in R_d(\mathbb{F}_q)$ be a homogeneous polynomial of degree d with coefficients in $\mathbb{F}_q$. Let C_f be the curve in $\mathbb{P}^2$ defined by f. Then a seminal result by Bucur–David–Feigon–Lalín [5] shows that the intuition about independence above is accurate if d is large enough with respect to q, in the following sense:

Proposition 3.1 ([5, Prop.1.6])**.** *Let $B_1, \dots, B_{q^2+q+1}$ be i.i.d. Bernoulli random variables that assume the value 1 with probability $1/q$. Then if $d \geq q^2+q$ we have*

$$\frac{\#\{f \in R_d, \#C_f(\mathbb{F}_q) = n\}}{\#R_d} = \mathrm{Prob}(B_1 + \ldots + B_{q^2+q+1} = n). \tag{3.1}$$

In turn, Proposition 3.1 is based on a general result of Poonen [25] but one can rederive this result by elementary means, while improving the bound on d in the meantime.

We choose an enumeration $P_1, \dots, P_{q^2+q+1}$ of the set $\mathbb{P}^2(\mathbb{F}_q)$, which we in turn lift to $\mathbb{F}_q$-rational affine representatives $\tilde{P}_1, \dots, \tilde{P}_{q^2+q+1}$ in $\mathbb{A}^3(\mathbb{F}_q)$. This allows us to construct the linear map

$$\begin{aligned} \psi : R_d(\mathbb{F}_q) &\to \mathbb{F}_q^{q^2+q+1} \\ f &\mapsto (f(\tilde{P}_1), \dots, f(\tilde{P}_{q^2+q+1})) \end{aligned} \tag{3.2}$$

The kernel of ψ defines those plane curves that go through all rational points of the projective plane, which are called *plane filling curves*. It is known (see [30, 31] and [13, Prop.2.1]) that the kernel of ψ is $R_d(\mathbb{F}_q) \cap J$ where J is the ideal generated by $x^q y - y^q x$, $y^q z - z^q y$ and $z^q x - x^q z$. The following proof is due to Maasaki Homma (see also his forthcoming article [12]).

Proposition 3.2. *For $d \geq 2q-1$ the map φ is surjective.*

Proof. For any $d \geq 2q-1$, let us consider the polynomial $x^{d-(2q-2)}(y^{q-1}-x^{q-1})(z^{q-1}-x^{q-1})$. This degree d polynomial takes non-zero value at $(1:0:0)$ and 0 at any other $\mathbb{F}_q$-rational point of the plane. Using the transitive action of $\mathrm{PGL}_3(\mathbb{F}_q)$, we see that we can construct degree d polynomials having the same properties for any rational point of the plane. Therefore the evaluation map φ is surjective. □

Remark 3.3. Let M be the module R/J over the homogeneous coordinate ring R. Note that M corresponds to the dimension 0 reduced closed subscheme of $\mathbb{P}^2_{\mathbb{F}_q}$ whose geometric points coincide with the set of rational points $\mathbb{P}^2(\mathbb{F}_q)$. The previous proposition also follows from the fact that M admits the free resolution

$$0 \longrightarrow R(-q-2) \oplus R(-2q-1) \xrightarrow{\varphi_2} R(-q-1) \oplus R(-q-1) \oplus R(-q-1) \xrightarrow{\varphi_1} R \xrightarrow{\varphi_0} M \longrightarrow 0. \tag{3.3}$$

Here φ_0 is the quotient map, φ_1 sends the canonical basis of $R(-q-1)\oplus R(-q-1)\oplus R(-q-1)$ to the elements $x^qy-y^qx, y^qz-z^qy, z^qx-x^qz$ of R, and φ_2 sends the canonical basis of $R(-q-2)\oplus R(-2q-1)$ to the elements (z,x,y) and (z^q,x^q,y^q) of $R(-q-1)\oplus R(-q-1)\oplus R(-q-1)$. This can be proved using the theory of Gröbner basis as described in [10, Ch.15].
Note, however, that Maasaki's proof is much faster and can easily be generalized to polynomials in $n+1$ variables of degree greater than $(q-1)n+1$.

Corollary 3.4. *Proposition 3.1 holds for $d \geq 2q-1$.*

Proof. Proposition 3.2 shows that under the given hypothesis on d we can always find a homogeneous polynomial with a prescribed zero set of cardinality n and given non-zero values at the complement. Hence, the cardinality of the set of such polynomials is the order of the kernel of ψ and does not depend on the prescribed zero set. This implies that the proportion of polynomials with a zero set of cardinality n follows a binomial distribution $\mathrm{Prob}(B_1+\ldots+B_{q^2+q+1}=n)$. □

For a (possibly singular) plane curve $C: f(x,y,z)=0$, we let $t=q+1-\#C(\mathbb{F}_q)$, and we define the *(normalized) trace* $x=t/\sqrt{q}$, in analogy with Section 2. Note that x is not bounded when $q\to\infty$. Let

$$N_{q,d}(x)=\sqrt{q}\frac{\#\{f\in R_d, \#C_f(\mathbb{F}_q)=q+1-\sqrt{q}x\}}{\#R_d} \tag{3.4}$$

and

$$V_{q,d}(x)=N_{q,d}(x)-N_{q,d}(-x). \tag{3.5}$$

Using Corollary 3.4 and Lemma 2.3 with $N=q^2+q+1$ (so $\alpha=1$), $n=q+1-\sqrt{q}x$ and $\epsilon=\frac{1}{q}$, we get

Corollary 3.5. *For $d\geq 2q-1$, any $\alpha>0$ and $x\in[-(\sqrt{q})^{1-\alpha},(\sqrt{q})^{1-\alpha}]$, we get the following approximation of $V_{q,d}(x)$ in the sense of Lemma 2.3*

$$V_{q,d}(x)=\left(\frac{1}{3\sqrt{2\pi}}x(3-x^2)\cdot e^{-x^2/2}\right)\frac{1}{\sqrt{q}}+o\left(\frac{1}{\sqrt{q}}\right). \tag{3.6}$$

We now restrict our considerations to only non-singular plane curves. Let $R_d^{\mathrm{ns}}\subset R_d$ be the subset of homogeneous polynomials corresponding to non-singular plane curves. The genus of these curves will then equal $g=(d+1)(d+2)/2$. Having restricted our considerations to a subset of the set of curves defined by the non-vanishing of the rather complicated discriminant form, the sieving process to get the distribution is correspondingly more involved.

Theorem 3.6 ([5, Th.1.1])**.** *Let $B_1,\ldots,B_{q^2+q+1}$ be i.i.d. Bernoulli random variables that take the value 1 with probability $(q+1)/(q^2+q+1)$. Then if $0\leq n\leq q^2+q+1$ we have*

$$\begin{aligned}\frac{\#\{f\in R_d^{ns}, \#C_f(\mathbb{F}_q)=n\}}{\#R_d^{ns}} &= \mathrm{Prob}(B_1+\ldots+B_{q^2+q+1}=n)\\ &\quad\left(1+O\left(q^n\left(d^{-1/3}+(d-1)^2q^{-\min(\lfloor\frac{d}{p}\rfloor+1,\frac{d}{3})}+dq^{-\lfloor\frac{d-1}{p}\rfloor-1}\right)\right)\right)\end{aligned}$$

As before, we let

$$N_{q,d}^{\mathrm{ns}}(x)=\sqrt{q}\frac{\#\{f\in R_d^{\mathrm{ns}}, \#C_f(\mathbb{F}_q)=q+1-\sqrt{q}x\}}{\#R_d^{\mathrm{ns}}} \tag{3.7}$$

and

$$V_{q,d}^{\mathrm{ns}}(x)=N_{q,d}^{\mathrm{ns}}(x)-N_{q,d}^{\mathrm{ns}}(-x). \tag{3.8}$$

When $d\geq q^{6q+3}$, the $O()$ term is negligible with respect to $o(q^{-1/2})$. Using this result and Lemma 2.3 with $N=q^2+q+1$, $n=q+1-\sqrt{n}x$ and $\epsilon=\frac{q+1}{q^2+q+1}=\frac{1}{q}+O\left(\frac{1}{q}\right)$ we hence get

Proposition 3.7. *For $d\geq q^{6q+3}$, any $\alpha>0$ and $x\in[-(\sqrt{q})^{1-\alpha},(\sqrt{q})^{1-\alpha}]$, we get the following approximation of $V_{q,d}^{ns}(x)$ in the sense of Lemma 2.3*

$$V_{q,d}^{ns}(x)=\left(\frac{1}{3\sqrt{2\pi}}x(3-x^2)\cdot e^{-x^2/2}\right)\frac{1}{\sqrt{q}}+o\left(\frac{1}{\sqrt{q}}\right). \tag{3.9}$$

4. Experimental results and their limitations

In this section we consider the case $d = 4$. The smooth plane quartic curves X_f described by $f \in R_4^{\mathrm{ns}}(\mathbb{F}_p)$ are then exactly the non-hyperelliptic curves of genus 3 over $\mathbb{F}_p$. Since now d is fixed and q tends to ∞, our previous results cannot be directly applied. However, as we mentioned in the introduction, we wish to compare the statistical distributions obtained in this way with the experimental results obtained in [21].

In order to do so, let $\mathcal{N}_{q,3}(t)$ denote the number of $\mathbb{F}_q$-isomorphism classes of non-hyperelliptic curves of genus 3 over $\mathbb{F}_q$ whose trace equals t. As in [3, 32], the most natural way to define $\mathcal{N}_{q,3}(t)$ by weighting the isomorphism classes involved by the order of their automorphism group over the ground field $\mathbb{F}_q$, in other words, by

$$\mathcal{N}_{q,3}(t) = \sum_{\substack{\{C/\mathbb{F}_q \text{ n.h. genus 3} \\ \text{curve with trace } t\}/\simeq}} \frac{1}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)}. \tag{4.1}$$

Indeed, with this definition, we have the following Lemma.

Lemma 4.1. *We have*

$$\#\operatorname{GL}_3(\mathbb{F}_q) \cdot \mathcal{N}_{q,3}(t) = \#\{f \in R_d^{ns}, \#X_f(\mathbb{F}_q) = q + 1 - t\}. \tag{4.2}$$

Proof. As smooth plane quartics can be identified with their own canonical embedding, an $\mathbb{F}_q$-rational isomorphism between two quartics is induced by an element of $\operatorname{PGL}_3(\mathbb{F}_q)$. Since on the other hand two ternary forms define the same subvariety of $\mathbb{P}^2$ if and only if they differ by scalar multiplication by an element of $\mathbb{F}_q^\times$, we have

$$\begin{aligned} \#\{f \in R_d^{\mathrm{ns}}, \#X_f(\mathbb{F}_q) = q + 1 - t\} &= \#\mathbb{F}_q^\times \sum_{C/\mathbb{F}_q} \frac{\#\operatorname{PGL}_3(\mathbb{F}_q)}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)} \\ &= \#\operatorname{GL}_3(\mathbb{F}_q) \sum_{C/\mathbb{F}_q} \frac{1}{\#\operatorname{Aut}_{\mathbb{F}_q}(C)} \\ &= \#\operatorname{GL}_3(\mathbb{F}_q) \cdot \mathcal{N}_{q,3}(t), \end{aligned} \tag{4.3}$$

where the indices of the sums involved are as in (4.1). □

Define

$$\mathcal{N}_{q,3}^{\mathrm{KS}}(x) = \frac{\sqrt{q}}{q^6+1}\mathcal{N}_{q,3}(t), \quad t = \lfloor \sqrt{p}x \rfloor, \quad x \in [-6, 6], \tag{4.4}$$

This coincides with the normalization of the trace distribution in [15]. We also define

$$\mathcal{V}_{q,3}^{\mathrm{KS}}(x) = \mathcal{N}_{q,3}^{\mathrm{KS}}(x) - \mathcal{N}_{q,3}^{\mathrm{KS}}(-x). \tag{4.5}$$

A graphical summary of our numerical results [21] is given in Figure 2.

Lemma 4.1 shows that Katz–Sarnak's quantity $\mathcal{N}_{q,3}^{\mathrm{KS}}(x)$ defined in (4.4) can be rewritten as

$$\mathcal{N}_{q,3}^{\mathrm{KS}}(x) = \frac{\#R_4^{\mathrm{ns}}}{(q^6+1)\#\operatorname{GL}_3(\mathbb{F}_q)} N_{q,4}^{\mathrm{ns}}(x). \tag{4.6}$$

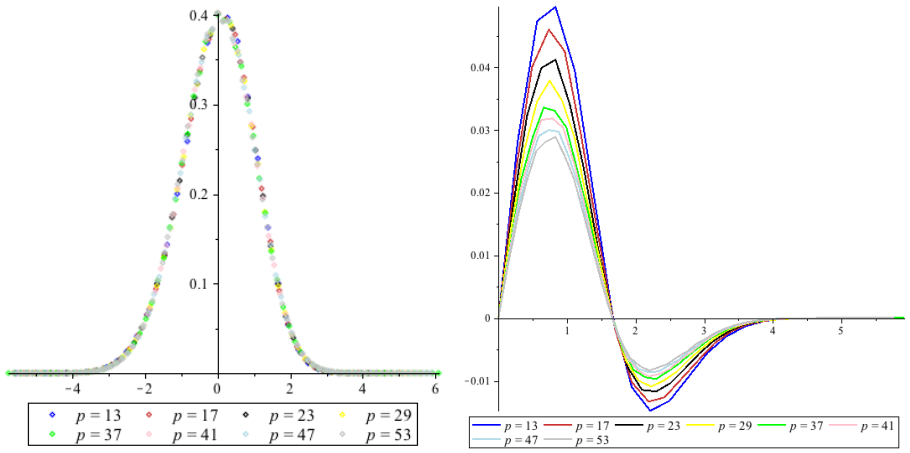
The singular quartics curves in the 14-dimensional space $\mathbb{P}R_4$ are contained in the discriminant locus, which is a hypersurface D of degree 27. By [29, Th.2.1], one has that $\#D(\mathbb{F}_q) \leq 27q^{13} + \frac{q^{13}-1}{q-1}$. Therefore

$$\frac{\#R_4^{\mathrm{ns}}}{(q^6+1)\#\operatorname{GL}_3(\mathbb{F}_q)} = \frac{\#R_4 - (q-1)\#D(\mathbb{F}_q)}{(q^6+1)(q^3-1)(q^3-q)(q^3-q^2)} = 1 + O\left(\frac{1}{q}\right). \tag{4.7}$$

We then have

$$\mathcal{N}_{q,3}^{\mathrm{KS}}(x) = N_{q,4}^{\mathrm{ns}}(x)\left(1 + O\left(\frac{1}{q}\right)\right) = N_{q,4}^{\mathrm{ns}}(x) + O\left(\frac{1}{q}\right) \tag{4.8}$$

since $\mathcal{N}_{q,3}^{\mathrm{KS}}(x)$ (and therefore $N_{q,4}^{\mathrm{ns}}(x)$) is uniformly bounded.



(A) Graph of $\mathcal{N}_{q,3}^{\mathrm{KS}}(x)$ (B) Linear interpolation of $\mathcal{V}_{q,3}^{\mathrm{KS}}(x)$

FIGURE 2. The numerical trace distributions $\mathcal{N}_{q,3}^{\mathrm{KS}}(x)$ and $\mathcal{V}_{q,3}^{\mathrm{KS}}(x)$.

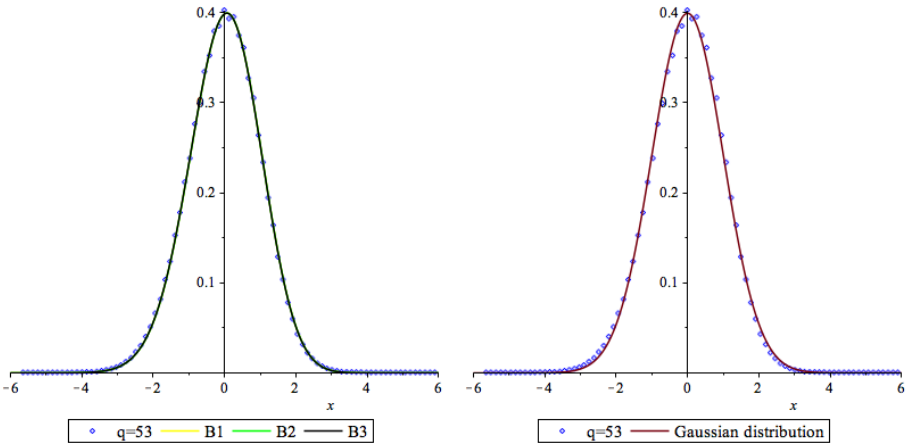
We can now make a graphical comparison of the experimental distribution of $\mathcal{V}_{q,3}^{\mathrm{KS}}$ for the largest value of q (to wit $q = 53$) with the results from Section 3. We define B_1, B_2, B_3 by

$$B_i(x) = \sigma_i \binom{q^2+q+1}{\mu_i - \sigma_i x} \epsilon_i^{\mu_i - \sigma_i x} (1-\epsilon_i)^{q^2+q+1-(\mu_i-\sigma_i x)} \tag{4.9}$$

where

(1) $\mu_1 = q+1+1/q$, $\sigma_1 = \sqrt{q-1/q^2}$ and $\epsilon_1 = 1/q$ (this corresponds to Corollary 3.4, *i.e.*, possibly singular plane quartics);
(2) $\mu_2 = q+1$, $\sigma_2 = \sqrt{q-q/(q^2+q+1)}$ and $\epsilon_1 = (q+1)/(q^2+q+1)$ (this corresponds to Theorem 3.6, *i.e.*, smooth plane quartics);
(3) $\mu_3 = q+1$, $\sigma_3 = \sqrt{q}$ and $\epsilon_1 = 1/q$ (a simplified model).

As Figure 3 shows, the various plots of B_1, B_2, B_3 and the Gaussian density function are almost indistinguable, and all these function interpolate the distribution $\mathcal{N}_{53,3}^{\mathrm{KS}}(x)$ quite well.



(A) $\mathcal{N}_{53,3}^{\mathrm{KS}}(x)$ against B_1, B_2, B_3 (B) $\mathcal{N}_{53,3}^{\mathrm{KS}}(x)$ against the Gaussian curve

FIGURE 3. Comparisons between $\mathcal{N}_{53,3}^{\mathrm{KS}}(x)$ and its approximations.

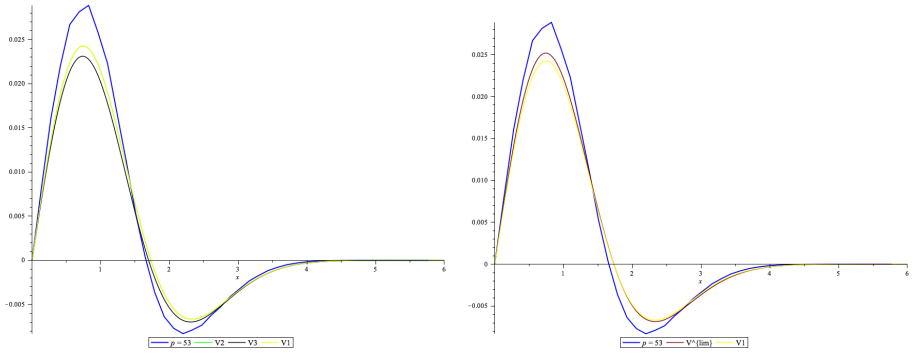
As above, we are led to define

$$V_i(x) = B_i(x) - B_i(-x) \tag{4.10}$$

and

$$V^{\lim}(x) = \left(\frac{1}{3\sqrt{2\pi}} x(3-x^2)e^{-x^2/2}\right) q^{-1/2}. \tag{4.11}$$

This gives rise to the plots in Figure 4. JS: [Do we plot this with the square root factor? Just checkin'] One observes that the various curves resemble the distribution of $\mathcal{V}_{53,3}^{\mathrm{KS}}(x)$ fairly well.



(A) $\mathcal{V}_{53,3}^{\mathrm{KS}}(x)$ against V_1, V_2, V_3 (B) $\mathcal{V}_{53,3}^{\mathrm{KS}}(x)$ against $V_1, V^{\lim}$

FIGURE 4. Comparisons betwee $\mathcal{V}_{53,3}^{\mathrm{KS}}(x)$ and its approximations.

This is quite remarkable, as the limit distribution $V^{\lim}$ does not depend on any parameters and hence cannot be adjusted.

5. Proof of Lemma 2.3

During this proof we drop the arguments of the functions N, μ, ν, m, n and X. Since $X_q - x = o(\frac{1}{q})$, it is easy to check that one can replace X by x in the following expansions. For later use, we also define

$$y = \nu x/\sigma, \tag{5.1}$$

$$z = \mu x/\sigma. \tag{5.2}$$

We use the Stirling approximation of the Gamma function. This is is given by

$$\Gamma(x+1) = \sqrt{2\pi x}\left(\frac{x}{e}\right)^x e^{\theta_x} \tag{5.3}$$

where $|\theta_x| \leq \frac{1}{12x}$. Then

$$b(q,x) = \frac{1}{\sqrt{2\pi}}\sqrt{\frac{N}{mn}}\left(\frac{N\mu}{m}\right)^m\left(\frac{N\nu}{n}\right)^n e^{\theta} \tag{5.4}$$

with $\theta = \theta_N - \theta_m - \theta_n$.

In Claims 1–6 below we approximate the individual factors in (5.4).

Claim 1. $\sqrt{\frac{N}{mn}} = \frac{1}{\sigma}\left(1 + \frac{x}{2\sqrt{q}} + o\left(\frac{x}{\sqrt{q}}\right)\right)$.

First note that

$$\frac{N}{mn} = \frac{1}{\sigma^2}\frac{1}{1+(\mu-\nu)\frac{x}{\sigma} - \frac{x^2}{N}} = O\left(\frac{1}{q}\right) = o\left(\frac{1}{\sqrt{q}}\right) \tag{5.5}$$

Using the Taylor expansion of the monotone function $z \mapsto 1/\sqrt{1+z}$ along with the estimate $\mu - \nu = 1 + o(q^{-1})$, we obtain

$$\sqrt{\frac{N}{mn}} = \frac{1}{\sigma}\frac{1}{\sqrt{1+(\mu-\nu)\frac{x}{\sigma} - \frac{x^2}{N}}} = \frac{1}{\sigma}\left(1 - (\mu-\nu)\frac{x}{2\sigma} + o\left(\frac{x}{\sigma}\right)\right) = \frac{1}{\sigma}\left(1 + \frac{x}{2\sqrt{q}} + o\left(\frac{x}{\sqrt{q}}\right)\right). \tag{5.6}$$

Claim 2. $e^{\theta} = 1 + o\left(\frac{1}{\sqrt{q}}\right)$.

For this, we first estimate θ. We get

$$|\theta| = |\theta_N - \theta_m - \theta_n| \leq \frac{1}{12}\left|\frac{1}{N} + \frac{N}{nm}\right| \tag{5.7}$$

From (2.4) and (5.6) we obtain that $\theta = o(q^{-1/2})$. The claim now follows since

$$\lim_{q\to\infty} \sqrt{q}(e^\theta - 1) = \lim_{q\to\infty} (\sqrt{q}\theta)((e^\theta - 1)/\theta) = \lim_{q\to\infty} (\sqrt{q}\theta) = 0. \tag{5.8}$$

To see this, note that we consider θ as a function of q and that $\lim_{q\to\infty} \theta = 0$.

Claim 3. $A = -\log\left(\frac{N\mu}{m}\right)^m = N\mu\left(-y + \frac{y^2}{2} + \frac{y^3}{6} + o(y^3)\right)$.

Indeed,

$$A = (N\mu - \sigma x)\log\left(\frac{N\mu - \sigma x}{N\mu}\right) = N\mu(1-y)\log(1-y) = N\mu(-y + \frac{y^2}{2} + \frac{y^3}{6} + o(y^3)). \tag{5.9}$$

An analogous computation, in which y is replaced by $-z$, yields

Claim 4. $B = -\log\left(\frac{N\nu}{n}\right)^n = N\nu\left(z + \frac{z^2}{2} - \frac{z^3}{6} + o(z^3)\right)$.

We can now approximate the product of the two middle factors in (5.4). For this we first note the following.

Claim 5. $A + B = \frac{1}{2}x^2 + \frac{x^3}{6\sqrt{q}} + o\left(\frac{x^3}{\sqrt{q}}\right)$.

We combine Claims 2 and 3 with the relations $\sigma^2 = N\mu\nu$ and $\mu^2 - \nu^2 = (\mu - \nu)(\mu + \nu) = \mu - \nu = 1 + o(q^{-1})$ to get

$$\begin{aligned} A + B &= N(-\mu\nu + \mu\nu)\frac{x}{\sigma} + N(\mu\nu^2 + \mu^2\nu) + N(\mu\nu^3 - \mu^3\nu)\frac{x^3}{6\sigma^3} + N\mu o(y^3) + N\nu o(z^3) \\ &= \frac{x^2}{2} + \frac{(\mu^2 - \nu^2)x^3}{6\sigma} + N\mu o(y^3) + N\nu o(z^3) \\ &= \frac{x^2}{2} + \frac{x^3}{6\sqrt{q}} + o\left(\frac{x^3}{\sqrt{q}}\right) + N\mu o(y^3) + N\nu o(z^3). \end{aligned} \tag{5.10}$$

The claim follows since because the asymptotic behavior of N, μ, ν, σ implies that $N\mu o(y^3)$ and $N\nu o(z^3)$ are both $o(x^3 q^{-1/2})$.

Claim 6. $e^{-(A+B)} = e^{-\frac{x^2}{2}}\left(1 - \frac{x^3}{6\sqrt{q}}\right) + o\left(\frac{1}{\sqrt{q}}\right)$. To see this, we first note that taking a first-order Taylor approximation of the monotone function $z \mapsto e^z$ shows that we have

$$e^z = 1 + z + R(z), \tag{5.11}$$

where the remainder term R satisfies $|R(z)| \leq (z^2/2)e^{|z|}$. We apply this to obtain

$$\begin{aligned} e^{-(A+B)} &= e^{-\frac{x^2}{2}} e^{-\frac{x^3}{6\sqrt{q}} + o\left(\frac{x^3}{\sqrt{q}}\right)} \\ &= e^{-\frac{x^2}{2}}\left(1 - \frac{x^3}{6\sqrt{q}} + o\left(\frac{x^3}{\sqrt{q}}\right)\right) + e^{-\frac{x^2}{2}} R\left(\frac{x^3}{6\sqrt{q}} + o\left(\frac{x^3}{6\sqrt{q}}\right)\right). \end{aligned} \tag{5.12}$$

The last term can be estimated by

$$\left|e^{-\frac{x^2}{2}} R\left(\frac{x^3}{6\sqrt{q}} + o\left(\frac{x^3}{6\sqrt{q}}\right)\right)\right| \leq \left|\left(\frac{1}{36q} + o\left(\frac{1}{q}\right)\right) x^6 e^{\left(\left|\frac{x}{6\sqrt{q}} + o\left(\frac{x}{\sqrt{q}}\right)\right| - \frac{1}{2}\right)x^2}\right|. \tag{5.13}$$

Here the assumption on x plays a role. The product of the last factors is bounded as q grows since we assumed that $x = o(q^{1/2})$. So in fact a stronger estimate holds:

$$e^{-\frac{x^2}{2}} R\left(\frac{x^3}{6\sqrt{q}} + o\left(\frac{x^3}{6\sqrt{q}}\right)\right) = o\left(\frac{1}{q}\right) = o\left(\frac{1}{\sqrt{q}}\right). \tag{5.14}$$

Since $x^3 e^{-\frac{x^2}{2}}$ is also bounded, and regardless of any growth assumptions on x at that, we also have

$$e^{-\frac{x^2}{2}}\left(o\left(\frac{x^3}{\sqrt{q}}\right)\right) = o\left(\frac{1}{\sqrt{q}}\right), \tag{5.15}$$

which concludes the proof of Claim 6.

By putting all our estimates together, we obtain a good approximation for $\sigma b(q,x)$ as q tends to infinity:

Claim 7. $\sqrt{2\pi}\sigma b(q,x) = e^{-\frac{x^2}{2}}\left(1+\frac{x}{2\sqrt{q}}-\frac{x^3}{6\sqrt{q}}\right)+o\left(\frac{1}{\sqrt{q}}\right)$. Indeed, since $x=o(q^{1/2})$, we have that $\frac{x}{\sqrt{q}}=o(1)$. Therefore

$$\begin{aligned}\sigma\sqrt{\frac{N}{mn}}e^{\theta} &= \left(1+\frac{x}{2\sqrt{q}}+o\left(\frac{x}{\sqrt{q}}\right)\right)\left(1+o\left(\frac{1}{\sqrt{q}}\right)\right)\\ &= 1+\frac{x}{2\sqrt{q}}+o\left(\frac{x}{\sqrt{q}}\right)+o\left(\frac{1}{\sqrt{q}}\right)\\ &= 1+\frac{x}{2\sqrt{q}}+o\left(\frac{x}{\sqrt{q}}\right).\end{aligned} \tag{5.16}$$

We now consider the product

$$\begin{aligned}\sqrt{2\pi}\sigma b(q,x) &= \left(1+\frac{x}{2\sqrt{q}}+o(\frac{x}{\sqrt{q}})\right)e^{-(A+B)}\\ &= e^{-\frac{x^2}{2}}\left(1+\frac{x}{2\sqrt{q}}+o\left(\frac{x}{\sqrt{q}}\right)\right)\left(1-\frac{x^3}{6\sqrt{q}}+o\left(\frac{1}{\sqrt{q}}\right)\right)\end{aligned} \tag{5.17}$$

Its main contribution is given by

$$e^{-\frac{x^2}{2}}\left(1+\frac{x}{2\sqrt{q}}\right)\left(1-\frac{x^3}{6\sqrt{q}}\right) = e^{-\frac{x^2}{2}}\left(1+\frac{x}{2\sqrt{q}}-\frac{x^3}{6\sqrt{q}}+\frac{x^4}{12q}\right). \tag{5.18}$$

As in the derivation of (5.15), we see that the final term in this sum is $o(q^{-1/2})$. The same technique allows one to conclude that the other cross-terms in the product (5.17) are $o(q^{-1/2})$.

This concludes the proof of Claim 7. After desymmetrizing, we obtain

$$3\sqrt{2\pi}\sigma(b(x,q)-b(-x)) = e^{-\frac{x^2}{2}}(3x-x^3)\frac{1}{\sqrt{q}}+o\left(\frac{1}{\sqrt{q}}\right). \tag{5.19}$$

References

[1] J. D. Achter, D. Erman, K. S. Kedlaya, M. M. Wood, and D. Zureick-Brown. A heuristic for the distribution of point counts for random curves over a finite field. *Phil. Trans. R. Soc. A*, 373(2040), 2015.

[2] A. Beauville and C. Ritzenthaler. Jacobians among abelian threefolds: a geometric approach. *Math. Annal.*, 350(4):793–799, 2011.

[3] K. A. Behrend. The Lefschetz trace formula for algebraic stacks. *Invent. Math.*, 112(1):127–149, 1993.

[4] P. Billingsley. *Probability and measure*. Wiley Series in Probability and Mathematical Statistics. John Wiley & Sons, Inc., New York, third edition, 1995. A Wiley-Interscience Publication.

[5] A. Bucur, C. David, B. Feigon, and M. Lalín. Fluctuations in the number of points on smooth plane curves over finite fields. *J. Number Theory*, 130(11):2528–2541, 2010.

[6] A. Bucur, C. David, B. Feigon, and M. Lalín. Statistics for traces of cyclic trigonal curves over finite fields. *Int. Math. Res. Not. IMRN*, (5):932–967, 2010.

[7] A. Bucur, C. David, B. Feigon, and M. Lalín. Biased statistics for traces of cyclic p-fold covers over finite fields. In *WIN—women in numbers*, volume 60 of *Fields Inst. Commun.*, pages 121–143. Amer. Math. Soc., Providence, RI, 2011.

[8] A. Bucur, C. David, B. Feigon, M. Lalín, and K. Sinha. Distribution of zeta zeroes of Artin-Schreier covers. *Math. Res. Lett.*, 19(6):1329–1356, 2012.

[9] G. Cheong, M. M. Wood, and A. Zaman. The distribution of points on superelliptic curves over finite fields. *Proc. Amer. Math. Soc.*, 143(4):1365–1375, 2015.

[10] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[11] A. Entin. On the distribution of zeroes of Artin-Schreier L-functions. *Geom. Funct. Anal.*, 22(5):1322–1360, 2012.

[12] M. Homma and S. J. Kim. The second largest number of points of plane curves over finite fields. work in progress.

[13] M. Homma and S. J. Kim. Nonsingular plane filling curves of minimum degree over a finite field and their automorphism groups: supplements to a work of Tallini. *Linear Algebra Appl.*, 438(3):969–985, 2013.

[14] T. Ibukiyama. On rational points of curves of genus 3 over finite fields. *Tohoku Math. J. (2)*, 45(3):311–329, 1993.

[15] N. M. Katz and P. Sarnak. *Random matrices, Frobenius eigenvalues, and monodromy*, volume 45 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 1999.
[16] J. E. Kolassa. *Series approximation methods in statistics*, volume 88 of *Lecture Notes in Statistics*. Springer-Verlag, New York, second edition, 1997.
[17] P. Kurlberg and Z. Rudnick. The fluctuations in the number of points on a hyperelliptic curve over a finite field. *J. Number Theory*, 129(3):580–587, 2009.
[18] G. Lachaud and C. Ritzenthaler. On some questions of Serre on abelian threefolds. In *Algebraic geometry and its applications*, volume 5 of *Ser. Number Theory Appl.*, pages 88–115. World Sci. Publ., Hackensack, NJ, 2008.
[19] G. Lachaud, C. Ritzenthaler, and A. Zykin. Jacobians among abelian threefolds: a formula of Klein and a question of Serre. *Math. Res. Lett.*, 17(2), 2010.
[20] K. Lauter. The maximum or minimum number of rational points on genus three curves over finite fields. *Compositio Math.*, 134(1):87–111, 2002. With an appendix by Jean-Pierre Serre.
[21] R. Lercier, C. Ritzenthaler, F. Rovetta, and J. Sijsling. Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. *LMS J. Comput. Math.*, 17(suppl. A):128–147, 2014.
[22] J.-F. Mestre. Courbes de genre 3 avec S_3 comme groupe d'automorphismes, 2010. `http://arxiv.org/abs/1002.4751`.
[23] E. Nart and C. Ritzenthaler. Jacobians in isogeny classes of supersingular abelian threefolds in characteristic 2. *Finite fields and their applications*, 14:676–702, 2008.
[24] E. Nart and C. Ritzenthaler. Genus three curves with many involutions and application to maximal curves in characteristic 2. In *Proceedings of AGCT-12*, volume 521, pages 71–85. Contemporary Mathematics, 2010.
[25] B. Poonen. Bertini theorems over finite fields. *Ann. of Math. (2)*, 160(3):1099–1127, 2004.
[26] C. Ritzenthaler. *Aspects arithmétiques et algorithmiques des courbes de genre* 1*,* 2 *et* 3. Habilitation à Diriger des Recherches, Université de la Méditerranée, 2009.
[27] C. Ritzenthaler. Explicit computations of Serre's obstruction for genus-3 curves and application to optimal curves. *LMS J. Comput. Math.*, 13:192–207, 2010.
[28] J.-P. Serre. Nombres de points des courbes algébriques sur $\mathbf{F}_q$. In *Seminar on number theory, 1982–1983 (Talence, 1982/1983)*, pages Exp. No. 22, 8. Univ. Bordeaux I, Talence, 1983.
[29] A. B. Sørensen. On the number of rational points on codimension-1 algebraic sets in $\mathbf{P}^n(\mathbf{F}_q)$. *Discrete Math.*, 135(1-3):321–334, 1994.
[30] G. Tallini. Le ipersuperficie irriducibili d'ordine minimo che invadono uno spazio di Galois. *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8)*, 30:706–712, 1961.
[31] G. Tallini. Sulle ipersuperficie irriducibili d'ordine minimo che contengono tutti i punti di uno spazio di Galois $S_{r,q}$. *Rend. Mat. e Appl. (5)*, 20:431–479, 1961.
[32] G. van der Geer and M. van der Vlugt. Supersingular curves of genus 2 over finite fields of characteristic 2. *Mathematische Nachrichten*, 159:73–81, 1992.
[33] M. M. Wood. The distribution of the number of points on trigonal curves over $\mathbb{F}_q$. *Int. Math. Res. Not. IMRN*, (23):5444–5456, 2012.
[34] M. Xiong. The fluctuations in the number of points on a family of curves over a finite field. *J. Théor. Nombres Bordeaux*, 22(3):755–769, 2010.
[35] M. Xiong. Distribution of zeta zeroes for abelian covers of algebraic curves over a finite field. *J. Number Theory*, 147:789–823, 2015.

DGA MI, La Roche Marguerite, 35174 Bruz, France.

Institut de recherche mathématique de Rennes, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France.
E-mail address: `reynald.lercier@m4x.org`

Institut de recherche mathématique de Rennes, Université de Rennes 1, Campus de Beaulieu, 35042 Rennes, France.
E-mail address: `christophe.ritzenthaler@univ-rennes1.fr`

Institut de Mathématiques de Luminy, UMR 6206 du CNRS, Luminy, Case 907, 13288 Marseille, France.
E-mail address: `florent.rovetta@univ-amu.fr`

Department of Mathematics, 27 N. Main Street, 6188 Kemeny Hall, Hanover, NH 03755-3551, United States of America.
E-mail address: `sijsling@gmail.com`

INRIA Saclay, Île-de-France, Laboratoire d'Informatique de l'École polytechnique (LIX), 91128 Palaiseau, France.
E-mail address: `smith@lix.polytechnique.fr`

Bibliographie

[AO00] D. Abramovich and F. Oort. Alterations and resolution of singularities. *Progr. Math.*, 181 :39,108, 2000.

[AQ12] Michela Artebani and Saül Quispe. Fields of moduli and fields of definition of odd signature curves. *Arch. Math. (Basel)*, 99(4) :333–344, 2012.

[Bas15] Romain Basson. *Arithmétique des espaces de modules des courbes hyperelliptiques de genre 3 en caractéristique positive*. Univeristé de Rennes 1, 2015. Thèse de doctorat.

[BCP13] Stéphane Ballet, Jean Chaumine, and Julia Pieltant. Shimura modular curves and asymptotic symmetric tensor rank of multiplication in any finite field. In *Algebraic informatics*, volume 8080 of *Lecture Notes in Comput. Sci.*, pages 160–172. Springer, Heidelberg, 2013.

[Ber08] Jonas Bergström. Cohomology of moduli spaces of curves of genus three via point counts. *J. Reine Angew. Math.*, 622 :155–187, 2008.

[Bra88] Rolf Brandt. *Über die Automorphismengruppen von algebraischen Funktionenkörpern*. Universität-Gesamthochschule Essen, 1988. Thèse de doctorat.

[CGLR99] G. Cardona, J. González, J. C. Lario, and A. Rio. On curves of genus 2 with Jacobian of GL_2-type. *Manuscripta Math.*, 98(1) :37–54, 1999.

[Cha78] H. C. Chang. On plane algebraic curves. *Chinese J. Math.*, 6(2) :185–189, 1978.

[Cle72] A Clebsch. *Theorie der binären algebraischen Formen*. Verlag von B. G. Teubner, Leipzig, 1872.

[CN07] Gabriel Cardona and Enric Nart. Zeta function and cryptographic exponent of supersingular curves of genus 2. In *Pairing-based cryptography—Pairing 2007*, volume 4575 of *Lecture Notes in Comput. Sci.*, pages 132–151. Springer, Berlin, 2007.

[CNP05] Gabriel Cardona, Enric Nart, and Jordi Pujolàs. Curves of genus two over fields of even characteristic. *Math. Z.*, 250(1) :177–201, 2005.

[CQ05] Gabriel Cardona and Jordi Quer. Field of moduli and field of definition for curves of genus 2. In *Computational aspects of algebraic curves*, volume 13 of *Lecture Notes Ser. Comput.*, pages 71–83. World Sci. Publ., Hackensack, NJ, 2005.

[CQ07] Gabriel Cardona and Jordi Quer. Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}. *Trans. Amer. Math. Soc.*, 359(6) :2831–2849 (electronic), 2007.

[dCP76] C. de Concini and C. Procesi. A characteristic free approach to invariant theory. *Advances in Math.*, 21(3) :330–354, 1976.

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

[DK02] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[FS11] D. M. Freeman and T. Satoh. Constructing pairing-friendly hyperelliptic curves using weil restriction. *J. of Number Theory*, 131(5) :959âà 983, 2011.

[Gey74] W. D. Geyer. Invarianten binärer Formen. In *Classification of algebraic varieties and compact complex manifolds*, pages 36–69. Lecture Notes in Math., Vol. 412. Springer, Berlin, 1974.

[GH97] S. P. Glasby and R. B. Howlett. Writing representations over minimal fields. *Comm. Algebra*, 25(6) :1703–1711, 1997.

[Gor68] Paul Gordan. Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist. *J. Reine Angew. Math.*, (69) :323–354, 1868.

[Gro71] A. Grothendieck. *Revêtements étales et géométrie algébrique (SGA 1)*, volume 224 of *Lecture Notes in Math.* Springer-Verlag, Heidelberg, 1971.

[GV12] A. Guillevic and D. Vergnaud. Genus 2 hyperelliptic curve families with explicit jacobian order evaluation and pairing-friendly constructions. In *Pairing-based cryptography—Pairing 2012*, volume 7708 of *Lecture Notes in Comput. Sci.*, pages 234–253. Springer, Berlin, 2012.

[Hil93] David Hilbert. *Theory of algebraic invariants*. Cambridge University Press, Cambridge, 1993. Translated from the German and with a preface by Reinhard C. Laubenbacher, Edited and with an introduction by Bernd Sturmfels.

[HKT08] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[HLT05] Everett W. Howe, Kristin E. Lauter, and Jaap Top. Pointless curves of genus three and four. In *Arithmetic, geometry and coding theory (AGCT 2003)*, volume 11 of *Sémin. Congr.*, pages 125–141. Soc. Math. France, Paris, 2005.

[HMSV09] Benjamin Howard, John Millson, Andrew Snowden, and Ravi Vakil. The equations for the moduli space of n points on the line. *Duke Math. J.*, 146(2) :175–226, 2009.

[Hom81] Masaaki Homma. Automorphisms of prime order of curves. *Manuscripta Math.*, 33(1) :99–109, 1980/81.

[Hug05] Bonnie Sakura Huggins. *Fields of moduli and fields of definition of curves*. ProQuest LLC, Ann Arbor, MI, 2005. Thesis (Ph.D.)–University of California, Berkeley.

[Hug07] Bonnie Huggins. Fields of moduli of hyperelliptic curves. *Math. Res. Lett.*, 14(2) :249–262, 2007.

[Igu60] Jun-ichi Igusa. Arithmetic variety of moduli for genus two. *Ann. of Math. (2)*, 72 :612–649, 1960.

[Kat96] P. Katsylo. Rationality of the moduli variety of curves of genus 3. *Comment. Math. Helv.*, 71(4) :507–524, 1996.

[Koi72] Shoji Koizumi. The fields of moduli for polarized abelian varieties and for curves. *Nagoya Math. J.*, 48 :37–55, 1972.

[KR84] Joseph P. S. Kung and Gian-Carlo Rota. The invariant theory of binary forms. *Bull. Amer. Math. Soc. (N.S.)*, 10(1) :27–85, 1984.

[LG15] Elisa Lorenzo Garcia. Twists of non-hyperelliptic curves. 2015. ArXive pre-print.

[Løn80] Knud Lønsted. The structure of some finite quotients and moduli for curves. *Comm. Algebra*, 8(14) :1335–1370, 1980.

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

[LRRS14] Reynald Lercier, Christophe Ritzenthaler, Florent Rovetta, and Jeroen Sijsling. Parametrizing the moduli space of curves and applications to smooth plane quartics over finite fields. *LMS J. Comput. Math.*, 17(A) :128–147, 2014.

[LRS12] Reynald Lercier, Christophe Ritzenthaler, and Jeroen Sijsling. Fast computation of isomorphisms of hyperelliptic curves and explicit descent, 2012. To appear in Proceedings of ANTS 2012, San Diego.

[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.

[MF82] David Mumford and John Fogarty. *Geometric invariant theory*, volume 34 of *Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]*. Springer-Verlag, Berlin, second edition, 1982.

[MM64] Hideyuki Matsumura and Paul Monsky. On the automorphisms of hypersurfaces. *J. Math. Kyoto Univ.*, 3 :347–361, 1963/1964.

[MSSV02] K. Magaard, T. Shaska, S. Shpectorov, and H. Völklein. The locus of curves with prescribed automorphism group. *Sūrikaisekikenkyūsho Kōkyūroku*, (1267) :112–141, 2002. Communications in arithmetic fundamental groups (Kyoto, 1999/2001).

[MT10] Stephen Meagher and Jaap Top. Twists of genus three curves over finite fields. *Finite Fields Appl.*, 16(5) :347–368, 2010.

[New78] P. E. Newstead. Introduction to moduli problems and orbit spaces. *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*, 51, 1978.

[Rök12] Karl Rökaeus. Computer search for curves with many points among abelian covers of genus 2 curves. In *Arithmetic, geometry, cryptography and coding theory*, volume 574 of *Contemp. Math.*, pages 145–150. Amer. Math. Soc., Providence, RI, 2012.

[Roq70] P. Roquette. Abschätzung der Automorphismenanzahl von Funktionenkörpern. *Math. Z.*, 117 :157–163, 1970.

[Sat09] T Satoh. Generating genus two hyperelliptic curves over large characteristic finite fields. In *Advances in Cryptology : EUROCRYPT 2009, Cologne*, volume 5479, Berlin, 2009. Springer.

[Sek85] Tsutomu Sekiguchi. Wild ramification of moduli spaces for curves or for abelian varieties. *Compositio Math.*, 54(3) :331–372, 1985.

[Ser68] Jean-Pierre Serre. *Corps locaux*. Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[Ser84] Jean-Pierre Serre. *Groupes algébriques et corps de classes*. Publications de l'Institut Mathématique de l'Université de Nancago [Publications of the Mathematical Institute of the University of Nancago], 7. Hermann, Paris, second edition, 1984. Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], 1264.

[Ser94] Jean-Pierre Serre. *Cohomologie galoisienne*, volume 5 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, fifth edition, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Stu08] Bernd Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, second edition, 2008.

[Suz82] Michio Suzuki. *Group theory. I*, volume 247 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1982. Translated from the Japanese by the author.

[vdGvdV92] Gerard van der Geer and Marcel van der Vlugt. Supersingular curves of genus 2 over finite fields of characteristic 2. *Math. Nachr.*, 159 :73–81, 1992.

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

[Wey39] Hermann Weyl. *The Classical Groups. Their Invariants and Representations*. Princeton University Press, Princeton, N.J., 1939.

Nomenclature

$(,)_h$ Le transvectant d'indice h, page 53

$[\mathcal{C}]$ point de l'espace de modules représentant la classe de la courbe $\mathcal{C}$, page 34

$\mathrm{Aut}'(\mathcal{C})$ Le groupe d'automorphismes réduits de $\mathcal{C}$, page 20

$\mathrm{Aut}(V)$ Le groupe d'automorphisme géométrique de la variété V, page 7

$\mathrm{Aut}_k(V)$ Le groupe d'automorphisme défini sur k de la variété V, page 7

$\mathbf{C}_n$ Le groupe cyclique d'ordre n, page 3

φ_α L'isomorphisme de V sur V_α, page 10

$\mathbf{D}_{2n}$ Le groupe diédral d'ordre $2n$, page 3

$\mathbb{F}_q$ Corps fini à q éléments, page 3

$\mathrm{Fr}(\mathrm{Aut}(V))$ L'ensemble des classes de conjugaison par Frobenius, page 9

ς Le morphisme de Frobenius, page 9

$\mathrm{Gal}_{\overline{k}/k}$ Le groupe de Galois absolu de k, page 7

$\mathbf{M}_V$ Le corps de modules de la variété V, page 35

$\mathcal{M}_{\mathfrak{g}}(k)$ L'espace de modules de genre $\mathfrak{g}$ sur k, page 34

$\overline{k}$ La clôture algébrique de k, page 3

φ^σ φ à la puissance σ, page 7

$\mathbb{P}^1$ La droite projective définie sur $\overline{k}$, page 19

$\mathbf{R}_{\mathcal{C}}$ Le corps résiduel du point $[\mathcal{C}]$, page 35

$\mathrm{Twist}(V)$ L'ensemble des tordues de V, page 7

$\widetilde{\mathcal{S}}_3$ la représentation de $\mathcal{S}_3$ dans $\mathrm{GL}_3(K)$ par l'action de permutation induite sur les coordonnées, page 38

$\widetilde{\mathcal{S}}_4$ un relèvement de degré 2 de $\mathcal{S}_4$ sur $\mathrm{GL}_3(K)$, page 38

$\{g\}_{\mathrm{Fr}}$ La classe de conjugaison par Frobenius de g, page 9

$D(K)$ le sous-groupe des matrices diagonales dans $\mathrm{PGL}_3(K)$, page 38

$Fr_g(\mathbb{F}_{q^a})$ La complexité bilinéaire de l'élévation à la puissance Frobenius d'une matrice de taille g, page 15

$H^1(\mathrm{Gal}_{\overline{k}/k}, \mathrm{Aut}(V))$ L'ensemble des classes de cohomologie de $\mathrm{Aut}(V)$, page 8

I_V L'intersection de tous les corps de définition de V, page 35

$Inv_g(\mathbb{F}_{q^a})$ La complexité bilinéaire d'une inversion de matrice de taille g dans le corps $\mathbb{F}_{q^a}$ sur le corps $\mathbb{F}_q$, page 15

k Un corps commutatif, page 3

$M_g(\mathbb{F}_{q^a})$ a complexité bilinéaire de la multiplication de deux matrices de taille g dans le corps $\mathbb{F}_{q^a}$, page 15

$T(K)$ le sous-groupe de $D(K)$ des matrices qui ont une valeur différente de 1 sur la diagonale seulement à la première ligne, page 38

V_α La tordue de V associée à l'automorphisme α, page 10

$\mathcal{B}(n)$ Le sous-anneau de $k[\mu_1, \nu_1, \mu_2, \nu_2, \ldots, \mu_n, \nu_n, x, z]$ engendré par les crochets, page 60

$\mathcal{B}_{reg,sym}(n)$ Le sous-anneau de $\mathcal{B}_{reg}(n)$ des polynômes en les crochets qui sont symétriques, page 60

$\mathcal{B}_{reg}(n)$ Le sous-anneau de $\mathcal{B}(n)$ des polynômes en les crochets qui sont réguliers, page 60

$\mathcal{S}_n$ Le groupe symétrique d'ordre factorielle n, page 3

$\mathcal{C}_n$ L'algèbre des covariants d'une forme binaire de degré n, page 53

$\mathcal{I}_n$ L'algèbre des invariants d'une forme binaire de degré n, page 53

$\mathcal{A}_n$ Le groupe alterné d'ordre factorielle n divisé par 2, page 3

Index